SSF Standard

스마트도시표준화포럼 단체표준 제정일: 2013년 1월 18일
SSF-ST-T-0009

스마트시티 내에서 보안 영역 표준

(Security Domain in the Smart City)

스마트도시표준화포럼 단체표준 제정일 : 2013년 1월 18일
SSF-ST-T-0009

스마트시티 내에서 보안 영역 표준

(Security Domain in the Smart City)

스마트도시표준화포럼

서 문

1. 표준의 목적

스마트시티 내에는 도시민이 필요로 하는 서비스를 안전하고, 정확하고, 신속하게 제공하기 위해 정보자산이 가지고 있는 취약점을 악용하는 보안위협의 노출 수준을 수용 가능한 수준으로 통제하기 위해 보안에 대한 영역을 정의하는데 그 목적이 있다.

2. 주요 내용 요약

스마트시티 시스템의 보안영역은 통합운영센터(서버팜, 자가망), 인터넷 망, 연계기관망, 운영자 보안영역으로 구성된다.

보안 위협을 최소화 할 수 있도록 국산 암호화 알고리즘인 SEED, ARIA 알고리즘을 탑재한 보안모듈을 사용하여 보안통신구간을 지정한다. 기존 인프라에서 지정되는 암호화 알고리즘 기준은 AES(256 이상)을 사용하기를 권고하며 신규 사업이나 SI프로젝트인 경우 국산암호화 알고리즘을 적용한다.

가. 스마트시티 인프라 보안통신구간을 정의
나. 보안 위협을 최소화 가능한 안전한 국산 암호화 보안 모듈 적용
다. 보안 망 구축 시 참조모델로 적용
라. 암호화 알고리즘 기준 AES 256 이상, 신규 개발의 경우 국산알고리즘 채택 하여 적용한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

4. 참조 표준(권고)

스마트시티 장비간 보안 통신 표준 (2011, SSF 단체표준)

4.1 국외표준(권고)

4.2 국내표준

5. 참조표준(권고)과의 비교

5.1 참조표준(권고)과의 관련성

5.2 참조한 표준(권고)과 본 표준의 비교표

단체표준안	(표준개정시, 개정전 표준)	참조표준 :	비고

6. 지적재산권 관련사항

해당 사항 없음

7. 적합인증 관련사항

7.1 적합인증 대상 여부

본 표준에 따라 개발된 ‘스마트시티내에서 보안 영역 정의’의 경우 본 표준에 따라 보안영역에 대한 표준화 적합성 시험을 통해 표준적합성 인증시험이 이루어져야 한다.

7.2 시험표준제정여부(해당 시험표준번호)

본 표준에 따라 ‘스마트시티내에서 보안 영역 정의’ 규격에 적합하게 개발되었는지 표준 적합성 시험 표준을 제정하고 있다.

8. 표준의 이력

판수	제/개정일	제·개정내역
제1판	2013.1.18	제정

목 차

스마트시티 내에서 보안 영역 표준
(Security Domain in the Smart City)

1. 개요

스마트시티 내에는 도시민이 필요로 하는 서비스를 안전하고, 정확하고, 신속하게 제공하기 위해 정보자산이 가지고 있는 취약점을 악용하는 보안위협의 노출 수준을 수용 가능한 수준으로 통제하기 위해 보안을 위한 통신 구간을 지정한다.

2. 지침의 구성 및 범위

본 지침에서는 보안 위협을 최소화 할 수 있도록 국산 암호화 알고리즘인 SEED, ARIA 알고리즘을 탑재한 보안모듈을 사용하여 보안통신구간을 지정한다. 기존 인프라에서 지정되는 암호화 알고리즘 기준은 AES(256 이상)을 사용하기를 권고하며 신규 사업이나 SI프로젝트인 경우 국산암호화 알고리즘을 의무적으로 사용하길 권고한다.

(1) 스마트시티 인프라 보안통신구간을 정의
(2) 보안 위협을 최소화 가능한 안전한 국산 암호화 보안 모듈 적용
(3) 보안 망 구축 시 참조모델로 적용
(4) 암호화 알고리즘 기준 AES 256 이상, 신규 개발의 경우 국산알고리즘 채택

3. 용어 정의

용어의 표기는 한국정보통신기술협회의 정보통신용어사전 표기를 기본으로 한다.

3.1 스마트시티 (Smart City)

첨단 정보통신 인프라와 스마트 컴퓨팅 기술 및 정보 서비스가 융합된 차세대 정보화 도시이다. 스마트시티는 첨단 정보통신 인프라와 정보 서비스를 도시공간에 융합하여 도시생활의 편의 증대, 체계적인 도시 관리에 의한 안정보장 및 도시기능의 지능화에 의한 삶의 질 향상 등 도시 제반 기능을 혁신시킬 수 있는 차세대 정보화 도시를 의미한다. 이와 동시에 『스마트도시 조성 및 산업진흥 등에 관한 법률』(법률 제15309호, 2017.12.26)제2조1항에 정의된 “스마트도시”를 의미한다.

3.2 단위 서비스 (Smart Service, 스마트 서비스)

하나 이상의 기능의 집합인 스마트시티 구현에 필요한 서비스. 『스마트도시 조성 및 산업진흥 등에 관한 법률』(법률 제15309호, 2017.12.26)제2조2항과 『스마트도시

조성 및 산업진흥 등에 관한 법률 시행령』(대통령령 제29045호, 2018. 7. 16)제2조에 정의된 “스마트도시서비스” 그 자체 또는 하위요소가 되는 서비스를 의미한다.

3.3 스마트시티 통합운영센터

스마트시티 통합운영센터는 스마트시티의 관리 및 운영을 담당하는 시설이다. 스마트시티를 관리하고 운영하기 위하여 연관된 각 분야의 정보시스템을 연계 및 통합하여 운영한다. 『스마트도시 조성 및 산업진흥 등에 관한 법률』(법률 제15309호, 2017.12.26)제2조3항과 『스마트도시 조성 및 산업진흥 등에 관한 법률 시행령』(대통령령 제29045호, 2018. 7. 16)제4조에 정의된 “스마트도시의 관리 • 운영에 관한 시설” 그 자체 또는 하위요소가 되는 시설을 의미한다.

3.4 통합플랫폼

스마트시티 통합운영센터의 구성요소로서 스마트시티와 연관된 각 분야의 정보시스템을 연계하는 소프트웨어 플랫폼이다.

3.5 인터페이스(Interface)

2개의 시스템이 상호 작용할 수 있도록 접속되는 경계에서 상호 접속하기 위한 조건 및 규약을 의미한다.

3.6 상호운용성(Ineroperability)

같은 기종 또는 다른 기종의 기기끼리 상호간에 통신할 수 있고, 정보 교환이나 일련의 처리를 정확하게 실행할 수 있는 것을 의미한다.

3.7 프로토콜(Protocol)

서로 다른 기종의 컴퓨터 사이에 어떤 자료를, 어떤 방식으로, 언제 주고 언제 받을지 등을 정해놓은 규약이다. TCP/IP가 대표적인 통신프로토콜이다.

3.8 네트워크(Network)

통신선로에 의해 서로 연결되어 있는 일련의 노드 또는 연결점들을 의미한다. 네트워크는 다른 네트워크와 연결될 수 있고, 서브 네트워크를 포함할 수 있다. 가장 보편적인 네트워크 형상인나 구성에는 버스형, 성형, 링형 등이 있으며 네트워크의 공간적인 범위에 따라서 LAN(Local Area Network), MAN(Metropolitan Area Network) 그리고 WAN(Wide Area Network) 등으로 구분된다.

3.9 서브네트워크(Sub-Network)

어떤 기관에 소속된 네트워크이지만 따로 분리되어 있는 한 부분으로 인식될 수 있는 네트워크를 말한다.

3.10 LAN(Local Area Network)

집, 사무실, 학교, 건물 내 등 가까운 지역의 컴퓨터들을 고속으로 연결하는 네트워크이다.

3.11 Ethernet

대표적인 근거리통신(LAN) 기술로서 10Mbps~수Gbps까지의 속도를 제공한다.

3.12 WAN(Wide Area Network)

공중 통신 사업자가 제공하는 전용선, 패킷 교환망, 종합 정보 통신망(ISDN) 등의 통신 회선 서비스를 사용하여 광범위한 지역을 상호 접속하여 형성한 대규모 통신망. LAN이 비교적 좁은 범위에서 고속으로 품질이 좋은 전송을 행하는 반면, WAN은 통신 속도 및 전송 품질은 다소 나쁘지만 넓은 지역을 서비스 할 수 있다.

3.13 Network Topology(네트워크 토폴로지)

컴퓨터, 케이블 및 기타 네트워크 구성 요소의 배열 또는 물리적 배치상태를 말하며, 네트워크에 필요한 장비의 성능과 수량, 네트워크 확장성 및 관리 방법에 따라 토폴로지의 선택이 달라진다.

3.14 Node(노드)

네트워크를 구성하는 기본요소인 라우터를 말한다. 또는 네트워크에 연결된 컴퓨터들을 포함해 노드라고 부르기도 한다.

3.15 OSI(Open System Interconnection)

OSI는 통신 네트워크로 구성된 컴퓨터가 어떻게 데이터를 전송할 것인가에 대한 표준규약 및 참조모델이다. 이것의 목적은 통신 제품을 만들 때 다른 제품과 모순됨이 없이 통신하도록 유도하는 것이다. OSI 참조모델은 통신의 종단에서 이루어지는 기능을 7계층으로 정의하였다.

3.16 OSI 참조모델(OSI Reference Model)

OSI 참조모델은 네트워크 내에서 메시지가 한쪽에서 다른 쪽으로 보내졌을 때, 각 단에서 필요한 관련 기능들의 다음 7개 계층으로 설명한다.

7계층 : 응용계층(Application Layer, L7)
6계층 : 표현계층(Presentation Layer, L6)
5계층 : 세션계층(Session Layer, L5)
4계층 : 전송계층(Transport Layer, L4)
3계층 : 네트워크계층(Network Layer, L3)
2계층 : 데이터링크계층(Data Link Layer, L2)
1계층 : 물리계층(Physical Layer, L1)

3.17 암호화

의미를 알 수 없는 형식(암호문)으로 정보를 변환하는 것을 말한다. 이는 개인 정보 취급자의 실수 또는 해커의 공격 등으로 인해 개인정보가 비인가자에게 유•노출되더라도 그 주요 내용을 확인할 수 없게 하는 보안기술이다.

3.18 암호키

메시지를 암호화 또는 복호화 하는데 사용되는 키로, 암호키를 소유한 자만이 암호문을 생성하거나 복호할 수 있다.

3.19 해쉬함수

임의 길이의 메시지를 항상 고정된 길이의 해쉬 값으로 변환하는 일방향 함수를 말한다.

3.20 일방향 함수

결과값을 가지고 입력값을 구하는 것이 어려운 함수로, 해쉬함수는 일방향 함수에 해당한다.

3.21 블록암호

평문을 일정한 블록 크기로 나누어, 각 블록을 송•수신자 간에 공유한 비밀 키를 사용하여 암호화 하는 방식

3.22 SSL(Secure Sockets Layer)

데이터를 송•수신하는 두 컴퓨터 사이, 종단 간 즉 TCP/IP 계층과 어플리케이션 계층(HTTP, TELNET, FTP 등) 사이에 위치하여 인증, 암호화, 무결성을 보장하는 사실 표준 프로토콜을 말한다.

3.23 TLS(Transport Layer Security)

SSL을 대신하는 차세대 안전 통신 규약으로, SSL을 대신하는 차세대 안전 통신 규약으로, SSL보다 적용 범위가 넓꼬 안전성과 활용성이 강화 되었다.

3.24 보안서버

인터넷상에서 전송되는 자료를 암호화하여 송•수신하는 기능르 제공하는 웹 서버를 지칭한다.

3.25 시스템관리자

다중 사용자 컴퓨터 시스템과 통신 시스템의 사용에 대한 관리 책임을 지는 사람으로, 사용자 계정과 암호의 할당, 기밀(보안) 접근 수준의 설정, 기억 장치 공간 할당 등을 수행하는 사람

3.26 보안관리자

비인가된 접근으로부터 통신 네트워크 및 시스템, 응용 서비스 등의 보호책임을 지는 사람 으로써, 보안 관련 이벤트의 분석, 암호 키의 분배 제어, 인가된 사용자의 접근 권한 관리 등을 수행

3.27 서비스 제공기관

가입자 또는 고객이 통신망을 이용해서 접속하는 서비스를 운영하는 기업 혹은 조직

3.28 정보통신망

여러 가지 통신 정보를 디지털 신호화함으로써 다양한 서비스를 종합적으로 제공하는 통신망

3.29 데이터 센터

기업고객들로부터 인터넷서비스를 아웃소싱 받아 서버와 네트워크를 제공하고 컨텐츠를 대신 관리해주는 곳

3.30 오픈 네트워크

개방형 네트워크로써 대표적인 예로 인터넷 등을 의미

3.31 암호키

전자문서를 대칭 암호화방식으로 암호화 또는 복호화하기 위하여 이용하는 전자적 정보

3.32 키 암호키

암호키를 대칭 암호화방식으로 암호화 또는 복호화하기 위하여 이용하는 전자적 정보를 말하며, “ 키 포장 키”라고도 함

3.33 마스터키

대칭 암호화방식을 사용하여 다른 암호키 또는 키 암호키를 유추하는 데 사용되는 전자적 정보

3.34 암호키분배키

암호키 또는 정보를 안전하게 전송 또는 분배하기 위하여 이용하는 공개키 암호화방식의 전자적 정보로서 암호키분배공개키와 암호키 분배개인키

3.35 에이전트

장면에 따라서 의도를 이해하고 자립적인 판단에 의해 처리를 실행하는 기능. 즉, 목적하는 웹 페이지를 찾아내면 특정 목적을 실행하는 프로그램

3.36 보안통제

정보 시스템을 보호하기 위해 제공된 하드웨어, 펌웨어 및 소프트웨어 안에서 구현되는 보안 메커니즘과 물리적, 인적, 절차적 및 관리적 보안 요구 사항을 포함하는 조치 사항들

3.37 공중망(Public Network)

통신 사업자나 통신 주관청이 제공하는 교환 접속형 전기 통신망으로써, 교환을 통하여 전국 또는 전 지역 불특정 다수의 사용자에게 서비스를 제공하는 통신망

3.38 사설망(Private Network)

공중망과 대칭되는 말로써, 인터넷, 네트워크 혹은 음성 통신을 기업 내의 전용선 통신망과 같이 사용하는 네트워크

3.39 터널링

하위층 통신 규약의 패킷을 상위층 통신 규약으로 캡슐화하는 것으로, 통신망상의 두 점 간에 통신이 되도록 하는 것

3.40 PPP(Point to Point Protocol)

컴퓨터 통신망에서 통신 데이터를 송수신하는 데에 사용하는 프로토콜로, 두 대의 컴퓨터가 직렬 인터페이스를 이용하여 통신을 할 때 필요한 프로토콜

3.41 인증 헤더(AH, Authentication Header)

IPSec에서 데이터의 무결성과 인증 및 재사용 방지를 위해 메시지 패킷에 덧붙이는 정보

3.42 ESP(Encapsulating Security Payload)

IP 보안 프로토콜(IPSec)에 있어서 데이터의 무결성과 프라이버시(privacy)를 제공하는 기능으로써, 인증되지 않은 데이터 스트림에 대한 공격을 막기 위해 제한적 트래픽 흐름의 비밀성을 제공함

3.43 IKE(Internet Key Exchange)

인터넷 표준 암호 키 교환 프로토콜 (RFC 2409)

3.44 PLS(Multi Protocol Label Switching)

IETF가 표준화 작업 중인 cut and through 방식의 패킷 전송의 계층 3 레벨 스위칭 기술

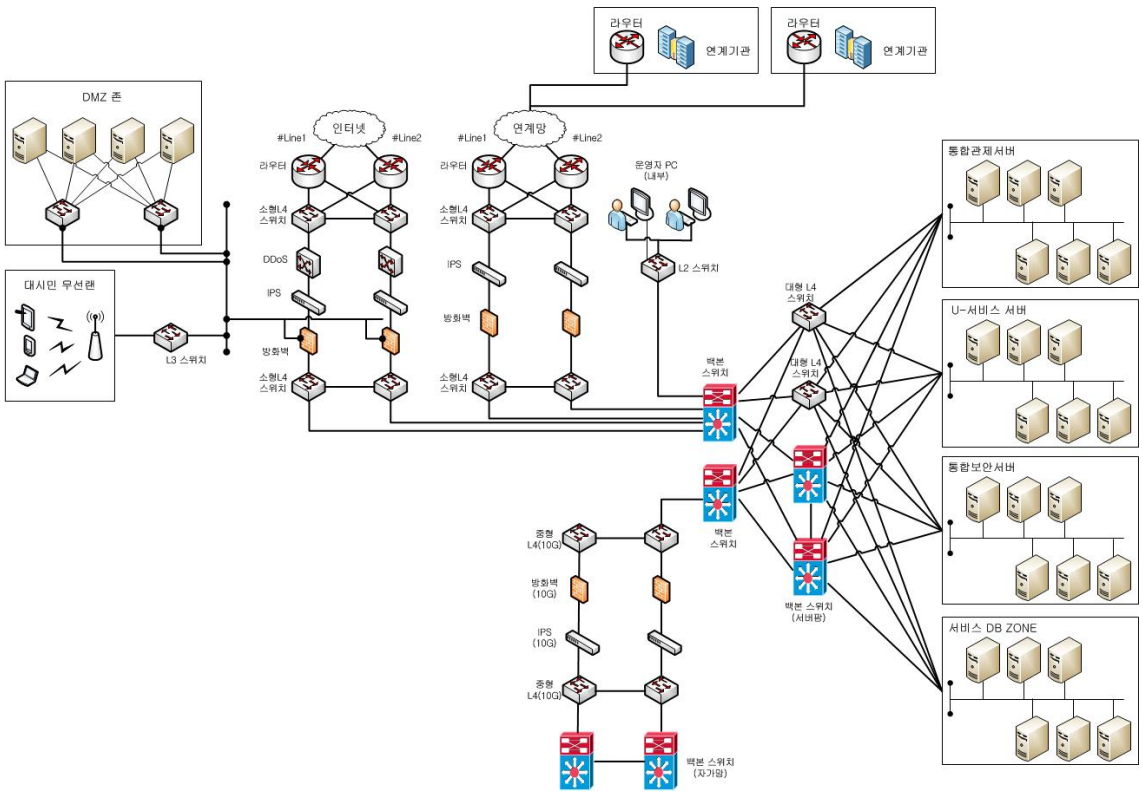
4. 스마트시티 보안영역 설계

4.1 설계 개요

스마트시티 시스템의 보안영역을 설계함에 있어 안정성, 확장성, 장애대응의 신속성 등을 고려하여, 스마트시티 보안영역을 정의한다.

4.2 보안영역 구성도

스마트시티 시스템의 보안영역은 다음 (그림 1)과 같이 통합운영센터(서버팜, 자가망), 인터넷 망, 연계기관망, 운영자 보안영역으로 구성된다.



(그림 4-1) 스마트시티 보안영역 구성도

4.3 보안영역 장비 내역

스마트시티 보안영역 구성에 사용되는 장비들은 다음 <표 4-1>과 같다.

<표 4-1> 스마트시티 보안영역 장비내역

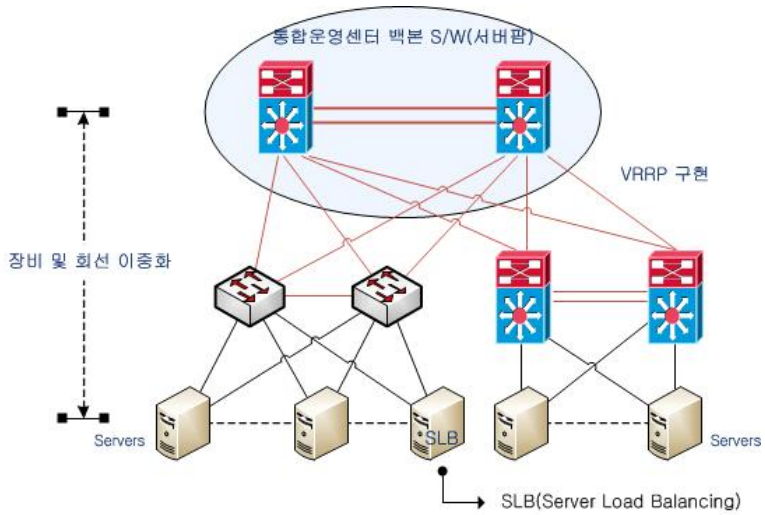
구분	사양	수량
백본 스위치	IP Routing Protocol (RIP, OSPF, BGP 등) 지원 스위치 성능 : 700Gbps SFlow, 유해트래픽 자동감지 및 자동차단 기능 H/W 기반의 IPv6 지원 H/W 기반의 IP 멀티캐스트 스위칭 전원 이중화 제공	6
L3 Switch	L3 Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 ports individually configurable to 10/100/1000 BaseT 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports.	1
L2 Switch	12.8Gbps 이상의 Switching Fabric 지원 9.52Mpps 이상의 Throughput 지원 128MB 이상의 DRAM 및 32MB 이상의 Flash 지원 24 Port 10/100T 및 2 Port 1000T or Gigabit Uplink 지원 Resilient Stacking, Across Stack 특징 및 관리 지원 IEEE 802.1D Spanning Tree 지원	2
라우터	2Gbps 이상의 시스템 백플레인 용량 제공 500Kpps 이상의 패킷 처리 성능 지원 LAN & WAN 인터페이스 지원 2GB 이상의 DRAM 및 1GB 이상의 Flash 제공 다양한 프로토콜 지원	6
L4 스위치 (대형+중형+소형)	2Gbps 이상의 Application 처리 성능 제공 최대 5,000,000개 이상의 Concurrent Session 지원 초당 40,000개 이상의 L4 Connection 처리율 제공 초당 1,200,000개 이상의 DDoS 공격에 대한 방어기능 제공 SLB, GSLB, FWLB 및 TCS 지원	12
Firewall(방화벽)	특정한 Signature를 이용하여 공격패턴 지원 비정상적인 프로토콜을 검사하여 차단 Traffic Anomaly Detection and Prevention Fail Over 기능 지원 Anti-Virus 엔진 내장으로 메일을 통해 유입되는 웜/바이러스에 대한 차단 제공 국산 암호화 알고리즘(SEED, ARIA) 탑재한 모듈 적용 국가정보원 및 한국정보보호진흥원으로부터 CC(EAL3+) 인증 획득	3 (1G) 2 (10G)
IPS (침입방지시스템)	유해트래픽(Worm, DoS/DDoS) 탐지 및 차단 실시간 트래픽 모니터링, 일체형 장비 이중화 구성 및 최신 공격패턴 / 공격 C;ass에 대한 2,500개 이상의 Signature 제공 정보보안취약성 DB서비스를 웹 또는 이메일을 통해 제공 네트워크 구성 및 패킷의 변경 없이 다양한 설치 지원 IPS CC(EAL4) 인증 취득한 제품	2 (1G) 2 (10G)
IP관리시스템	IP SCAN AGENT IP SCAN S/W H/W 및 DBMS포함	1
DDos방지 시스템	분산서비스 공격 방어용 제품 UDP, ICMP등 네트워크 공격 유해트래픽 차단 실시간 감시 및 관리자 알림	2

4.4 보안영역 구성

가. 통합운영센터 보안영역 구성

스마트시티 보안영역의 안정적인 운영을 위하여 이중화 체계로 구축

(1) 통합운영센터 서버팜 보안영역 구성



(그림 4-2) 통합운영센터 서버팜 보안영역 구성도

(가) 통합운영센터 서버팜 보안영역 구축방안

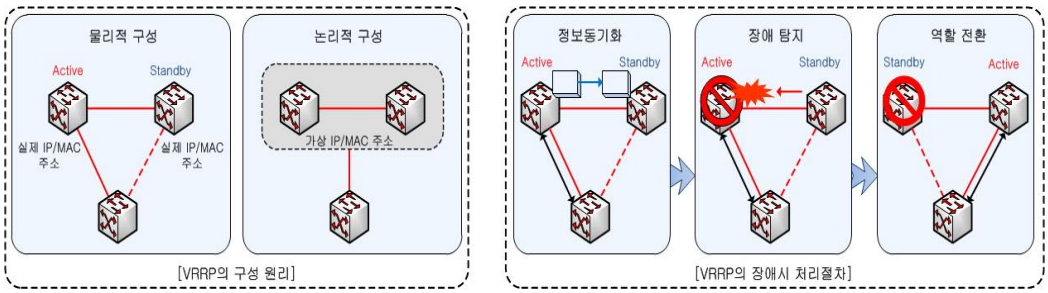
1) 백본 스위치의 안정성을 위해 장비, 회선 이중화 구현
2) 백본 스위치 성능 향상 및 안정성을 위해 CPU, Power 이중화 구현
3) L4 스위치 부문 다양한 Server들과 연결
   - SLB(Server Load Balancing)을 통해 서버 부하 분산 처리
   - L4 Switch를 통한 Traffic 부하 분산 처리함으로써, 보안장비 부하 감소
   - 일반 Server는 1000Base-T 또는 1GbE로 연결 되며, 회선 이중화 함
   - L4 Switch 이중화를 통한 안정성 확보
4) 1000Base-Tx Server는 L3 Switch를 통해 연결되며, 회선 이중화 함
   - 백본 스위치와 L3 스위치간 VRRP 구현
   - L3 스위치간 Trunk 구성

(나) 통합운영센터 서버팜 보안영역 구현 기술

1) VRRP (Virtual Router Redundancy Protocol): 물리적인 두 대의 장비를

가상의 논리적인 한대의 장비로 구성하도록 하는 기술

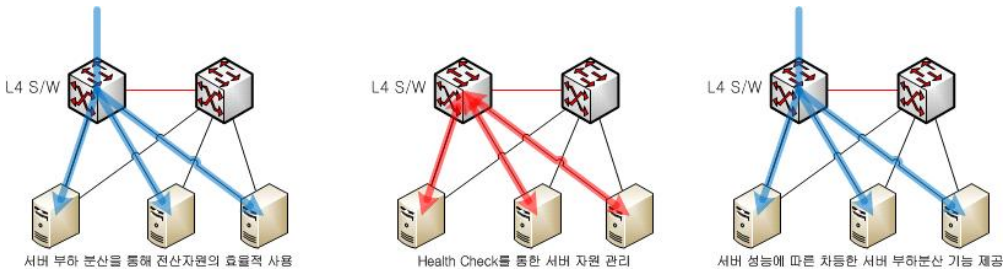
- 가상의 IP/MAC 주소를 사용하여 타 장비와 통신
- 물리적인 두 대의 장비는 Active/Standby 방식으로 평상시에는 Active 장비만 동작
- Active 장비의 장애 시 Standby 장비는 장애 탐지 및 활성화되어 Active 장비의 역할 수행
- Active / Standby 장비간 연결회선을 통해 수집된 정보를 동기화하여 역할 전환 시 무중단 서비스 제공



(그림 3-3) VRRP 구현기술

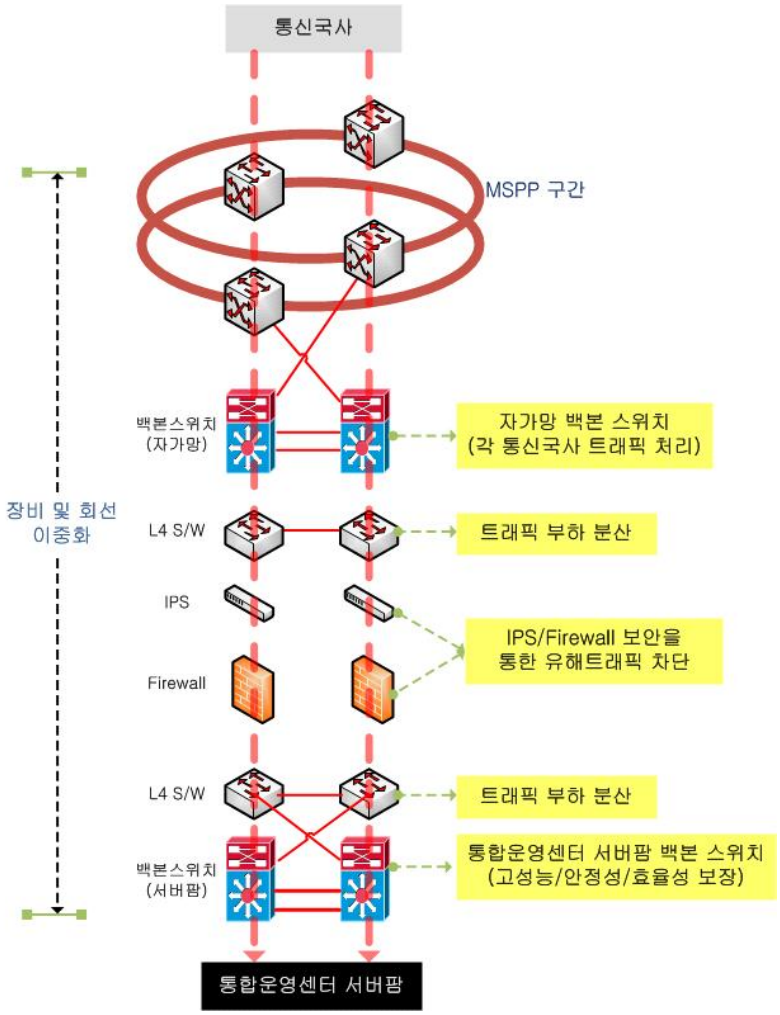
2) SLB (Server Load Balancing)

- L4 스위치/모듈의 서버 부하분산 기능을 통해 서버로 향하는 트래픽 부하분산
- 다양한 부하분산 기능을 통해 회선 대역폭 사용률 증대 전산자원의 효율적 사용
- L4 스위치/모듈의 Health Check 기능을 통해 서버 자원의 정상 서비스 여부 확인



(그림 4-4) SLB 구현기술

(2) 통합운영센터 자가망 보안영역 구성



(그림 4-5) 통합운영센터 자가망 보안영역 구성

(가) 자가망 보안영역 연결 구성

1) MSPP 이중화 구성

- Dual Ring형 구조로 신뢰성 우수

2) 자가망 백본스위치는 각 통신국사의 트래픽을 원활하게 처리

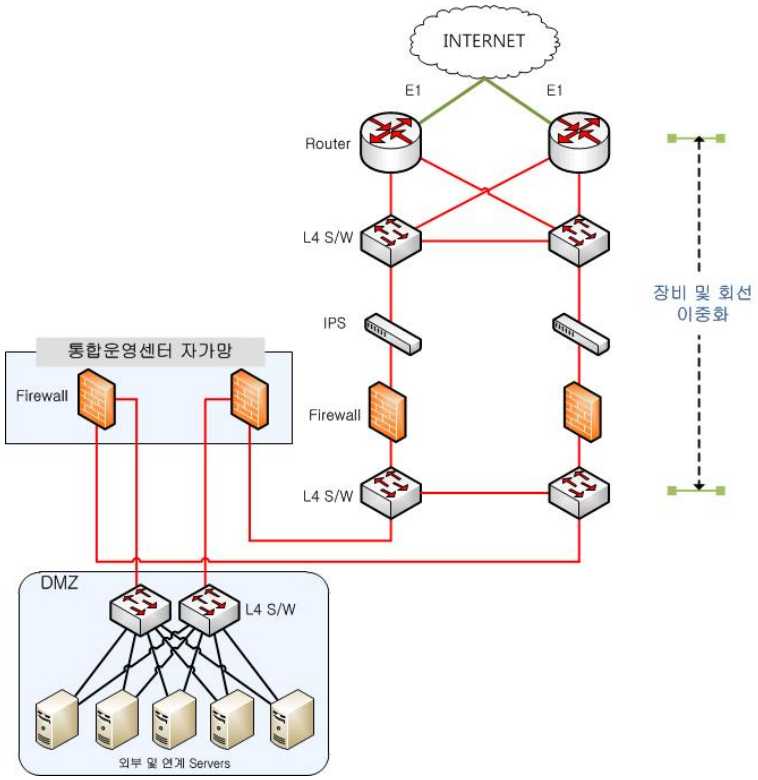
3) 자가망 보안영역은 장비 및 회선 이중화로 안정성 확보

4) 통신국사에서 올라오는 트래픽에 대해 보안 강화 및 부하분산

- 보안강화 : Firewall, IPS 장비 구축
- L4 스위치를 통한 Traffic 분산처리

나. 인터넷 망 보안영역 구성

(1) 인터넷 망 보안영역 구성



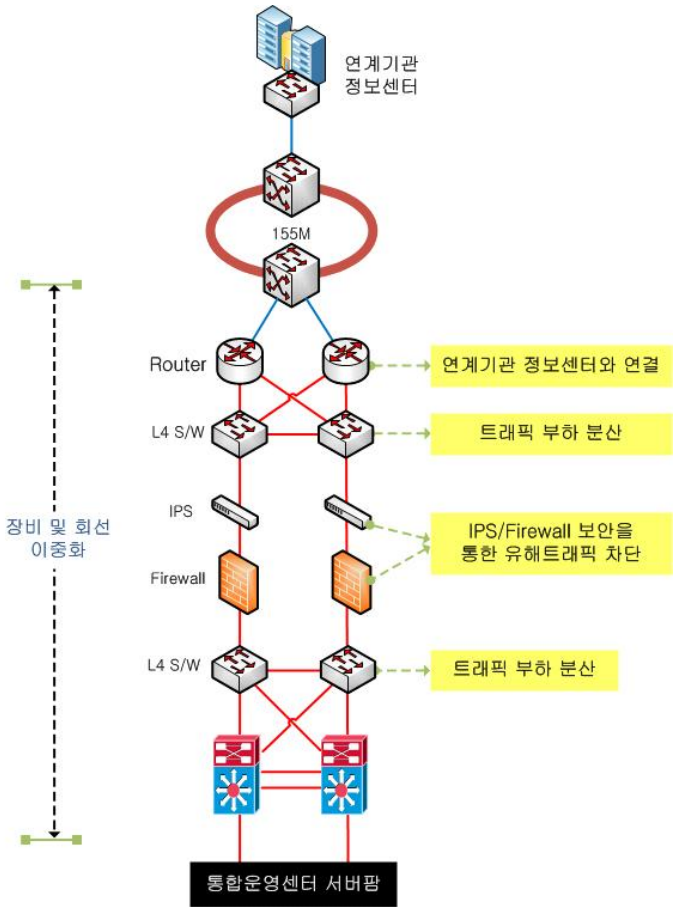
(그림 4-6) 인터넷 망 보안영역 구성

(가) 인터넷 망 보안영역 구성

1) 인터넷 망 보안영역은 통합운영센터의 주요 Server를 보호하기 위해 물리적으로 분리
   - 업무망 Firewall단에서 분리
   - 통신국사에서 올라오는 인터넷 트래픽을 통합운영센터 자가망의 Firewall에서 분리
2) 장비 및 회선 이중화로 안정성 확보
3) L4 스위치를 통한 FLB(Firewall Load Balancing) 구현
   - Firewall 성능 보장(트래픽 부하분산으로 인한 Firewall 부하 감소)
4) 보안 장비를 통한 인터넷 망 보호
   - IPS(침입방지시스템)
   - Firewall(방화벽)
5) DMZ 구간 구현
   - 주요 웹서버 및 기타 서버는 L4 스위치를 통해 트래픽 분산 처리
   - DMZ 포트는 별도의 정책 설정으로 인한 보안 강화

다. 연계기관망 보안영역 구성

(1) 연계기관망 보안영역 구성



(그림 4-7) 연계기관 망 보안영역 구성

(가) 연계기관망 보안영역 연결 구성

1) 연계기관망 보안영역 구성은 장비 및 회선 이중화를 통해 안정성 확보

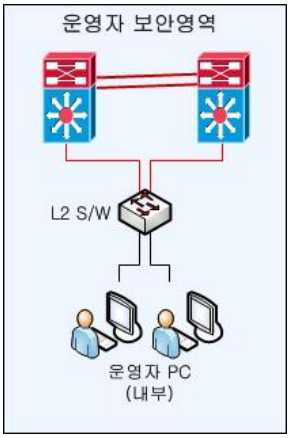
2) Router를 통해 연계기관과의 연결

- 인천교통정보센터 연결(사용 예)
- 155M MSPP와 연결 (Router와 MSPP간 100Mbps로 연결)

3) 연계기관에서 올라오는 트래픽에 대한 보안강화 및 부하분산

- 보안강화 : Firewall, IPS 장비 구축
- L4 스위치를 통한 Traffic 분산처리

(2) 운영자 보안영역 구성



(그림 4-8) 운영자
보안영역 구성

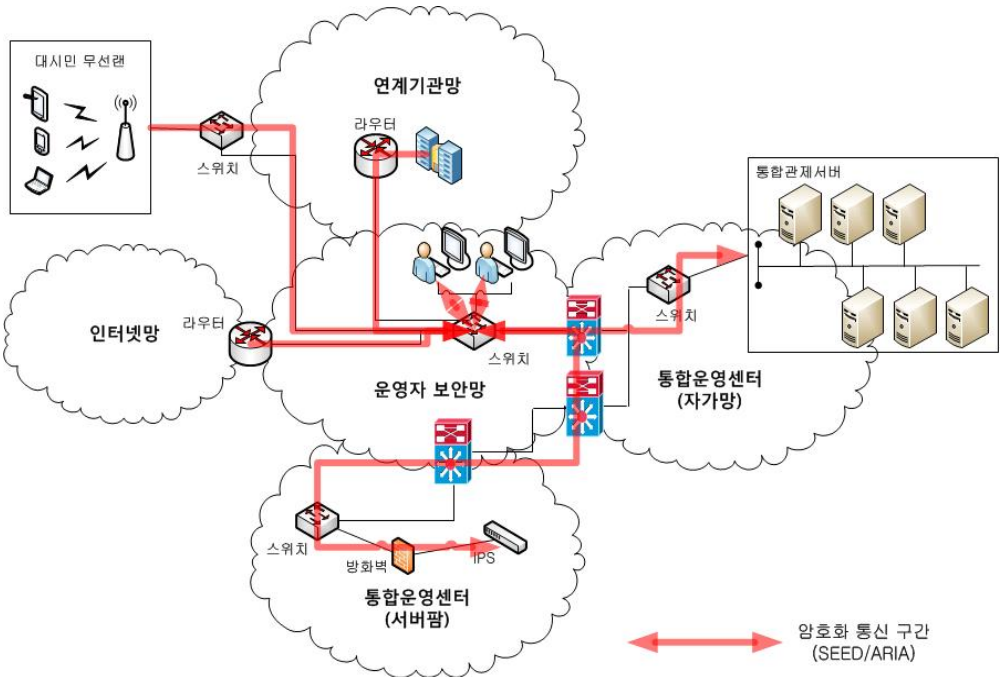
(가) 운영자 PC 연결 구성

1) 운영자 L2 스위치는 통합운영센터 서버팜 스위치와 회선 이중화로 연결

2) 사용자는 주요 네트워크 장비 및 시스템 관리

5. 스마트시티 보안모듈 적용

다음 (그림 5-1)은 암호 알고리즘을 적용한 암호화 통신구간을 보인다.



(그림 5-1) 스마트시티 암호화 통신구간

5.1 보안 모듈의 목적

보안모듈은 스마트시티 환경에서 스마트 단말(스마트 Device)와 대시민 서비스 제공 서버에 설치되어, 스마트 Device 사용자가 대시민 서비스 제공 서버로부터 제공되는 서비스들을 안전하게 이용하기 위해 필요한 사용자 인증, 안전한 메시지 교환을 위한 암호키 및 MAC키 협상, 메시지 암호화 및 무결성 검증 기능을 수행한다.

보안모듈은 스마트시티 인프라를 구성하는 단말, AP, 스위치, 게이트웨이, 스마트 서비스 제공 서버 등에 각각 설치되어 이들 장치 간 안전한 메시지 교환을 위해 필요한 장치 인증, 안전한 메시지 교환을 위한 암호키 및 MAC키 협상, 메시지 암호화 및 무결성 검증 기능을 수행한다.

보안모듈은 단말 및 장치 간 동작과정 중 발생한 중요 정보를 기록하며, 인가된 사용자에 의해 조회될 수 있도록 관리한다.

5.2 보안 모듈 동작 환경

보안모듈은 스마트시티 환경에서 동작하는 모든 단말장비, AP, 스위치, 게이트웨이, 스마트 서비스 제공 서버 등에 설치되어 동작한다.

보안모듈은 라이브러리 형태로 C 언어를 이용하여 구현되며, 보안모듈에서 제공되는 서비스를 이용하는 응용은 규정된 API를 이용한다.

보안모듈에서 사용자 인증과 장치 인증은 스마트시티 인프라 관리기능을 담당하는 기관이 지정한 인증기관에서 발행된 인증서를 기반으로 이루어진다.

스마트시티 인프라를 구성하는 모든 장치와 스마트시티 서비스를 이용하려는 사용자의 스마트 Device에는 스마트시티 인프라 관리기능을 담당하는 기관이 지정한 인증기관에서 발행된 인증서가 지정된 절차에 따라 설치되어야 한다. (스마트 Device와 장치의 인증서 발급, 저장, 검증, 관리, 오류 처리 및 인증기관에 관한 체계 등은 논의 후 별도로 결정되어야 함)

사설인증서나 공인인증서가 없이 장비를 인증하는 경우에는 별도로 인증서버나 장비인증을 수행 가능토록 하는 시스템에 연계하여 관리자와 기관의 사용을 득한 후에 통신 개폐가 이루어 질수 잇도록 한다.

5.3 보안 모듈 기능

가. 사용자 인증

- 스마트 Device를 이용하여 대시민 서비스 등을 이용하려는 사용자는 먼저 스마트 Device에서 제공되는 단말인증 설정기능을 통해 EAP-TLS 인증방법을 이용한 802.1X 인증절차를 완료해야 한다.
- 사용자 인증은 사용자가 스마트 Device를 통해 접속하려는 장치 또는 서버 간

“암호키 및 MAC키 협상” 절차 중 전달되는 스마트 Device 사용자 인증서를 이용하여 이루어진다. 사용자 인증서를 이용한 인증 절차는 SSL Handshake 프로토콜 절차에 준하여 이루어진다.
- 사용자 인증에 관련된 인증 서버는 외부와 내부로 엄격히 분리하여 수행하되 인증서의 유무와 관계없이 인증을 득한 후에 통신 개폐를 수행해야 한다.

나. 장치 인증

- 스마트시티 인프라를 구성하는 장치들은 스마트시티 서비스 환경의 안전성을 높이기 위해 각 장치에는 스마트시티 인프라 관리기능을 담당하는 기관이 지정한 인증기관에서 발행된 인증서가 설치되어야 한다.
- 장치 인증은 해당 장치가 연결하려는 상대 장치 간 “암호키 및 MAC키 협상” 절차 중 전달되는 해당 장치의 인증서를 이용하여 이루어진다. 장치 인증서를 이용한 인증 절차는 SSL Handshake 프로토콜 절차에 준하여 이루어진다.
- 장비 인증에 관련된 인증 서버는 외부와 내부로 엄격히 분리하여 수행하되 인증서의 유무와 관계없이 인증을 득한 후에 통신 개폐를 수행해야 한다.

다. 암호키 및 MAC키 협상

- 보안모듈을 이용하여 안전한 메시지를 교환하는 통신 상대들은 메시지 교환이 이루어지기 전 암호키 및 MAC키를 결정하는 협상과정을 거쳐야 한다.
- 통신 상대 간 암호키 및 MAC키 계산 이전에 메시지 암호화에 사용될 암호알고리즘 종류, MAC 계산용 해쉬알고리즘이 먼저 결정되어야 하며 이 결정과정은 SSH Handshake 프로토콜 절차에 준하여 이루어진다.
- 통신 상대 간 이용되는 암호 알고리즘에 ARIA, SEED 암호 알고리즘이 필수적으로 지원되어야 한다.
- 그 외에 암호화 알고리즘은 국제법상 통용되는 AES 256이상을 지원하면 인정하도록 한다.
- 통신 상대 간 암호키 및 MAC키 계산을 위한 비밀정보(pre-master secret) 교환은 각 통신 상대의 인증서에 포함된 공개키를 이용하여 교환한다.
- 암호키 및 MAC키 협상은 SSH Handshake 프로토콜 절차에 준하여 이루어지며, 협상이 성공적으로 이루어는 경우 통신 상대는 각각 암호키와 MAC키를 계산하게 된다.
- 암호키 및 MAC키 협상이 성공하거나 실패한 경우 각 보안모듈은 시각 정보, 통신 상대 식별정보, 협상 내용, 성공 여부 및 오류 코드 등을 기록, 보관한다.
- 키관리와 관련된 정보는 상단에 인증서버나 혹은 인증기관에서 별도록 관리토록 하여 키에 대한 분실 및 제어에 대한 보안을 강화 할수 있도록 한다.

라. 메시지 암호화 및 무결성 검증

- 보안모듈을 이용하는 통신 상대는 암호키 및 MAC키 협상 과정에서 계산된 암호키, MAC키를 이용하여 모든 메시지에 대해 암호화와 무결성 점검 기능을 수행한다.
- 암호화 과정과 무결성 점검용 정보가 추가된 메시지는 신뢰성있는 통신 채널을 이용하여 통신 상대에게 전달되어야 하며, 통신 상대로부터 메시지 수신에 대한 응답을 확인한 후 다음 메시지가 전송되어야 한다.
- 메시지 암호화 및 무결성 검증과정에서 오류가 발생한 경우 각 보안모듈은 시각 정보, 통신 상대 식별정보, 오류 관련 정보를 기록, 보관한다.

마. 로그 생성 및 관리

- 보안모듈은 사용자 인증 및 장치 인증, 암호키 및 MAC키 협상, 메시지 암호화 및 무결성 검증 과정에서 발생되는 주요 정보를 기록, 보관해야 한다.
- 필요 시 별도 설정에 의해 기록되는 로그 기능 활성화 여부와 생성되는 로그 항목을 설정할 수 있어야 한다.
- 기록된 로그 정보는 인가된 사용자에 한해 조회, 검색될 수 있도록 저장, 관리되어야 한다.

5.4 보안 모듈 API

가. 제공 API 종류

- 보안모듈에서 제공되는 각 기능에 대해 API를 정의하여 해당 기능을 이용하려는 응용에게 제공되어야 한다.
- 보안모듈을 이용하는 클라이언트 응용이 특정 서버 응용으로 접속을 요청하는 API가 제공되어야 한다. 클라이언트 응용이 서버 응용과 접속이 정상적으로 이루어지면 API는 안전한 통신채널 식별자를 응용으로 회신해야 한다.
- 보안모듈을 이용하는 서버 응용이 클라이언트 응용으로부터 접속이 발생할 때까지 대기하는 API가 제공되어야 한다. 서버 응용이 클라이언트 응용과 접속이 정상적으로 이루어지면 API는 안전한 통신채널 식별자를 응용으로 회신해야 한다.
- 보안모듈을 이용하는 클라이언트 응용과 서버 응용이 동시에 이용할 수 있는 암호화 및 무결성 점검기능을 수행하는 API가 제공되어야 한다.

나. API 형식

- 클라이언트 응용이 특정 서버 응용으로 접속을 요청하는 API에는 서버 식별정보등이 포함되어야 한다.
- 서버 응용이 클라이언트 응용으로부터 접속이 발생할 때까지 대기하는 API에

는 서버의 인증서 정보 등이 포함되어야 한다.

- 클라이언트 응용과 서버 응용이 동시에 이용할 수 있는 암호화 및 무결성 점검 기능을 수행하는 API에는 안전한 통신채널 식별자, 메시지 내용 등이 포함되어야 한다.

5.5 보안 모듈 이용 응용 동작 구조

가. 서버 측

- 보안모듈을 이용하여 작성된 서버 응용은 특정 TCP 포트에 접속 요청이 발생할 때까지 대기한다. 이 절차는 서버 응용이 보안모듈에서 제공되는 지정된 API를 호출함으로써 이루어진다.
- 특정 TCP 포트로 접속 요청이 발생되면 암호키 및 MAC키 협상 절차가 자동적으로 진행된다.
- 암호키 및 MAC키 협상 절차가 정상적으로 이루어지면 서버 응용은 클라이언트와 교환되는 모든 메시지에 대해 암호화 및 무결성 점검을 수행한다. 이 절차는 서버 응용이 보안모듈에서 제공되는 지정된 API를 호출함으로써 이루어진다.

나. 클라이언트 측

- 보안모듈을 이용하여 작성된 클라이언트 응용은 접속하려는 서버의 특정 TCP 포트에 접속 요청을 시도한다. 이 절차는 클라이언트 응용이 보안모듈에서 제공되는 지정된 API를 호출함으로써 이루어진다.
- 서버 응용과의 접속 요청 후 서버 측 보안모듈과 암호키 및 MAC키 협상 절차가 자동적으로 진행된다.
- 암호키 및 MAC키 협상 절차가 정상적으로 이루어지면 클라이언트 응용은 서버 교환되는 모든 메시지에 대해 암호화 및 무결성 점검을 수행한다. 이 절차는 클라이언트 응용이 보안모듈에서 제공되는 지정된 API를 호출함으로써 이루어진다.

5.6 암호 알고리즘 적용

스마트시티 보안영역내 사용하는 암호 알고리즘은 SEED, ARIA를 사용할 것으로 권고한다. 이에 대한 적용 방식은 한국인터넷진흥원(http://www.kisa.or.kr)내 전자서명 인증관리센터에서 발간한 “암호 알고리즘 및 키길이 이용 안내서”를 활용하여 사용할 것을 권고한다.

일반적으로 암호 알고리즘은 다음과 같이 RSA, SEED, ARIA, SHA를 사용한다.

가. RSA

RSA는 "Rivest"와 "Shamir", "Adleman"에 의해 개발된 공개키 암호화 방식이다. RSA 알고리즘은 두 개의 큰 소수들의 곱과, 추가 연산을 통해 하나는 공개키를 구성하고 또 하나는 개인키를 구성하는데 사용되는 두 세트의 수 체계를 유도하는 작업이 수반된다. 한 번 그 키들이 만들어지면, 원래의 소수는 더 이상 중요하지 않으며, 버릴 수 있다. 공개 및 개인키 둘 모두는 암호화/복호화를 위해 필요하지만, 오직 개인키의 소유자만이 그것을 알 필요가 있다. RSA 시스템을 사용하면, 개인키는 절대로 인터넷을 통해 보내지지 않는다.

아래 <표 5-1>는 용도에 따라 사용되는 키를 정리하고 있다.

<표 5-1> 키에 따른 용도

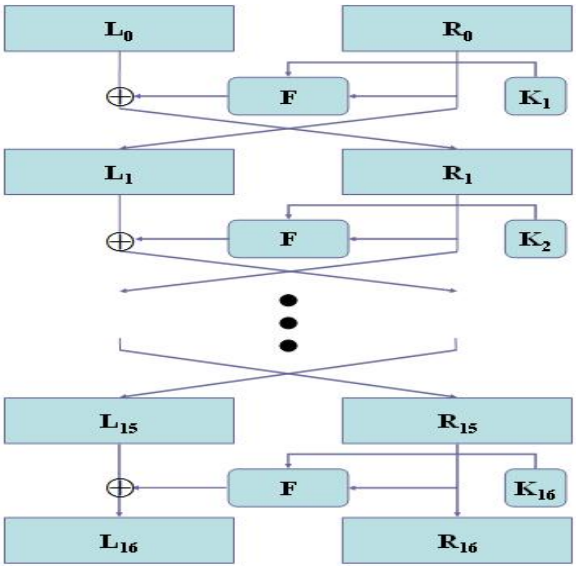
구 분	누구의 어떤 키를 사용하나?
암호화된 메시지를 보냄	수신자의 공개키
암호화된 서명을 보냄	발신자의 개인키
암호화된 메시지를 복호화	수신자의 개인키
암호화된 서명 (발신자 인증)을 복호화	발신자의 공개키

나. SEED

SEED는 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 2월 한국인터넷진흥원과 국내 암호전문가들이 순수 국내 기술로 개발한 128비트 블록 암호 알고리즘이다. 1999년에는 128비트 키를 지원하는 SEED 128을 개발하였으며, 암호 알고리즘 활용성 강화를 위해 2009년 256 비트 키를 지원하는 SEED 256을 개발하였다.

SEED 알고리즘의 전체 구조는 Feistel 구조로 이루어져 있으며, 128비트의 평문 블록과 128비트 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트 암호문 블록을 출력한다. 아래 그림은 SEED 알고리즘의 전체구조를 도식화한 것이다.

아래 그림에서 F 함수는 수정된 64비트 Feistel 형태로 구성된다. F 함수는 각 32비트 블록 2개를 입력으로 받아, 32비트 블록 2개를 출력한다. 즉, 암호화 과정에서 64비트 블록과 64비트 라운드 키를 F 함수의 입력으로 처리하여 64비트 블록을 출력한다.



(그림 5-2) SEED 전체 구조도

다. ARIA

ARIA는 Academy(학계), Research Institute(연구소), Agency(정부 기관)의 첫 글자들을 딴 것으로 ARIA 개발에 참여한 학·연·관의 공동 노력을 표현하기 위하여 생성된 이름으로써 경량 환경 및 하드웨어에서의 효율성 향상을 위해 개발되었으며, ARIA가 사용하는 대부분의 연산은 XOR과 같은 단순한 바이트 단위 연산으로 구성되어 있다. ARIA는 경량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다. ARIA는 128비트의 블록 단위로 암호화를 진행하며 키 크기는 AES와 동일한 규격인 128/192/256 비트를 지원한다. 라운드는 12/14/16이며 키 크기에 따라 결정된다. ARIA의 전체 구조는 Involutional Substitution-Permutation Network 구조이다.

ARIA는 블록 암호에 대한 알려진 모든 공격에 대한 내성을 갖도록 설계되었고 일차적으로 설계자들에 의한 내부적인 안전성 분석을 거친 뒤에, 객관적인 안정성 및 효율성 평가를 위하여 NESSIE의 주관 기관인 벨기에 루벤 대학으로부터 평가를 받았다.

라. SHA

SHA(Secure Hash Algoritm) 함수들은 서로 관련된 암호화적 해쉬 함수들의 모임이다. 이들 함수는 미국 국가 안전 보장국(NSA)이 1993년에 처음으로 설계했으며 미국 국가 표준으로 지정되었다. SHA 함수군에 속하는 최초의 함수는 공식적으로 SHA라고 불리지만, 나중에 설계된 함수들과 구별하기 위하여 SHA-0라고도 불린다. 2년 후 SHA의 변형인 SHA-1이 발표되었으며, 그 후에 4종류의 변형이 더 발표되었다. SHA는 160비트의 크기의 해쉬 값을 만들어 낸다.

마. AES

AES(Advanced Encryption Standard)는 미국의 연방 표준 알고리즘으로서 20년이 넘게 사용되어 온 DES(Data Encryption Standard)를 대신할 차세대 표준 알고리즘이다.DES는 1972년에 미국 상무성 산하 NIST (National Institute of Standards and Technology)의 전신인 NBS(National Bureau of Standards)에서 컴퓨터 데이터를 보호할 목적으로 표준 알고리즘을 공모하여 IBM사가 개발한 암호 알고리즘이다. DES는 연방 표준으로 제정된 후에 5년마다 안정성을 인정받으면서 표준으로 존속되어 왔으나, 1997년 이후 안정성에 대한 논란이 대두되자 NIST가 DES를 대체할 차세대 표준 암호 알고리즘 제정을 위한 프로젝트로 추진한 것이 AES이다. AES 알고리즘이 채택되면 현재 사용되고 있는 DES를 대신하게 되고, 로열티 없이도 사용할 수 있게 된다.[출처: 매일경제 매경닷컴 지식 사전]

부록 Ⅰ
보안 설계 방안

스마트시티 통신망 네트워크의 보안성을 강화하기 위해 Switch단에서의 보안 및 전용 보안장비(Firewall, IPS)을 통해 구현한다.

Ⅰ.1 Switch 보안

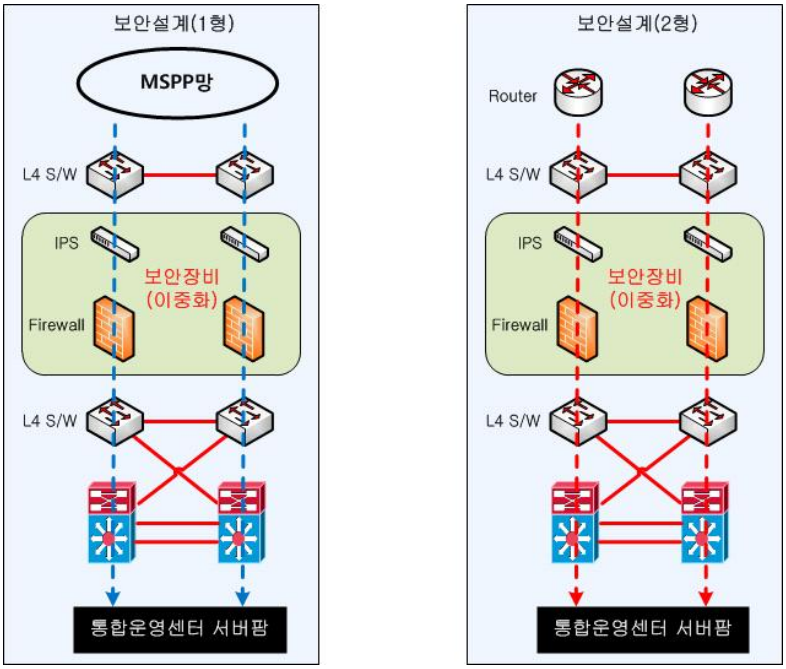
Ⅰ.1.1 백본 스위치는 분산형 다계층 보안기능, 다양한 사용자 인증 기능, 서비스 보호 거절 기능 등의 기능을 통해 보안성 제공

- 중계망과 코어망에 구현 가능한 통신망 사업자 수준의 보안성 관리 기능을 포함한 분산형 다계층 보안기능
- 사용자 인증기능, VLAN, ACL, 스위치 액세스 인증, 암호화, NAT/PAT, 서비스 보호 거절 기능
- 분산형 다계층 보안기능은 관리기능 및 스마트 카드, PKI, 바이오 매트릭 기능 등 첨단 보안관리 기술과 통합 가능한 하드웨어 및 소프트웨어 기반 솔루션의 구축을 가능하게 함
- 안정적인 시스템 관리를 위해서 사용자 인증기능, SNMPv3, 암호화 세션용 SSL, 다계층 액세스 및 단계적 네트워크 관리를 위한 분할 관리 기능 등 다양한 기능 지원

Ⅰ.2 전용 보안장비(Firewall, IPS)을 통한 보안

Ⅰ.2.1 보안 설계 (1형, 2형) 구성 방안

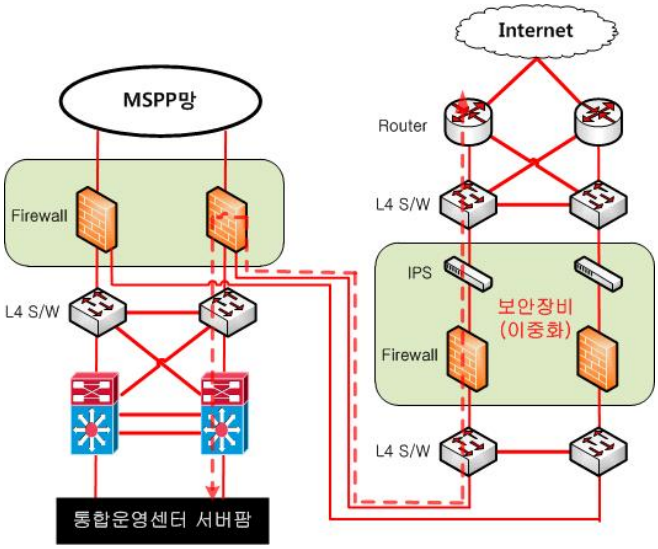
- Firewall, IPS 장비 이중화 구성
- L4 Switch를 통한 Traffic 부하 분산 처리함으로써, 보안장비 부하 감소
- 1형: 각 통신국사에서 들어오는 센터 보안장비를 통해 유해트래픽을 IPS에서 차단하며, Firewall에서는 불필요한 포트를 사전에 차단 및 보안 정책을 통하여 안정적인 서비스 제공
- 2형: 연계기관망에서 들어오는 유해트래픽을 IPS에서 차단하며, Firewall 에서는 불필요한 포트를 사전에 차단 및 보안 정책을 통하여 안정적인 서비스 제공



(그림 Ⅰ-1) 전용 보안장비(Firewall, IPS)을 통한 보안

Ⅰ.2.2 인터넷 구성 방안

- 통합운영센터 서버팜 백본스위치와 자가망 백본스위치 사이에 Firewall 이용
  - Firewall 포트 중 1개의 포트를 인터넷을 위한 포트로 사용
  - 별도의 정책을 적용
- 인터넷 구간에 별도의 보안 장비를 구축
  - Firewall, IPS 장비 이중화 구성
  - L4 Switch를 통한 Traffic 부하 분산 처리함으로써, 보안장비 부하 감소
  - 인터넷에서 들어오는 유해트래픽을 IPS에서 차단하며, Firewall에서는 불필요한 포트를 사전에 차단 및 보안 정책을 통하여 안정적인 서비스 제공
- 보안장비 CC인증 현황
  - Firewall(방화벽) : EAL3+
  - IPS(침입방지시스템) : EAL4



(그림 Ⅰ-2) 인터넷 구성 방안

부록 Ⅱ
장비별 주요 기능

<표 Ⅱ-1> 통합운영센터 서버팜 백본, 자가망 백본, 서버팜 L3 스위치

구 분	상 세 내 역
이중화 Hot-Swap 기능	• CMM(Chassis Management Module) • 팬 트래이 / 전원 장치 / 스위칭 패브릭 • 네트워크 인터페이스 모듈 (NI)
시스템 세부 기능	• 분산형 L2/L3/L4 서비스 및 처리 기능 • 논-블러킹 스토어 앤 포워드(non-blocking store and forward) 스위칭 구조 • 유선 속도의 L2 / 유선 속도 L3 IP, IPX • 유선 속도 ACL(Access Control Lists) • 멀티캐스트 다계층 스위칭 • 유선 속도 서버 부하 분담
하드웨어 세부 기능	• 10Gbps 이더넷 802.3ae 표준 지원 • 10/100/1000 이더넷 자동 감지 및 PoE 지원 • 역방향 데이터에 대한 포트 미러링 • 802.3ad와 OmniChannel 포트 통합으로 포트 장애 복구 및 MAC 어드레스를 이용한 부하분담 기능 • 포트당 트래픽 흐름 제한 • IP 멀티캐스트 스위칭에 필요한 하드웨어 지원
VLAN 기능	• 포트 기반, IEEE 802.1Q VLAN 지원 • MAC 어드레스, L3기반, 포트 연결, 프로토콜 형태 별 구성 또는 맞춤형 구성 • 인증 기반, 정책 기반 VLAN • 802.1p-태그 프래임 (하이브리드 및 트랜스패어런트 포트 포함)을 위한 하드웨어 지원
QoS 기능	• 포트별 8개 우선순위에 따른 큐 처리 • 출력 시 802.1p, IP TOS, DiffServ 제어점 설정, 분산형 L2/L3/L4 서비스 및 처리 기능 • MAC DA, IP 프로토콜, IP SA/DA, TCP/UDP SA/DA, 포트, 인터페이스 형태, VLAN, 멀티캐스트 기준 우선순위 지정
라우팅 프로토콜	• Layer2/3/4 Switching 및 Multi Protocol 지원 • Routing Protocol 지원 : RIP v1/v2, OSPF v2, BGP4, I스마트 IS • Multicast Protocol 지원 : IGMP v1/v2/v3, BSR, PIM-SM/SSM/DM, DVMRP • Security Protocol 지원 : 원격 인증 RADIUS, TACACS+, LDAP, ACE 서버
IPv6	• 회선 최대 속도의 하드웨어 기반의 포워딩, 패킷 분류, 터널링 등 IPv6를 완벽히 지원 • 스위치 성능에 영향을 주지 않고 IPv4, IPv6, IPv4/IPv6를 선택하여 설치할 수 있는 유연성 제공
관리 기능	• 완벽한 NMS 통합을 위한 SNMP v1/v2/v3 지원 • 원격 모니터링(RMON) : 통계, 히스토리, 경고, 이벤트, sFlow 지원

<표 Ⅱ-2> 통합운영센터 서버팜 L4 스위치

구 분	상 세 내 역
구조	• Standalone Type
인터페이스	• FE, GE(Fiber/Copper), 10GE 인터페이스 각 4개이상 제공
안정성	• 전원 이중화 지원
Layer 3 기능	• L3 프로토콜 : Static, RIPv2, OSPF, VRRP, VRRP-E • VLAN 및 VLAN Trunking 지원
Layer 4 기능	• SLB, FWLB,VPNLB, IPSLB, 등 동시 부하분산 지원 • Health Check : ARP, ICMP, Layer 4(Port Based), Layer 7(Content Based)
Layer 7 기능	• Contents Analysis 기능을 통한 L7 Contents 감지 로드벨런싱
보안(옵션)	• L3 기반의 ACL 정책 지원 • PORTSCAN 차단 지원 및 출발지 또는 목적지 기준 범람 제어 제공 • DDoS 공격에 대한 방어기능 제공

<표 Ⅱ-3> DMZ 구간 L4 스위치

구 분	상 세 내 역
구조	• Standalone Type
인터페이스	• FE, GE(Fiber/Copper), 10GE 인터페이스 각 4개이상 제공
안정성	• 전원 이중화 지원
Layer 3 기능	• L3 프로토콜 : Static, RIPv2, OSPF, VRRP, VRRP-E • VLAN 및 VLAN Trunking 지원
Layer 4 기능	• SLB, FWLB,VPNLB, IPSLB, 등 동시 부하분산 지원 • Health Check : ARP, ICMP, Layer 4(Port Based), Layer 7(Content Based)
Layer 7 기능	• Contents Analysis 기능을 통한 L7 Contents 감지 로드벨런싱
보안(옵션)	• L3 기반의 ACL 정책 지원 • PORTSCAN 차단 지원 및 출발지 또는 목적지 기준 범람 제어 제공
보안	• 하드웨어 기반 ACL(Access Control List) 지원 • DDoS 공격에 대한 방어기능 제공

<표 Ⅱ-4> 보안 장비 연결용 L4 스위치

구 분	상 세 내 역
구조	• Standalone Type
인터페이스	• FE, GE(Fiber/Copper) 각 4개이상 제공
안정성	• 전원 이중화 지원
Layer 3 기능	• L3 프로토콜 : Static, RIPv2, OSPF, VRRP, VRRP-E • VLAN 및 VLAN Trunking 지원
Layer 4 기능	• SLB, FWLB,VPNLB, IPSLB, 등 동시 부하분산 지원 • Health Check : ARP, ICMP, Layer 4(Port Based), Layer 7(Content Based)
Layer 7 기능	• Contents Analysis 기능을 통한 L7 Contents 감지 로드벨런싱
보안(옵션)	• L3 기반의 ACL 정책 지원 • PORTSCAN 차단 지원 및 출발지 또는 목적지 기준 범람 제어 제공 • DDoS 공격에 대한 방어기능 제공

<표 Ⅱ-5> Firewall(방화벽)

구 분	상 세 내 역
DPI	Stateful Inspection의 한계를 넘어 단순 패킷의 상태 검사가 아닌 패킷 내용까지의 검사를 통해 보안성을 강화하며, 최신의 취약성 리스트를 빠르게 제공 받아 Worm 또는 바이러스 및 침해사고에 대해 빠르고 신속한 차단 공인된 DB를 이용하여 가장 빠르고 정확한 패턴 DB제공 국내 실정에 맞는 취약성 DB인 Hot List 제공 관제 센터에 의한 빠른 Hot List 업데이트
Anti Virus (V3 Warp Engine)	SMTP Gateway를 이용하여 전자우편을 통하여 유입되는 바이러스를 실시간 차단 및 치료 안철수연구소의 V3 Warp 엔진 탑재 최신의 바이러스 정보 데이터를 매주 자동으로 업데이트 긴급 바이러스 정보 데이터 자동 업데이트
다양한 Application Gateway	SMTP, HTTP, FTP, Telnet Gateway 등 다양한 Proxy 기능 SMTP Gateway를 통한 Mail Bomb, Mail Relay 등 방지 E-mail 수신자 수 제어 및 사용자별 일일 허용개수 제한기능 DNS 및 Reverse DNS Check을 통한 SPAM 차단 기능 HTTP Gateway를 통한 웹 접속 시 업로드 파일 크기 제한 정보통신윤리위원회 유해사이트 DB에 의한 접속 차단
NAT	침입차단시스템 내/외부의 공인 IP 대역과 사설 IP 대역의 주소 변환 기능 1:1, 1:N, M:N 주소 변환 기능 내부 네트워크의 IP 대역 숨김 기능 Normal / Redirect / Exclude / Reverse NAT 등 다양한 네트웍 환경에 적합한 NAT 기능
실시간 모니터링	프로토콜, 출발지, 목적지, 포트에 대한 상세정보 제공 패킷량, 바이트 수, 현재 세션 상태 정보 제공 연결된 세션에 대하여 실시간 세션 차단 기능 제공 NAT 상태, QOS 상태, Clustering 상태, Traffic Anomaly에 의해 차단된 Black List 정보 제공
Packet Filtering	출발지 주소, 목적지 주소, Protocol 별, 서비스 별, 시간대 별, 사용자 별 속성에 의한 접근제어 NIC 별 보안정책 수립 각 Rule 별 DPI 정책, Traffic Anomaly 정책 및 QOS 정책 설정 각 Rule 별 NAC (Network Admission Control) 설정 SEED, ARIA 알고리즘 탑재 보안모듈 적용

<표 Ⅱ-6> IPS(침입방지시스템)

구 분	상 세 내 역
Network Quata	인터페이스별 대역폭 제한 기능 IPS에서는 bps(사이즈별), pps(패킷수별)를 기준으로 제한 프로토콜, 포트별 필터링 기능 제공 제한된 패킷들은 Drop 되어짐
Real Time Monitor	실시간 세션정보(HTTP, FTP, Telnet등) 및 네트워크 트래픽 상황 확인 실시간 탐지/방어정보(해킹, 유저정의, 네트워크) 및 방어상황(방어제한 시간등) 확인
내부정보 유출 감시	IPS를 경유하는 세션에 대해 사용자가 어떤 작업을 수행하는지 확인 Telnet을 이용하여 어떤 명령의 수행 및 결과물을 실시간으로 확인 FTP를 이용한 파일의 전송내역을 실시간으로 확인 HTTP 프로토콜을 이용한 웹페이지의 접속상황을 실시간으로 확인
X Driver	IPS의 네트워크 드라이버 정상 동작 여부 확인 NIC를 통행하는 전체 패킷수와 각 에러 패킷수 즉시 확인 네트워크 문제 발생 시 신속한 원인 파악 및 해결
차단관리	Filtering & Matching으로 차단된 순간 그 정보가 Blocking List에 등록 Blocking List에서 만료된 리스트는 시간이 경과 하면 방어상태에서 해제 엔진에서 탐지한 공격 뿐만 아니라 수동으로 실시간 차단 리스트 관리
One Hop Failover	IPS간에는 Sync Trunk(Heartbit 링크)를 이용하여 Local 서버팜에 접속하는 세션 테이블 정보 및 기타 상태 정보 교환, 한쪽 시스템의 장애 발생시에도 서비스는 안정적으로 제공
Defragmentation	IPS는 Layer3 ~ Layer7에서 수행되는 단편화 공격에 대해 재조합 기술을 이용하여 탐지/방어 기능 제공
이벤트 축약	여러 공격패넡에 대한 대응전략을 수립함으로써 이벤트 발생에 대한 축약을 통한 탐지, 방지정책의 효율성 증대 같은 공격의 탐지 이벤트는 라인수의 증가가 아닌 카운트(횟수) 증가로 대응
Packet Capture	Hacking Proof확보를 위한 실시간 패킷 캡쳐기능 제공 관리자의 직접분석을 통하여 실제 공격여부 판단 (오탐지 최소화)
Live Update	정기적으로 새로운 보안 동향 분석 및 취약점 분류 실행 연구 및 분석에 따른 위험도 구분 및 공격 테스트, 취약점 필터 개발
Scheduling	업데이트 스케줄링 기능으로 자동으로 업데이트 서버와 통신하여 새로 추가된 패턴과 엔진을 업데이트
로그조회	네트워크, 공격정보의 상세내역 출력 Excel, CSV, Bmp, Jpeg 파일의 형식으로 별도 저장을 통한 보고서 커스터마이징

<표 Ⅱ-7> 인터넷망, 연계기관망

구 분	상 세 내 역
주요 부문	4개의 온보드 GigE 포트 및 모듈을 통해 확장 가능한 WAN/LAN 인터페이스 제공 IPv4/v6 기능 및 라우팅 프로토콜 등 가장 풍부한 MPLS 기능 결합 음성 솔루션 지원 음성과 같은 미션 크리티컬 트래픽의 우선순위를 지정하기 위한 풍부하고 상세한 QoS 지원
보안성	외부 위협으로부터 라우터들을 완벽하게 보호하기 위해 일련의 최첨단 메커니즘 제공 라우터는 네트워크 직원이 간단히 몇 단계를 거쳐 새로운 필터와 정책들을 언제든지 추가할 수 있는 콘솔 포트를 이용해 공격을 당하고 있는 동안에도 완벽한 통제력 유지
탁월한 업타임	운영체제의 모듈형 장애 방지 소프트웨어 설계는 J-series 라우터에서 높은 수준의 복원력과 안정성 발휘 일부 소형 버그가 더 큰 문제로 확산될 수 있었던 기존 라우터들과는 달리, JUNOS 운영체제 내 각 소프트웨어 모듈은 독립적으로 실행되기 때문에 다른 영역에 영향을 주지 않음 복원 기능으로는 정확한 구성을 위한 차세대 CLI와 신속한 시스템 복구를 위한 rescue 버튼 제공
예측 가능한 성능	J-series 라우터는 네트워크 혼잡으로 성능 요구치가 가장 높아지는 동안에도 높은 수준의 QoS 제어와 처리 성능 유지 모듈형 소프트웨어 아키텍처는 트래픽의 정렬 및 스케줄링을 위한 필수 요소로서, 가장 중요한 애플리케이션이 네트워킹 자원에 대한 가장 높은 우선순위를 확보할 수 있도록 지원
탁월한 가치	라이센스 비용에 대한 부담 없이 IPv6, MPLS, IPSec 및 stateful 방화벽 등과 같은 고급 서비스를 활용할 수 있으며, 포트 라이센스 없이 온보드 또는 모듈식 인터페이스 실행
안정적인 라우팅 서비스	공격을 받는 중에도 모든 라우터 제어를 보장하기 위하여 시스템 자원을 비축: DoS(Denial of Service) 공격 등 Control Plane을 위한 Stateful Firewall, Rate limit Protection 제공 공격중에도 동적인 공격 필터 추가/변경 기능 제공 라우팅 엔진과 전송 엔진 분리 구성으로 잦은 프로토콜 변동(Flapping 현상)으로 인한 라우팅 엔진 과부하 상태에서도 손실없는 트래픽 전송 서비스 제공
독립적인 OS 모듈로 높은 신뢰성 제공	각 모듈 프로세스는 모듈당 보호된 메모리를 가지며, 모듈간 메모리 공유를 하지 않음 하나의 모듈 장애시에도 전체 시스템에는 영향을 주지 않음 모듈간 독립적인 리부팅 기능 제공

<표 Ⅱ-8> L2 스위치

구 분	상 세 내 역
고 가용성	802.1d/1w/1s 지원 Fast Forwarding 지원 802.ad link aggregation 지원 브로드캐스트 트래픽 제어 RPS 지원 Fault Tolerant loop stack 지원
VLAN 지원	255 VLAN 4094 802.1q VLAN 지원 Port based, 802.1q, MAC based, IP subnet based, protocol based VLAN 지원 VLAN Stacking 지원
QoS 기능	802.1p, TOS, DSCP 마킹 지원 QOS 매핑: 802.1p to TOS/DSCP, TOS to 802.1p/DSCP, DSCP to 802.1p/TOS 분류 기능: port, 802.1p(COS) value, MAC SA/DA, Ethertype, TOS Precedence, DSCP value, ICMP code/type, IP SA/DA, IP Protocol, TCP/UDP port 포트당 4개의 egress 큐 Strict/WRR 알고리즘 Rate Limiting 지원
보안 기능	802.1x 지원 802.1x multi-client, multi0vlan 지원 Guest vlan 지원 MAC address lockdown 지원 RADIUS/TACACS+ 및 SSL, SSH, SNMPv3지원 ACL 기능 : Port, MAC SA/DA, IP SA/DA, ICMP type/code, Ethertype, TCP/UDP port STP root guard 방지

표준 작성 공헌자

표준 번호 : SSF-ST-T-0009

이 표준의 제·개정 및 발간을 위하여 아래와 같이 여러분들이 공헌하였습니다.

구분	성명	위원회직위	연락처	소속
과제 제안	류동주	분과위원장	ryu@infosec.co.kr	(주)정보보호기술
표준초안제출	류동주	분과위원장	ryu@infosec.co.kr	(주)정보보호기술
표준초안작성	류동주	분과위원장	ryu@infosec.co.kr	(주)정보보호기술
	강장묵	분과위원	mooknc@gmail.com	동국대학교
	장종수	분과위원	jsjang@etri.re.kr	전자통신연구원
	김정욱	과제책임자	jukim@smu.ac.kr	상명대학교
	최연석	자문위원	changwah@hoseo.edu	호서대학교
	김학준	자문위원	kimhj@mail.howon.ac.kr	호원대학교
	송재형	참여연구원	jhsong@smu.ac.kr	상명대학교
	박재화	참여연구원	parkjwha@gmail.com	상명대학교
	채운용	참여연구원	wycheah@hanmail.net	상명대학교
	정호석	참여연구원	jhshopi@empas.com	상명대학교
	김 활	참여연구원	hwalkim@paran.com	상명대학교
	박종만	참여연구원	ap5364@naver.com	상명대학교
	김미나	참여연구원	kmina070707@gmail.com	상명대학교
	홍영상	참여연구원	mineequalurs@naver.com	홍익대학교
	김서영	참여연구원	rlatjdud56@naver.com	상명대학교
	이윤아	참여연구원	yalee92@naver.com	상명대학교
표준안 심의	김은형	교수	ehkim1@gachon.ac.kr	경원대학교
	이정우	교수	jlee@yonsei.ac.kr	연세대학교
	백송훈	부장	baiksh01@paran.com	KT
	김정훈	교수	junghkim@ynu.ac.kr	영남대학교
	송지성	총괄	jissong@lgcns.com	LG-CNS
	류동주	팀장	ryu@infosec.co.kr	정보보호기술
	홍상기	교수	skhong@anyang.ac.kr	안양대학교
	정용규	교수	ygjung@eulji.ac.kr	을지대학교
	김정욱	교수	jukim@smu.ac.kr	상명대학교
사무국	권준철	사무국	jckwon65@paran.com	스마트도시협회
	최지원	사무국	hklee@smartcity.or.kr	스마트도시협회
	여화진	사무국	hjyeo@smartcity.or.kr	스마트도시협회

스마트도시표준화포럼표준

스마트시티 내에서 보안 영역 표준
(Security Domain in the Smart City)

발행인 : 이우종
발행처 : 스마트도시표준화포럼
08506, 서울특별시 금천구 가산디지털2로 98 롯데IT캐슬 1동 911호
Tel : 02-3667-5005, Fax : 02-3667-5511
발행일 : 2013. 1. 18.