Open Networking Korea (ONK) 2016 Fall

SDN 기반 동적 네트워크 은닉 핵심 기술 개발

2016. 11. 25.

고 남 석 실장

신뢰네트워킹연구실
한국전자통신연구원

KAIST Atto Research NAIM networks LANBIRD

목 차

1. 과제 개요

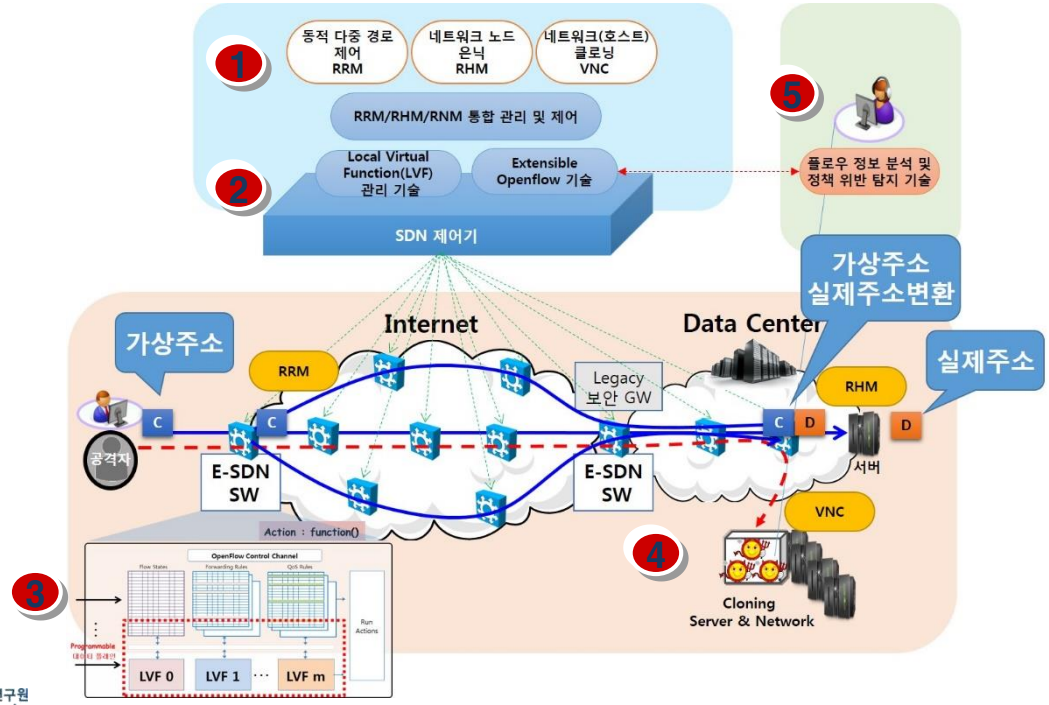
기술 정의 및 개념

기술 정의

SDN 기반으로 **네트워크 구성을 동적으로 변경하여** 악의적 사용자의 공격에 대한 **예측불가능성(Unpredictability), 불확정성(Uncertainty) 및 비용(Cost)**을 증가시켜 취약점 노출을 어렵게 만드는 **네트워크 보호 기술**

핵심 기술

- **RRM** : 라우팅 경로의 동적 변경으로 네트워크를 보호하는 기술
- **RHM** : Host의 IP 주소/Port 동적 변경으로 네트워크를 은닉하는 기술
- **VNC** : 유해/의심 트래픽을 유인하여 분석 · 탐지하는 가상 네트워크 기술
- **E-SDN 스위치** : 데이터 플레인의 Programmability가 가능한 고성능 SDN 스위치 기술



<SDN 기반 네트워크 은닉 개념도>

최종 산출물

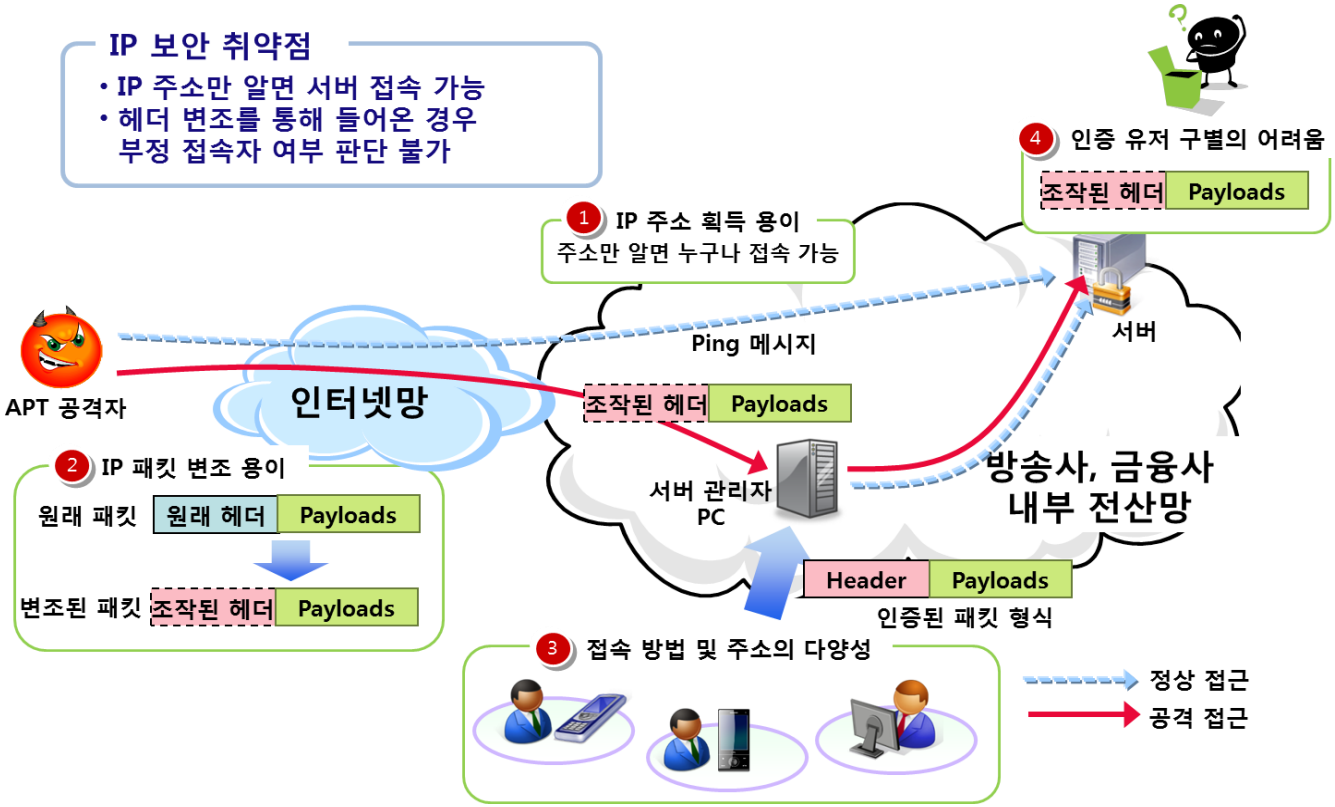
1. RRM, RHM, VNC 응용(SW)
2. SDN 제어기(SW)
3. SDN 스위치(HW+SW)
4. 클로닝 서버(HW+SW)
5. 정책위반 탐지 및 추적(SW)

RRM : Random Route Mutation
RHM : Random Host Mutation
VNC : Virtual Network Cloning
E-SDN : Extensible SDN
LVF : Local Virtual Function

1. 과제 개요

현황 및 문제점

- 1.25 인터넷 대란, 7.7 DDoS 사태에 이어, 3.20 방송·금융 전산망 마비 사태 등 **인터넷 경제 인프라에 대한 심각한 위기 지속적 증가**
- 인터넷 인프라의 가장 큰 문제는 **인터넷 기술의 개방성**!
  - 경계 기반 기존 네트워크 보안 체계 한계 직면
  - 네트워크 기술 기반 변혁적인 R&D 필요



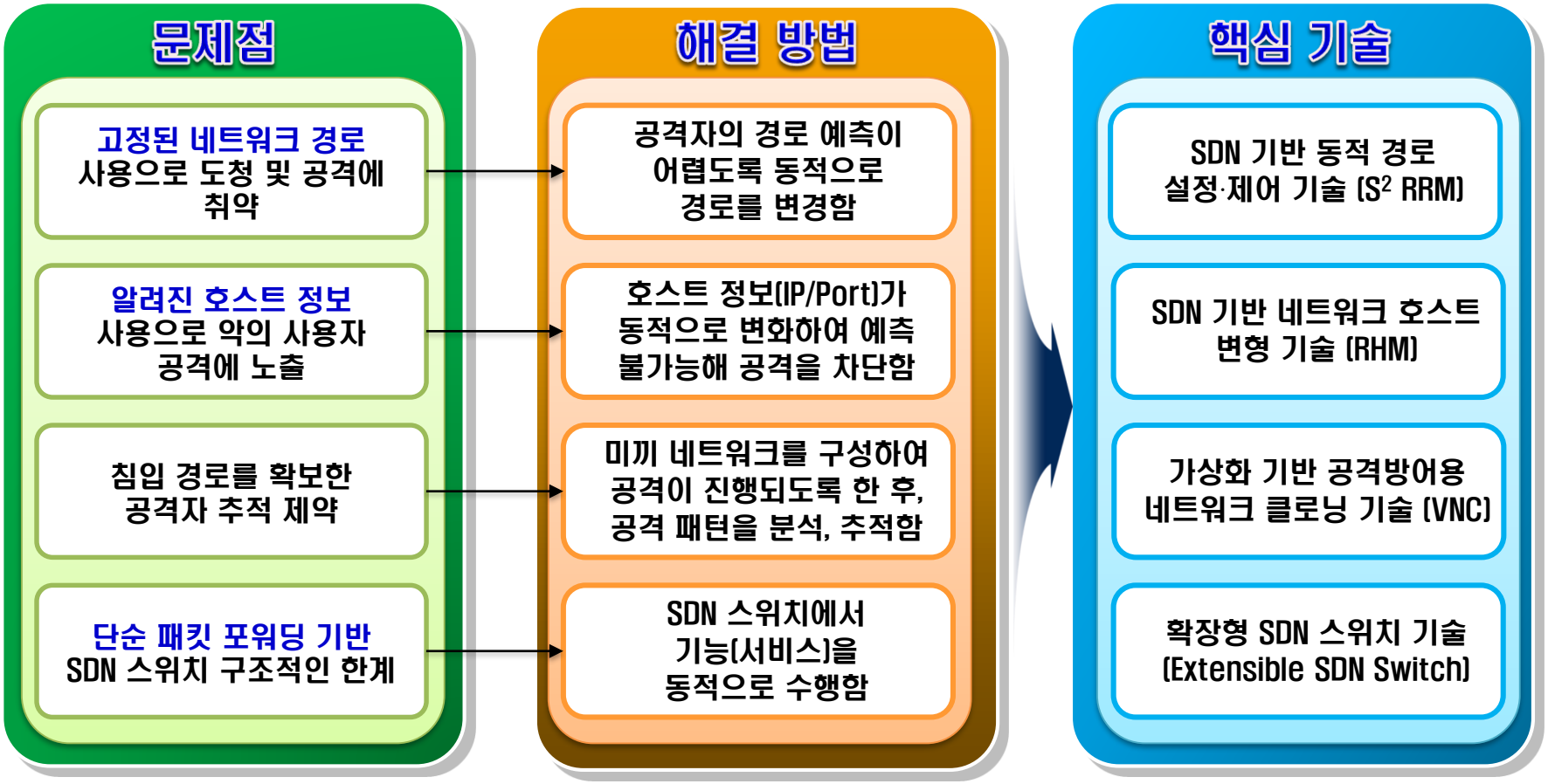
1. 과제 개요

목표 및 핵심 기술 도출

비전 및 목표

비전 : 사이버 위협을 야기하는 현 인터넷 구조의 기술적 결함을 해결하여 **신뢰성 있는 네트워크 구축**

목표 : SDN 기반 동적 네트워크 은닉 원천기술 확보 및 시작품 완성(TRL6)



S² RRM : Secure & Survivable RRM, RHM : Random Host Mutation, VNC : Virtual Network Cloning

1. 과제 개요

정량적 목표

평가 항목 (주요 성능 Spec.)	단위	비중 (%)	개발 목표치			평가 방법
① 경로 변경 설정 시간	msec	10	200	100	20	공인시험 성적(확인)서
② 반응 경로 계산 시간	msec	20	1000	500	100	공인시험 성적(확인)서
③ 서버 정보 변경 파라미터 수	수	20		1 (IP)	2 (IP, Port)	공인시험 성적(확인)서
④ 가상 네트워크 유인 방법	제어 방법	20			네트워크 기반	공인시험 성적(확인)서
⑤ 확장형 SDN 스위치 포워딩 성능	Gbps	30		100	200	공인시험 성적(확인)서

① 경로 변경 설정 시간

→ SDN 제어기의 RRM 모듈에서 경로 변경을 설정하는 메시지가 SDN 스위치에 전달되어 플로우 테이블의 해당 엔트리가 변경되는데 걸리는 시간

② 반응 경로 계산 시간

→ SDN 스위치로부터 발생된 네트워크 이벤트(경로 단절 등) 메시지가 SDN 제어기에 전달된 시점으로부터 네트워크 이벤트에 반응하여 계산한 새로운 경로를 반영하는 플로우 제어 메시지를 SDN 스위치로 출력하는데 걸리는 시간

③ 서버 정보 변경 파라미터 수

→ 서버를 보호하기 위한 정보 변경 갯수 (IP 주소, 포트 번호 등)

④ 네트워크 기반의 가상 네트워크 유인 방법

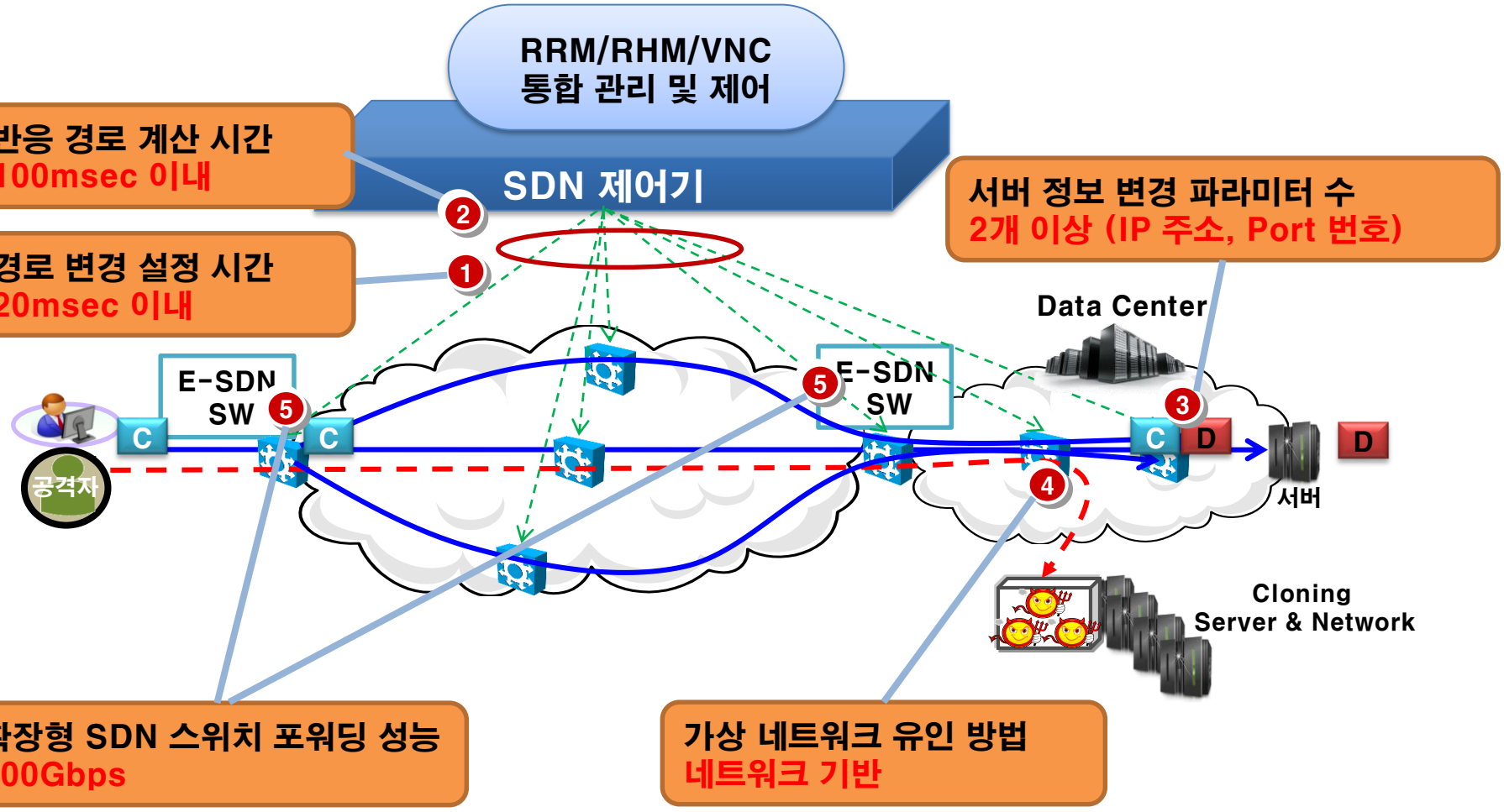
→ 탐지된 공격자를 유인용 가상네트워크로 유인하기 위한 방법을 의미함

⑤ 확장형 SDN 스위치 포워딩 성능

→ 기존 OpenFlow 프로토콜을 확장하여 새로운 기능을 수용할 수 있도록 확장된 SDN 스위치의 기본 패킷 포워딩에 대한 성능을 의미함

1. 과제 개요

정량적 목표


RRM/RHM/VNC
통합 관리 및 제어
SDN 제어기
반응 경로 계산 시간
100msec 이내
경로 변경 설정 시간
20msec 이내
서버 정보 변경 파라미터 수
2개 이상 (IP 주소, Port 번호)
Data Center
E-SDN SW
E-SDN SW
C
C
C
D
D
공격자
서버
Cloning
Server & Network
확장형 SDN 스위치 포워딩 성능
200Gbps
가상 네트워크 유인 방법
네트워크 기반

목 차

2-1. 연구 개발 일정

전체 추진 일정

순번	분야	개발 내용	1차년도				2차년도				3차년도			
			1	2	3	4	1	2	3	4	1	2	3	4
1	SDN 기반 네트워크 은닉 프레임워크	SDN 기반 네트워크 은닉 프레임워크 구조 설계	요구사항 정의/프레임워크 공동 설계											
		동적 네트워크 생존성 강화를 위한 구조 연구												
2	동적 다중 통신 경로 설정·제어(RRM) 기술	고확장성 Proactive RRM 구조 설계 및 개발	RRM 구조 설계/알고리즘 개발											
		Reactive RRM 설계 및 알고리즘 개발					Reactive RRM 설계/알고리즘 개발							
		고확장성&고생존성 RRM 알고리즘 최적화									RRM 알고리즘 최적화			
3	네트워크 노드 변형 (RHM) 기술	RHM 구조 연구 및 설계	RHM 구조 설계/알고리즘 개발											
		고속 RHM 기술 개발					가상 IP/Port 할당 알고리즘 및 관리 기술 개발							
		고속 RHM 기술 개발									가상 IP/Port 할당 성능 개선			
4	공격방어용 네트워크 클로닝 (VNC) 기술	VNC 시나리오 연구 및 구조 설계	VNC 구조/SDN 연동구조 설계											
		서버 클로닝 기반 VNC 기술 개발					서버 클로닝 기반 VNC 기술개발 / 네트워크 클로닝 기반 VNC 설계							
		네트워크 클로닝 기반 VNC 기술 개발 및 연동									VNC 기술 개발/성능 검증			
5	네트워크 은닉을 위한 SDN 기술	SDN 기반 제어 구조 설계 및 개발	RRM/RHM/VNC 연동구조 설계											
		SDN 기반 제어 서비스 개발					RHM 제어 기능/VF 관리 기능 개발							
		SDN 기반 제어 서비스 연동									RRM/RHM/VNC 통합제어/연동			
		정책위반 탐지 및 추적 기술 개발							정책 위반 탐지 기술 개발		정책 위반 추적/탐지 기술 연동			
6	Extensible SDN 스위치 기술	Extensible SDN 스위치 구조 설계 및 개발	E-SDN 프로토콜/스위치 패킷 포워딩 기본 기능 개발											
		Extensible SDN 스위치 기능 개발					실험 시제품 개발/LVF 기능 및 연동 기본 기능 개발							
		Extensible SDN 스위치 기능 연동 및 시제품 개발									시험 시제품/LVF 기능 및 제어기 연동 안정화			
7	SDN 기반 동적 네트워크 시스템 통합 및 성능 개선	기능 시험			기능 시험									
		기능 연동 및 시험							1차 연동					
		시스템 연동 및 시험												2차 연동

2-2. 핵심기술 – RRM 기술

기술 개념

고정 경로

- 고정 경로 사용으로 도청 및 공격 용이
- 감지된 공격에 따른 경로 변화 불가능
- Dynamic routing을 사용하면 경로는 바뀌나 예측이 쉬움

RRM 기술
Random Route Mutation

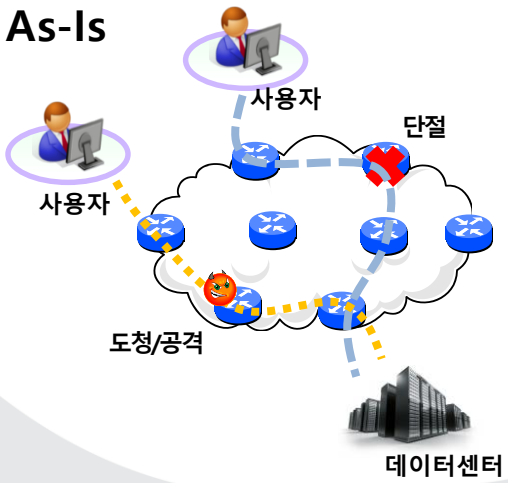
네트워크 경로를 주기적으로 변경하여 공격에 대응하는 동적 경로 설정 제어 기술

동적 경로 설정 제어 기술

- 플로우별 동적 경로 사용으로 **도청 및 공격 지점 선택이 어려움**
- 공격 감지시 경로 재설정 가능 (반응성)
- 공격을 고려한 **예측이 어려운 경로 설정**

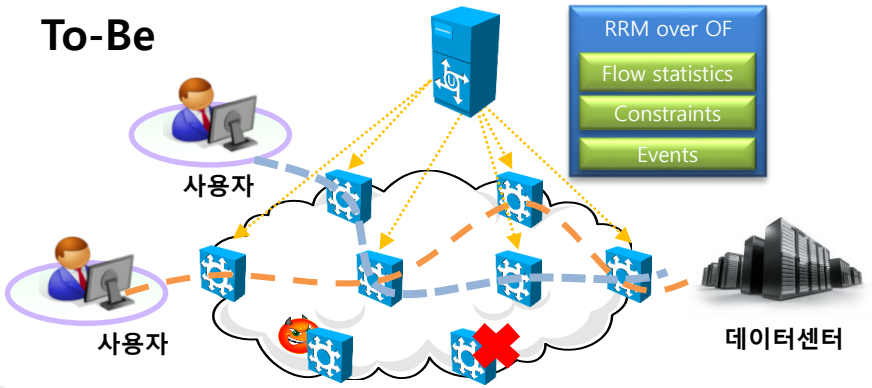
고정 경로 사용으로 도청 및 공격 용이

As-Is



경로의 주기적 변경을 통한 공격 대응

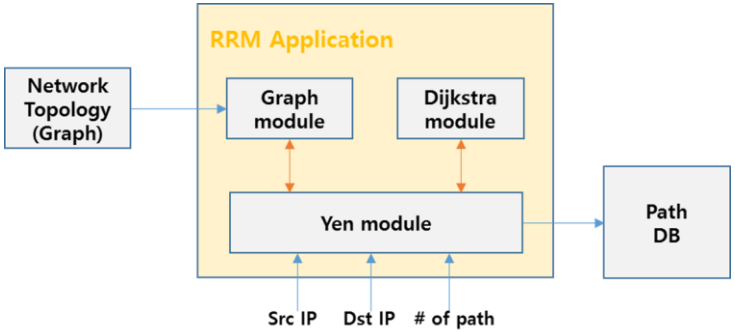
To-Be



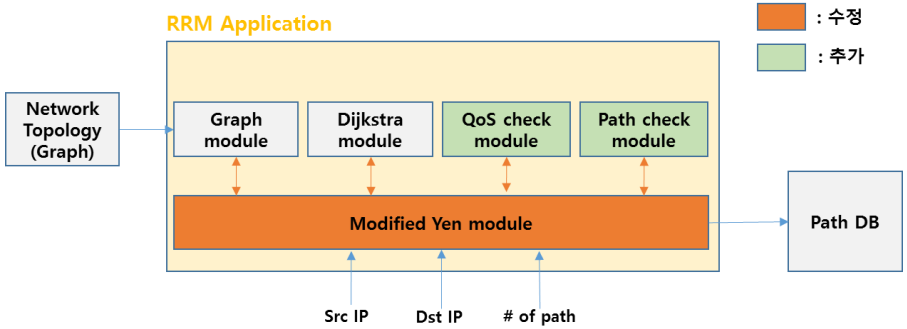
- 플로우별 동적 경로 설정으로 도청 및 공격 방어
- 네트워크 단절 및 공격에 대응하기 위한 반응형/적응형 경로 재설정 가능
- 공격 감지시 경로 재설정으로 도청 및 공격 무력화

Proactive RRM 기술

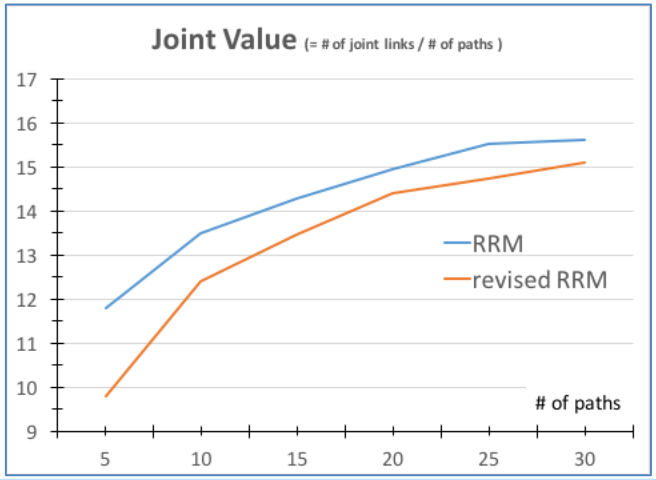
- Path 중복성 제어 모듈 (Path-check): 경로 간 중복성 최소화
  → 예측 난이도 증가 위한 중복 방지 K-shortest path 알고리즘 개발
- QoS 보장 제어 모듈 (QoS-check) : QoS 보장 경로 만족 여부 확인



<1차년도>



<2차년도>

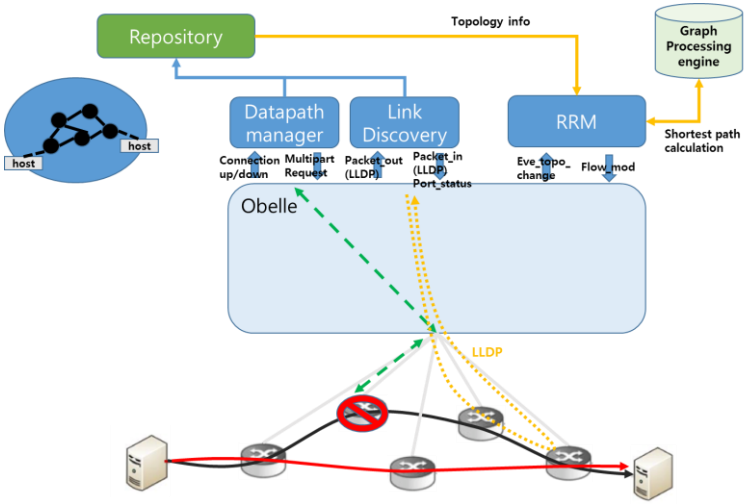


Simulation Environments:
Intel(R) Core(TM) i5-3470 3.20GHz, 1-core, 64bit,
Memory 4Gb (VM환경)
Mesh Topology : 10 x 10

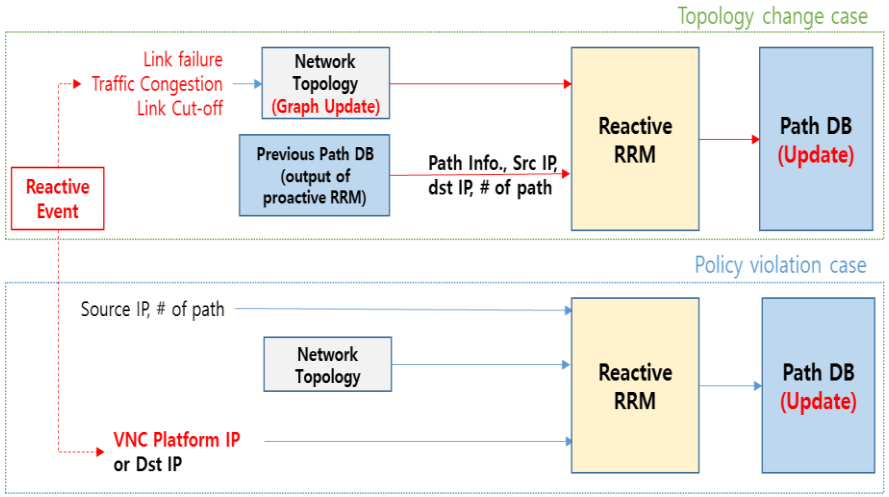
10x10 mesh(k=5) 결과:
경로 중복율 17% 경감 (중복 경로 59개 ➔ 49개)

고생존성(Reliable) Reactive RRM 기술

- Reactive RRM 기술
  - → 네트워크 장애시 경로 풀 재생성을 통한 경로 복구 기능
    - * Link failure/Port down/Switch Off
  - → 정책위반시 VNC Platform으로 경로 우회 기능
  - → 공격탐지 시 해당 Port/Switch를 제외한 경로 생성 기능
- RRM 기술 구현 및 시험
  - → OBelle 컨트롤러용 RRM 응용 및 관리 기능 구현 완료
  - → R&D 시험 검증 사업과 연계한 RRM 기능 및 성능 시험 예정



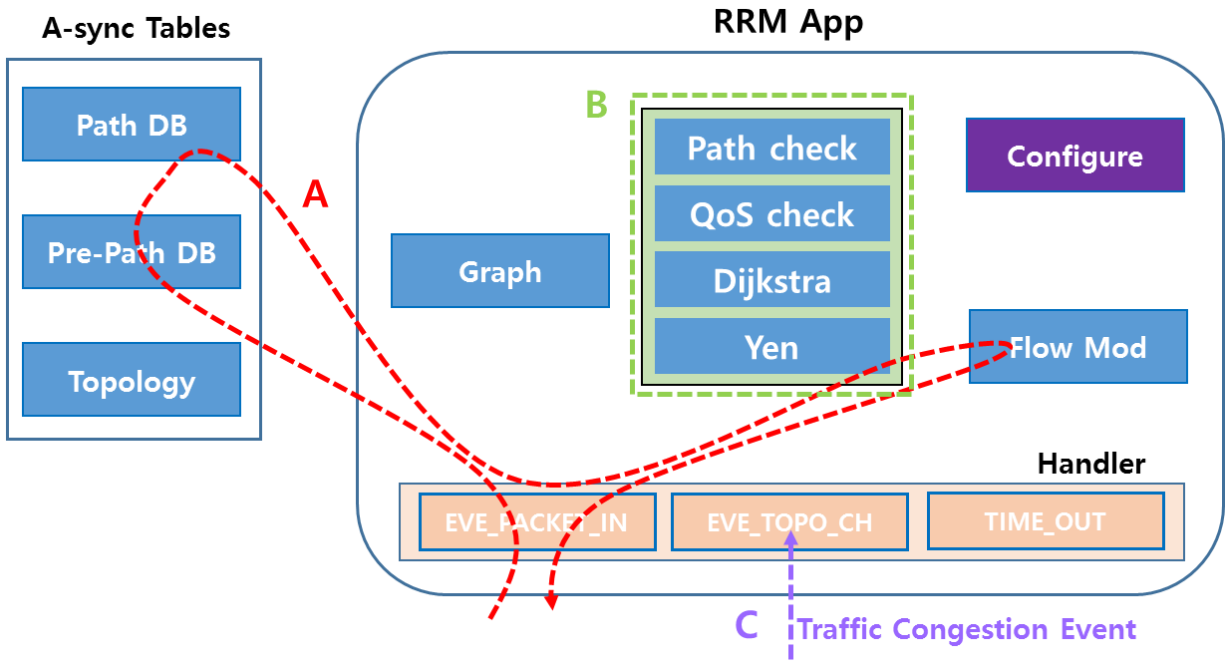
<고생존성 Reactive RRM 구조>



<고생존성 Reactive RRM 동작 >

3차년도 계획

- RRM 성능 최적화
  - → 사전 경로 탐색 및 Pre-Path DB 기능 추가를 통한 경로 설정 시간 단축 (A)
  - → 알고리즘 최적화를 통한 경로 계산 시간 단축 (B)
  - → Reactive Event 추가(실시간 Network Traffic 반영)를 통한 고생존성 강화 (C)



< RRM 성능 최적화 시스템 모델 >

2-3. 핵심기술 – RHM 기술

개발 현황

고정 호스트 주소

- 노출된 고정 서버 IP 주소 사용
- 스캐닝을 통해 쉽게 공격 대상에 노출
- 사후 탐지, 수동적 방어 중심의 이상 트래픽 방지 기술

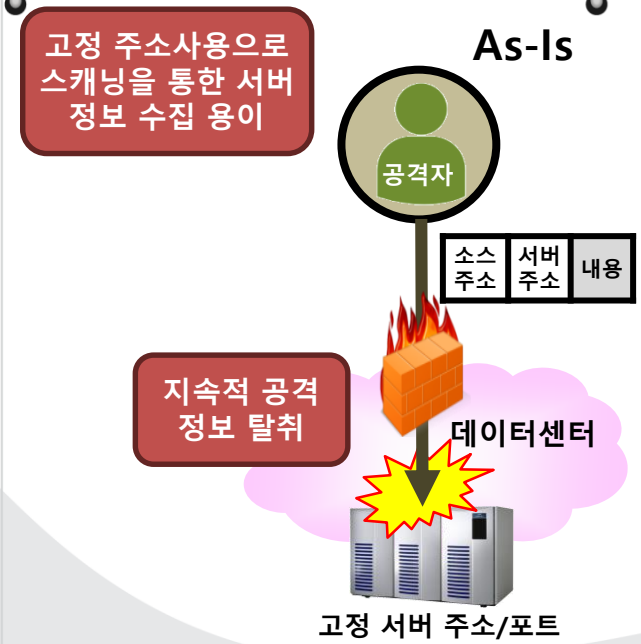
RHM 기술
Random Host Mutation

네트워크 호스트 정보를 변경하여 스캐닝 공격에 대응하는 기술

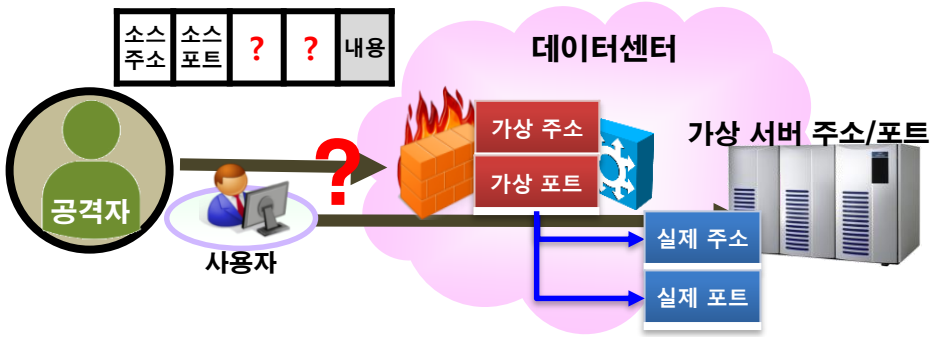
가변 호스트 주소

- 호스트 정보 변경으로 스캐닝 공격 방어
- 주기적 변경으로 지속적인 특정 주소 접근 차단
- SDN을 통하여 동적으로 변경하는 호스트 정보를 신속하게 네트워크에 적용

As-Is



To-Be

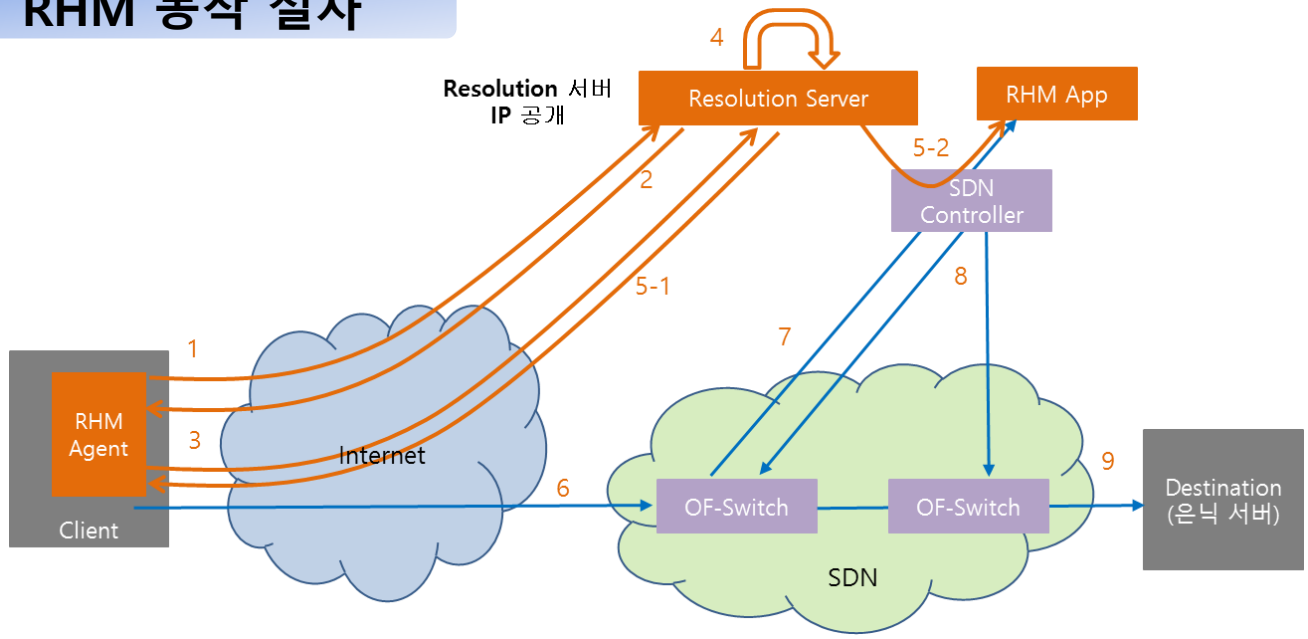


- 가변 주소 사용으로 스캐닝을 통한 서버 정보 수집 어려움
- 서버의 주소를 동적으로 변경하여 지속적인 특정 주소 접근 차단

RHM 기술 개발

- Virtual IP 생성 알고리즘 개발
  - → RHM 응용(SDN 제어기 상의 응용으로 구동)의 Virtual IP 생성 기능 (클라이언트 Source IP, 목적지 Real IP, 시간 정보 기반)
- RHM 응용 및 클라이언트 에이전트 개발
  - → RHM 응용
    - ✓ IP 변환/검증 모듈 : 클라이언트의 요청에 따른 서버 Virtual IP를 Real IP로 변환 (Virtual IP 생성 알고리즘 탑재)
    - ✓ Virtual IP를 이용한 클라이언트 – 은닉 서버 간 은닉 경로 설정 (SDN 스위치 경로 제어)
  - → 클라이언트 에이전트
    - ✓ Virtual IP 요청 모듈 : 서버 URL/Real IP에 대응하는 Virtual IP 요청
    - ✓ IP 변환 모듈 : 패킷 헤더의 목적지 IP를 Virtual IP로 변환
- RHM 기술 구현 및 시험
  - → R&D 시험 검증 사업과 연계한 RRM 기능 및 성능 시험 예정

RHM 동작 절차

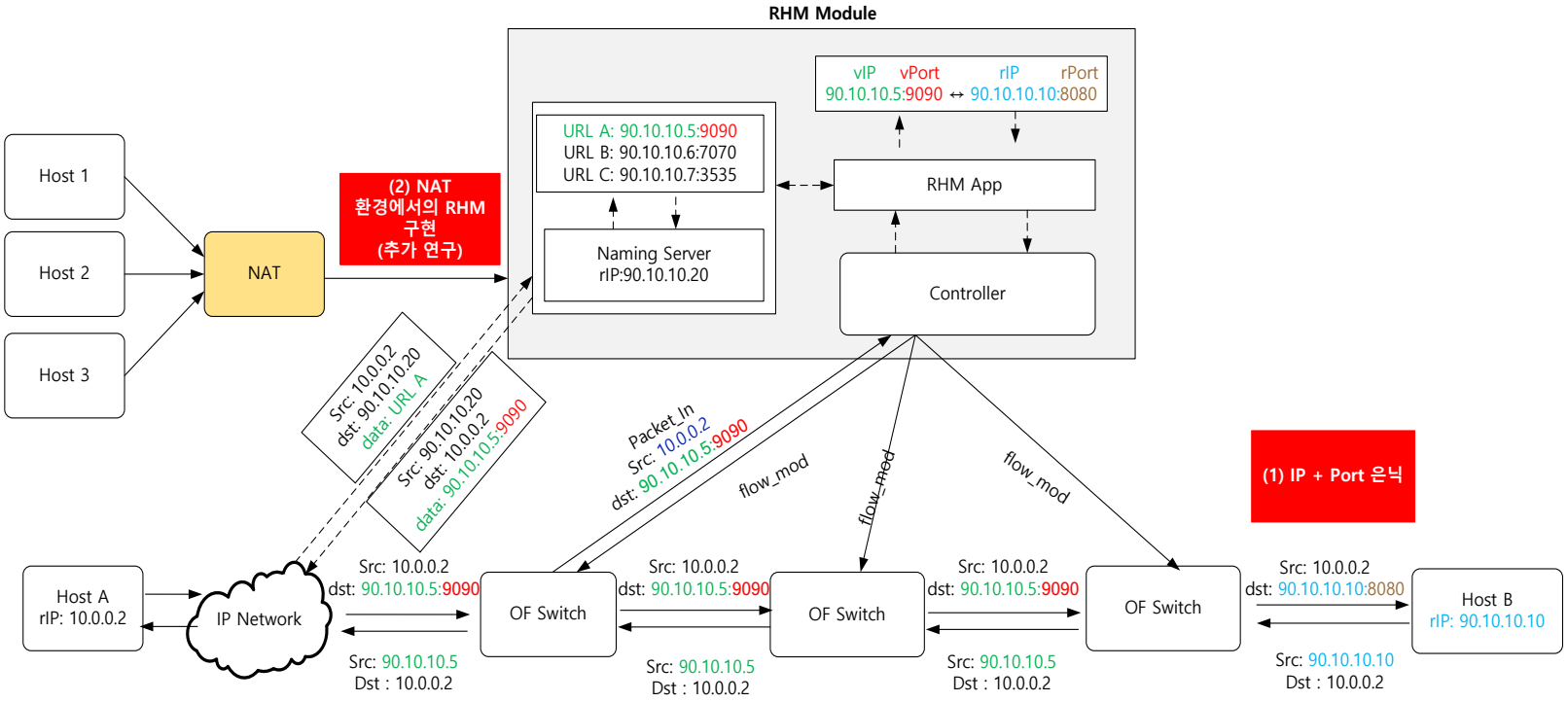


1. Client(Agent) → Resolution Server : 접속 가능한 사이트(URL, Etc.,) List 요청
2. Resolution Server → Client(Agent) : 사이트(URL, Etc.,) List 전달
3. Client(Agent) → Resolution Server : Client가 접속하기 원하는 사이트(URL, Etc.,) 선택(dst vIP 요청)
4. vIP 생성
5-1. Resolution Server → Client(Agent) : 해당 사이트(URL, Etc.,)에 대한 vIP를 전달
5-2. rIP-vIP mapping 정보 전달
6. 패킷 전달
7. packet_in 메시지를 보고 허용된 sIP/dst vIP인지 확인
8. 7번 만족시 경로 계산 및 flow_mod, set-field 메시지 전달
9. 목적지로 패킷 전달

< RHM 개념도 및 동작 절차 >

3차년도 계획

- 가상 IP/Port 할당 알고리즘 성능 개선
- Port 은닉 구현
- NAT 환경에서의 RHM 구현 (추가 연구)



2-4. 핵심기술 – VNC 기술

기술 개념

차단 기술

- 다양한 우회 공격 기술 존재
- 경계점 방어를 무력화 가능
- APT의 경우 특정 서버 및 사용자를 지속적으로 공격하여 방어가 어려움

VNC 기술
Virtual Network Cloning

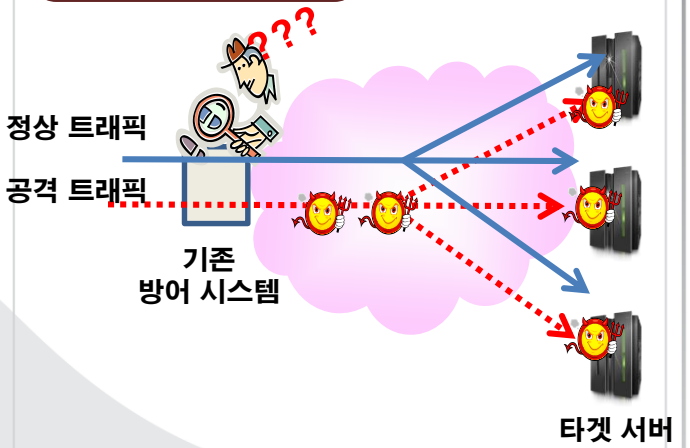
미끼 네트워크를 구성하여
공격자 유인을 통한 효과적
공격 탐지 및 추적환경 제공

기만 기술

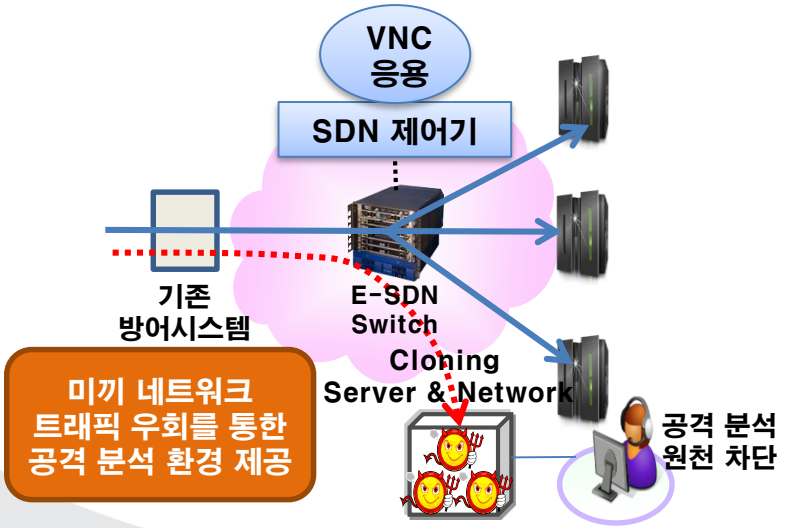
- 공격자 유인용 미끼 네트워크 구성
- 침입 트래픽 유인
- 공격 근원 차단을 위한 추적환경

As-Is

경계 기반 방어
APT 방어 능력 부재

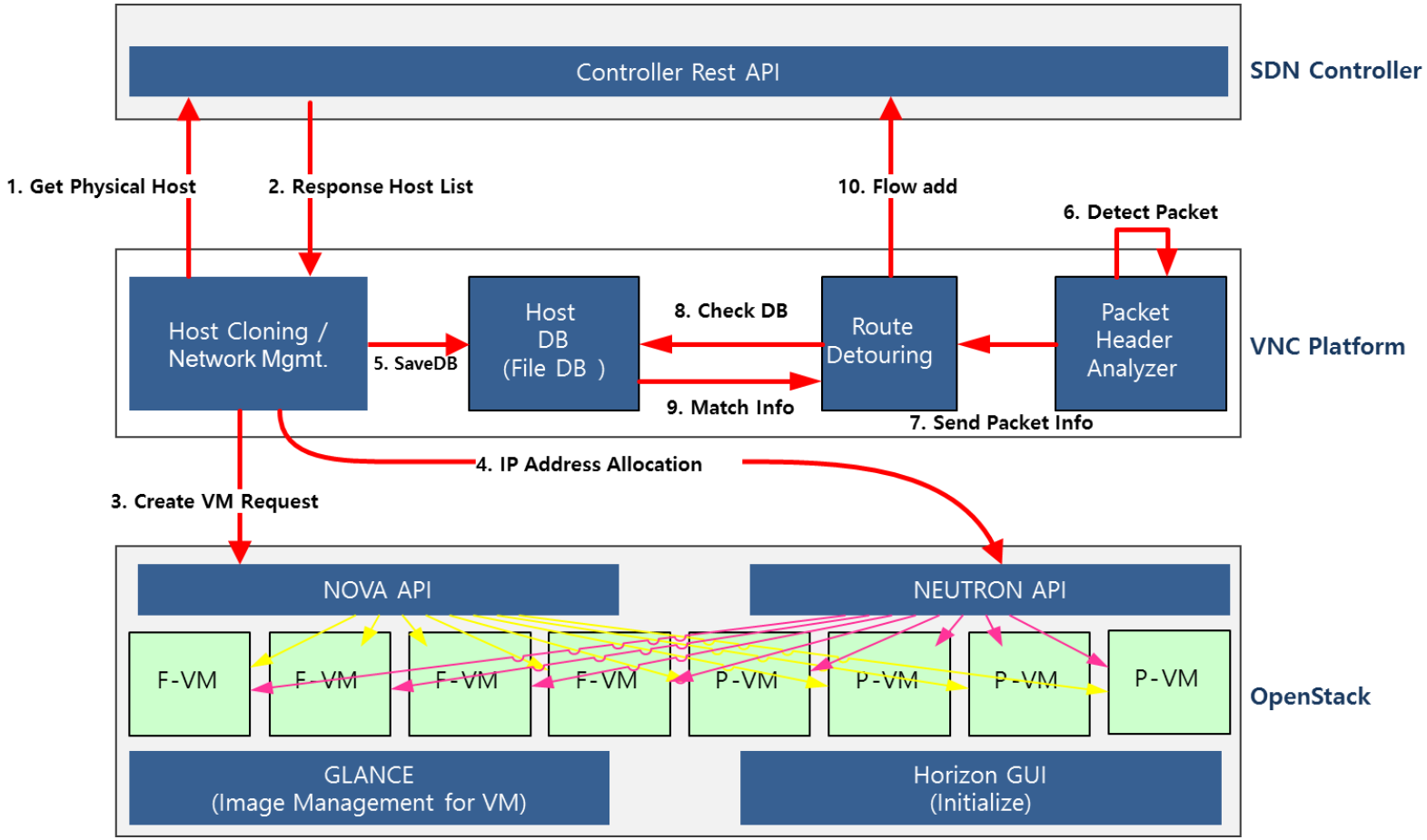


To-Be



미끼 네트워크
트래픽 우회를 통한
공격 분석 환경 제공

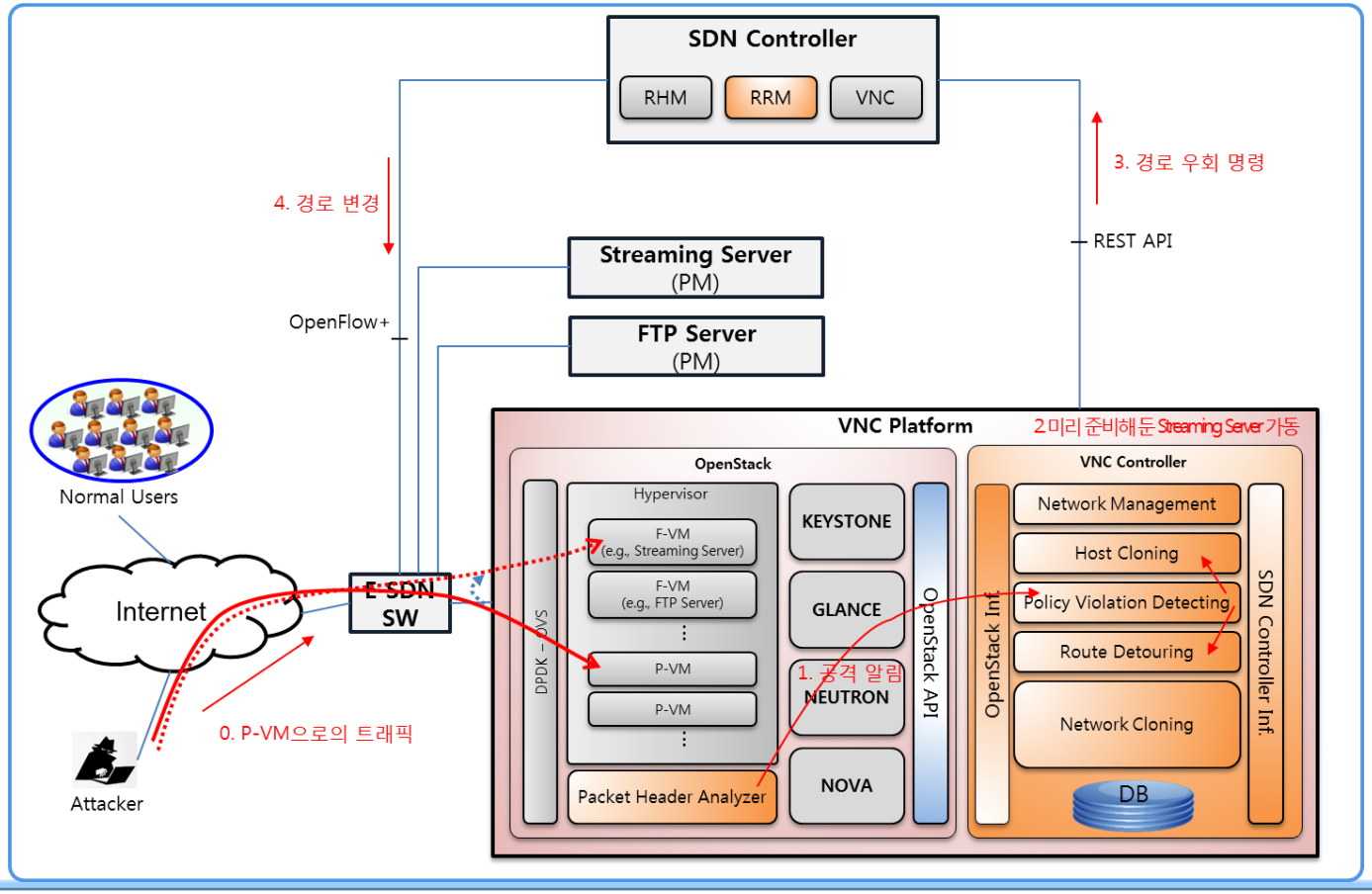
VNC 플랫폼 개념도



- **Host Cloning** : 공격에 따른 Host 복제 관리
- **Network Management**: 네트워크 토폴로지 정보 및 PM/VM IP 관리
- **Route Detouring**: 공격 탐지시 Host Cloning 및 경로 우회 관리
- **Packet Header Analyzer**: VM으로 인입되는 의심트래픽 탐지

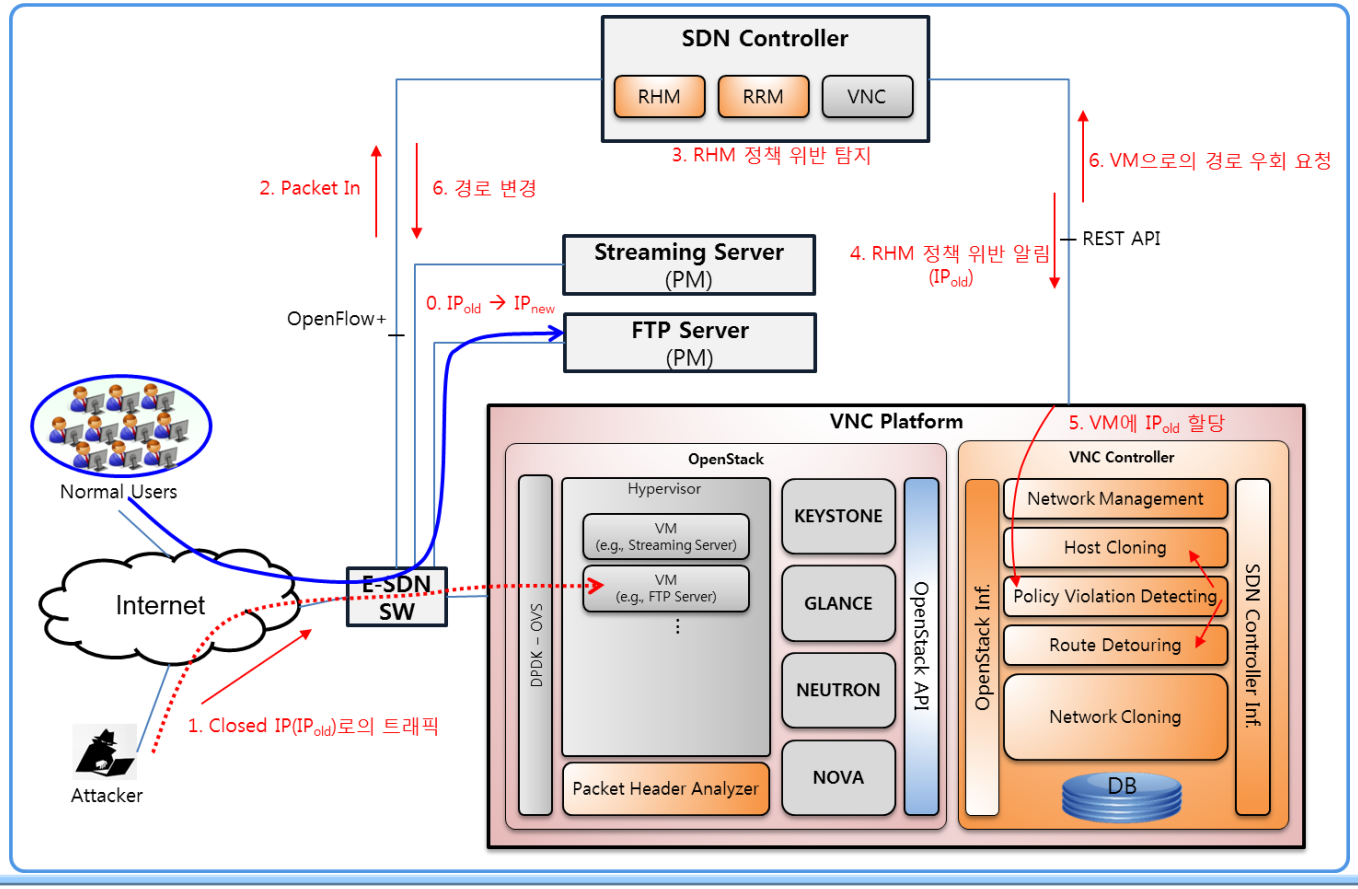
VNC 정책 위반 탐지 – RRM 연동 기술

- 가상 네트워크로 물리 네트워크를 은닉함으로써, 공격 목표 탐지 확률을 낮춤
- RRM 기술과 VNC 기술을 연동하여 공격 트래픽 우회



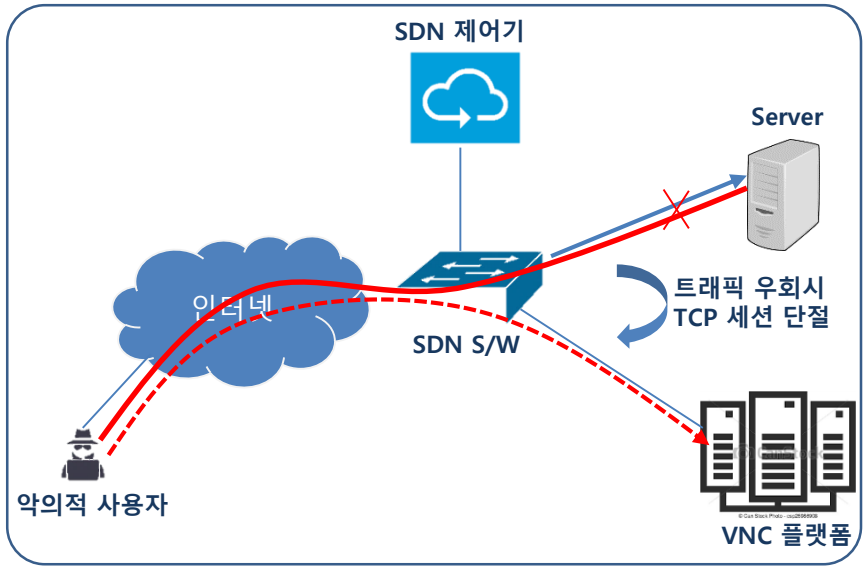
RHM 정책 위반 탐지 – VNC 연동 기술

- RHM 정책을 위반하여 유효하지 않는 서버 주소로 접근하는 클라이언트를 VM으로 우회시킴으로써 **APT와 같은 지속적 공격 사전 차단**
- RHM 기술과 VNC 기술을 연동함으로써 **DoS 공격 유효성을 낮춤**

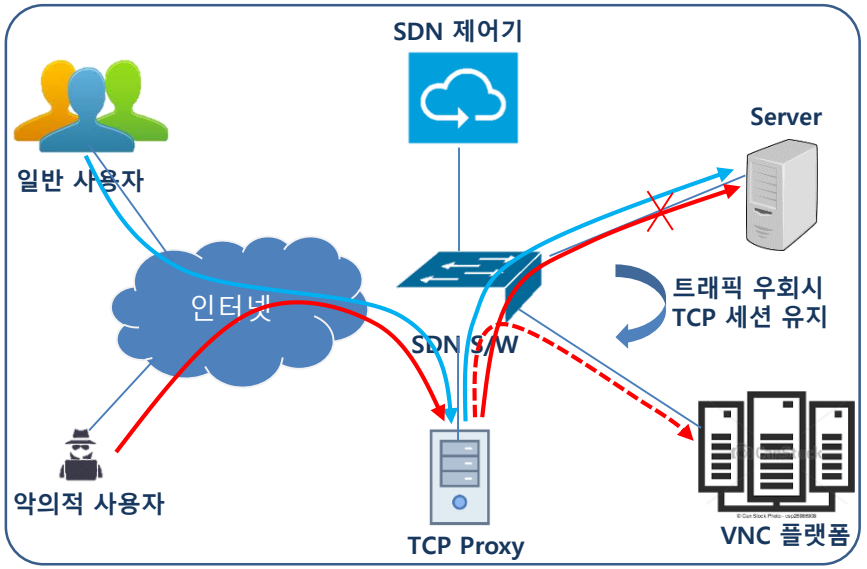


공격자의 VNC 인지 방지를 위한 TCP Proxy 기술

- 의심 트래픽 탐지에 따른 경로 우회 시 TCP 세션 단절로 공격 인지 가능
- 공격자가 인지할 수 없도록 **세션을 끊김없이 VNC 플랫폼으로 우회**
- DPDK 기반으로 **고속 패킷 처리 및 플로우 처리 유연성 확보**



< TCP Proxy 적용 전 >

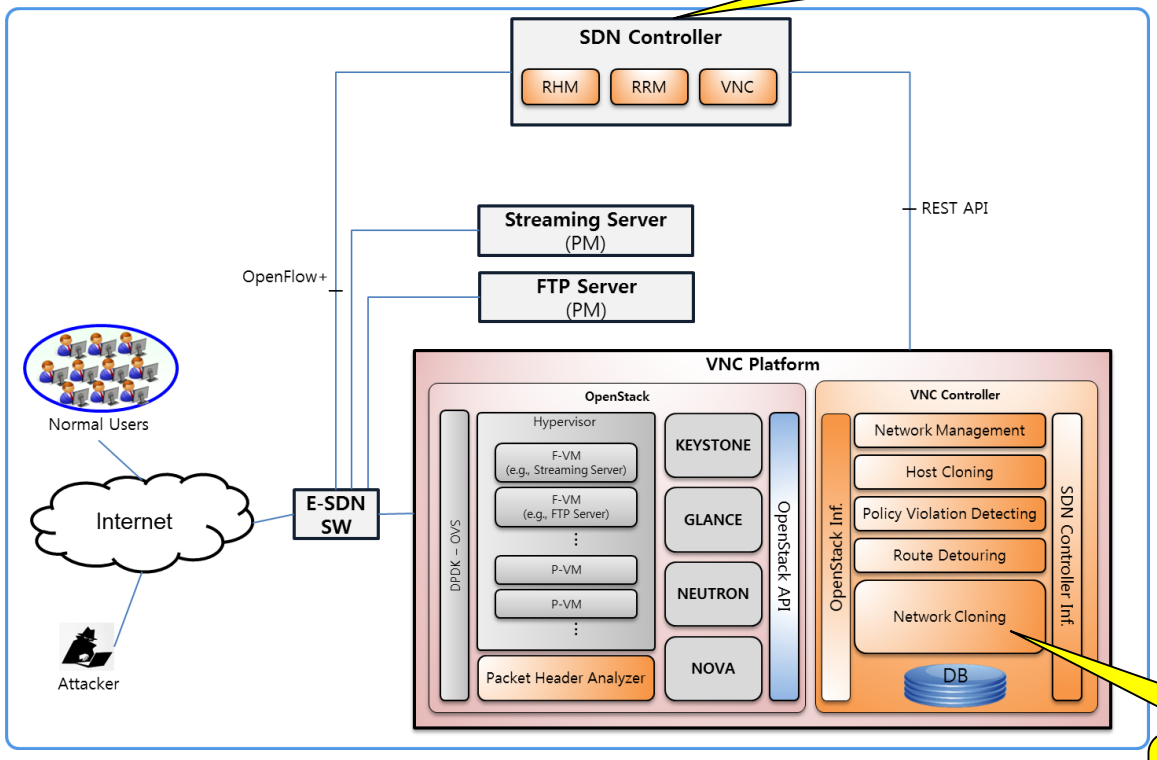


< TCP Proxy 적용 후 >

3차년도 계획

- 네트워크 클로닝 기반 VNC 기술 개발 및 연동
- SDN 기반 동적 네트워크 시스템 통합

SDN 기반 동적 네트워크 시스템 통합



네트워크 클로닝 기반 VNC 기술 개발 및 연동

2-5. 핵심기술 – E-SDN 기술

기술 개념

Legacy SDN

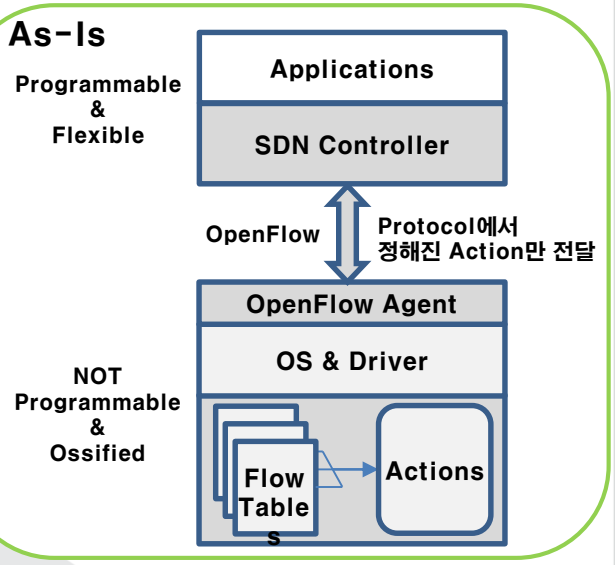
- 외부 장치에 의존적인 기능/서비스 처리 구조
  - 서비스 지연 및 성능 이슈
  - 신규 패킷 유형 수용 불가능

E-SDN 스위치 기술

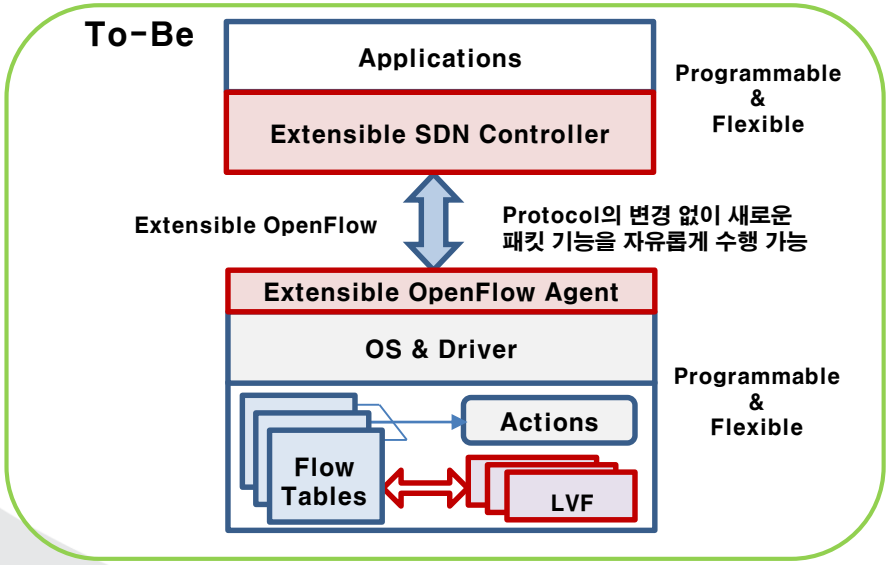
데이터 플레인 프로그래머빌리티 제공을 통한 소프트웨어 정의형 네트워킹 제공 기술

E-SDN

- 데이터플레인 프로그래머빌리티 제공
  - 스위치 내에서 기능(서비스)의 동적 수행 가능
  - 신규 패킷 유형 수용 가능



새로운 패킷 포맷 수용 불가능 &
외부 장치에 의존한 기능/서비스 수행

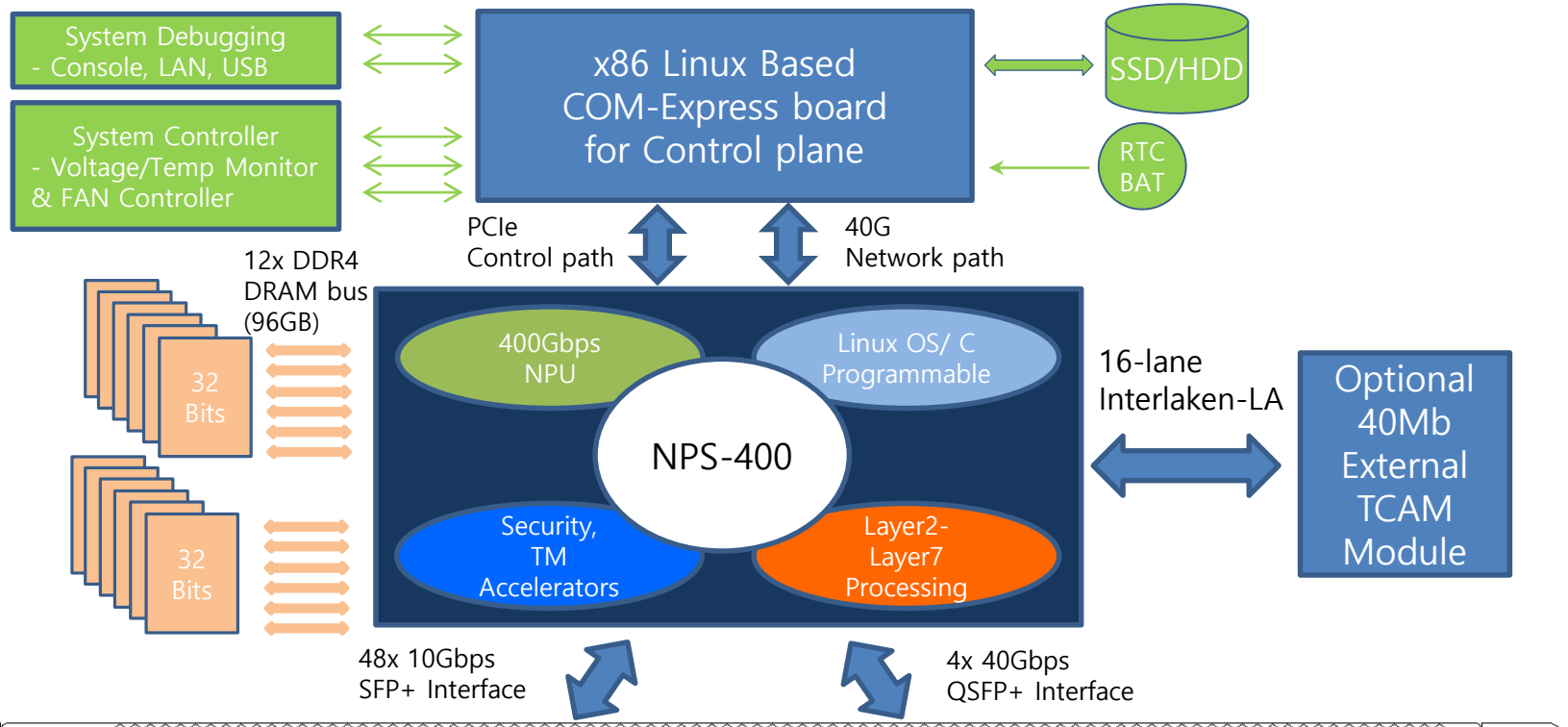


새로운 패킷 포맷 수용 가능 &
데이터 플레인에서의 동적 기능/서비스 수행 지원

LVF : Local Virtual Function

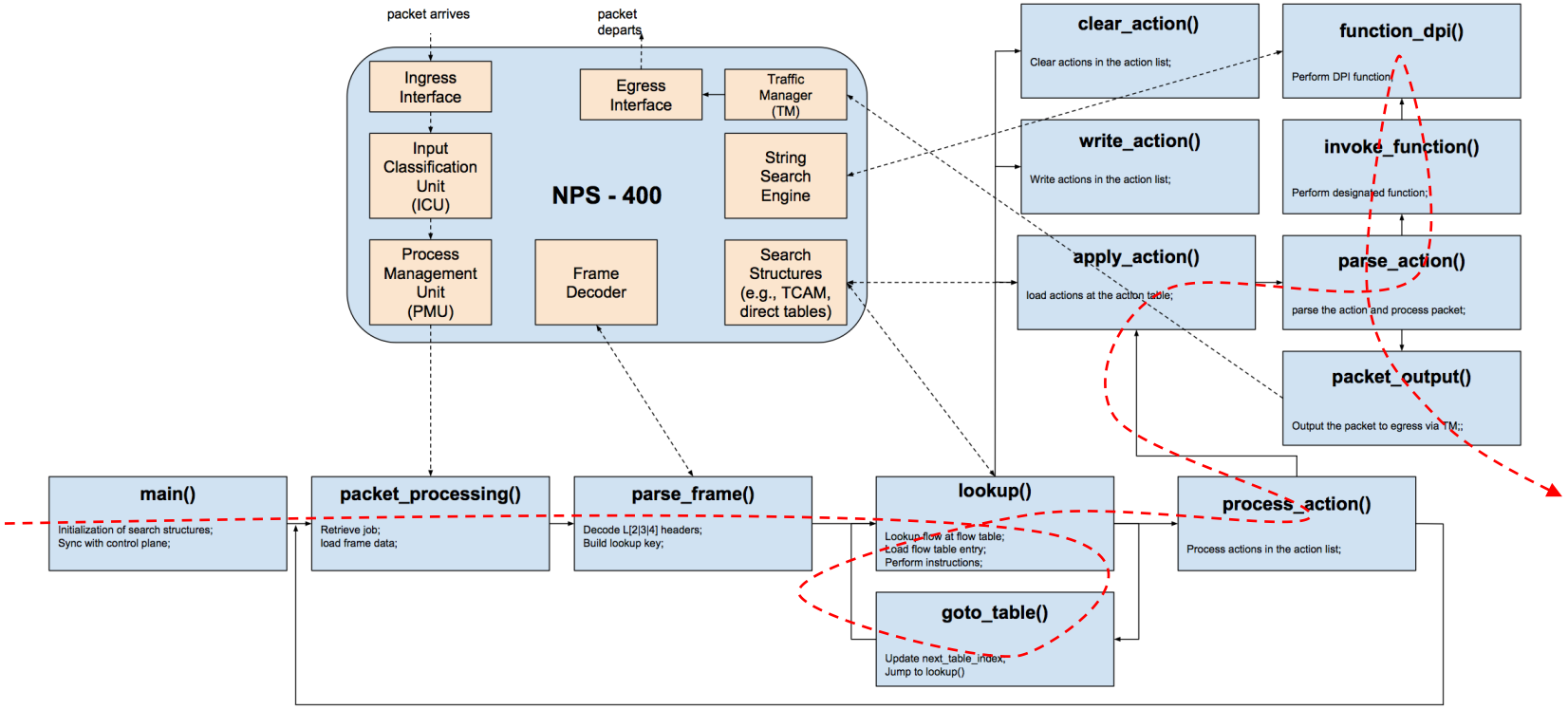
E-SDN 스위치 하드웨어

- **NPS-400 프로세서를 기반으로 한 고성능 확장형 SDN 스위치 하드웨어 플랫폼**
  - →**내/외장 TCAM, 암호화 엔진, H/W 트래픽 관리 기능을 통한 저지연 네트워크 및 보안 기능 처리**
  - →**고성능 40Gbps Data plane ↔ Control plane 채널을 통한 Scalable flow setup**



E-SDN 스위치 소프트웨어 - 데이터플레인

- 멀티 테이블 및 멀티 LDF을 지원하는 고성능 Run-to-completion Lock-free 구조
  - → Action을 통한 LDF 수행으로 임의의 테이블-LDF 체인 구성 가능
  - → NPS-400 PMU의 플로우 분배에 기반한 Lock-free 구조로 높은 성능 (2차년도:100Gbps) 실현
  - → TCAM, 스트링 검색, TM, Frame decoder 등 H/W affinity 활용을 통한 저지연 처리

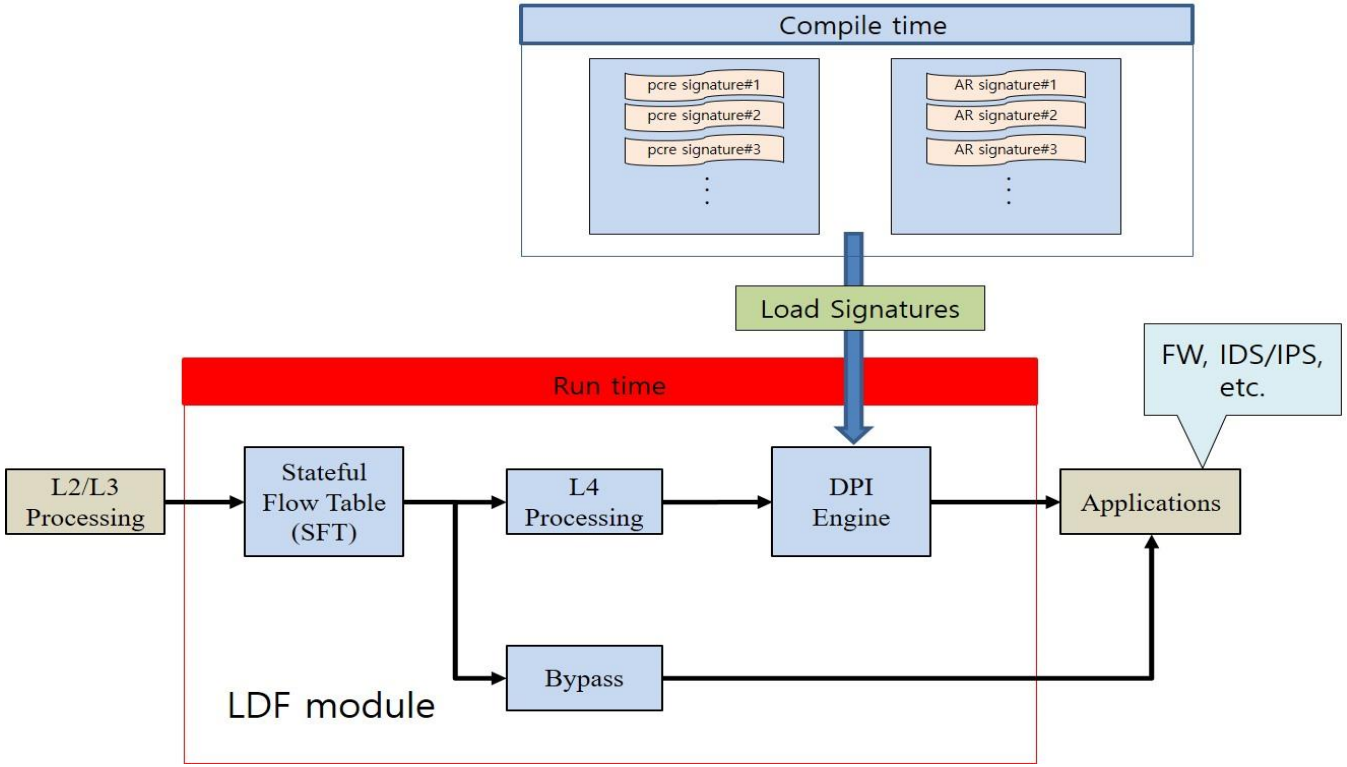


<E-SDN 스위치 데이터플레인 흐름 및 NPS-400 프로세서 기능 블록과의 관계>

LDF: Local Dataplane Function, PMU: Processor Management Unit, TM: Traffic manager

E-SDN 스위치 소프트웨어 – DPI LDF

- SFT와 DPI를 이용하여 Layer4-7 처리를 지원하는 DPI LDF 모듈
  - → SFT를 기반으로 한 Stateful parsing을 통해 DPI 작업에 필요한 리소스 절약
  - → Stateful 크로스 패킷 검색을 지원하여 같은 동일 세션의 패킷들 간 연속적인 검색 기능 제공
  - → PCRE를 기반으로 한 효율적인 String search 기능 제공

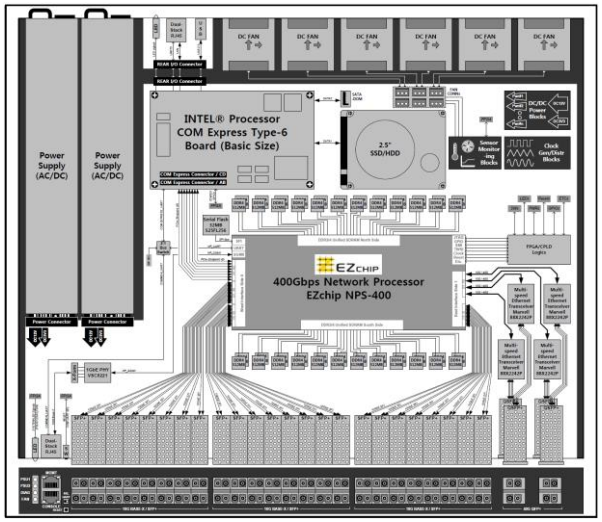


<E-SDN 스위치 DPI LDF module 작업 프로세스>

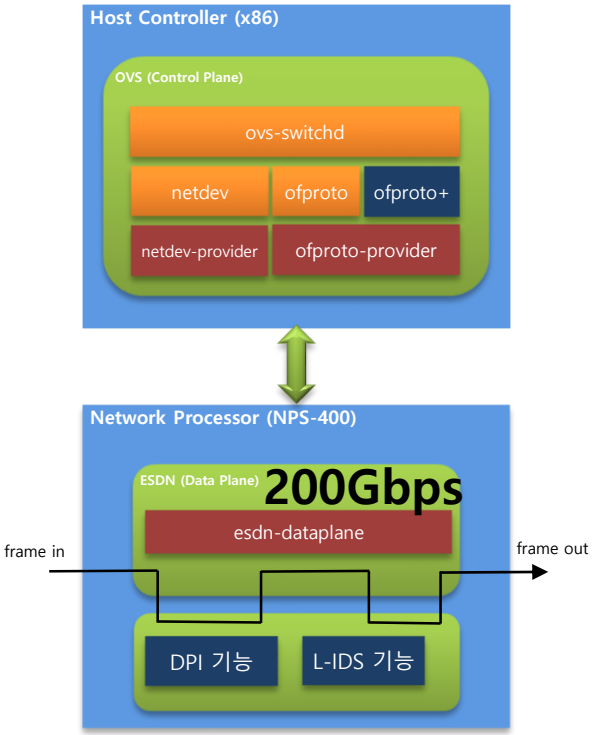
STF: Stateful Flow Table, DPI: Deep packet inspection, PCRE: Perl Compatible Regular Expression

3차년도 계획

- 확장형 SDN 스위치 하드웨어 안정화
- 확장형 SDN 스위치 소프트웨어 최적화 (200Gbps 포워딩 성능)
- L-IDS(Lightweight Intrusion Detection System) 데이터플레인 기능 개발



<E-SDN 스위치 하드웨어>

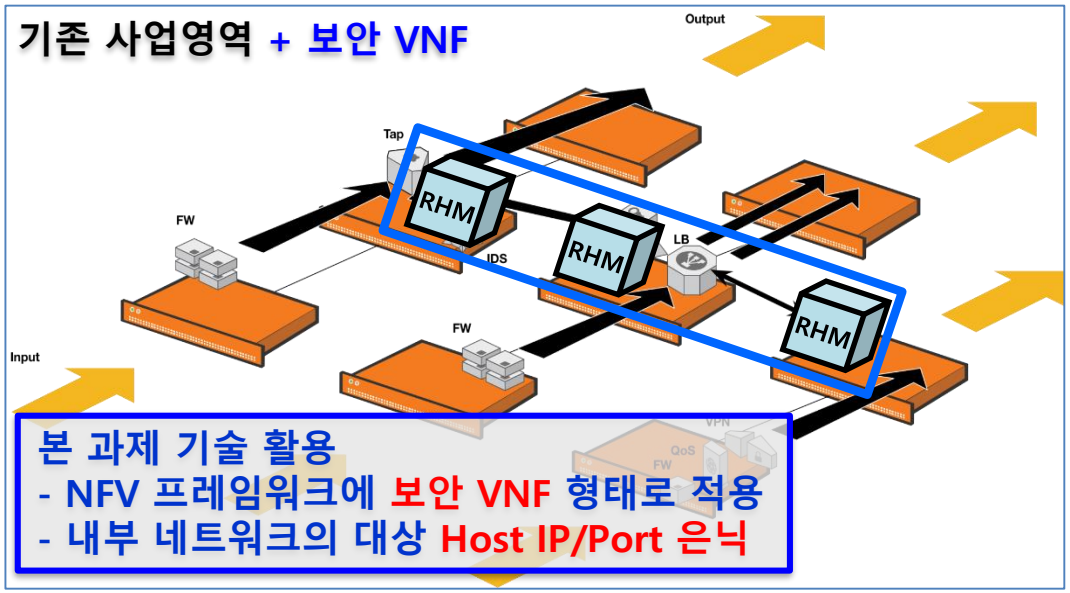


<E-SDN 스위치 소프트웨어>

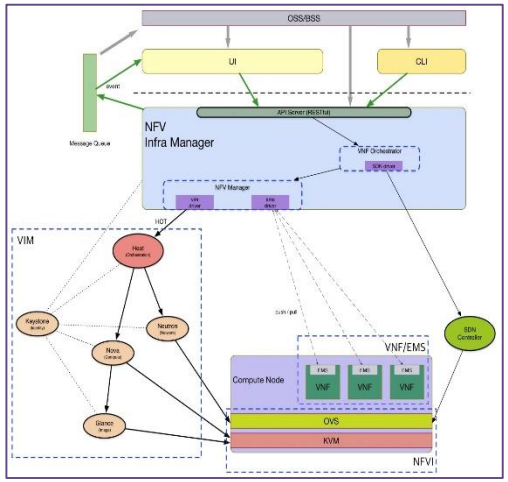
목 차

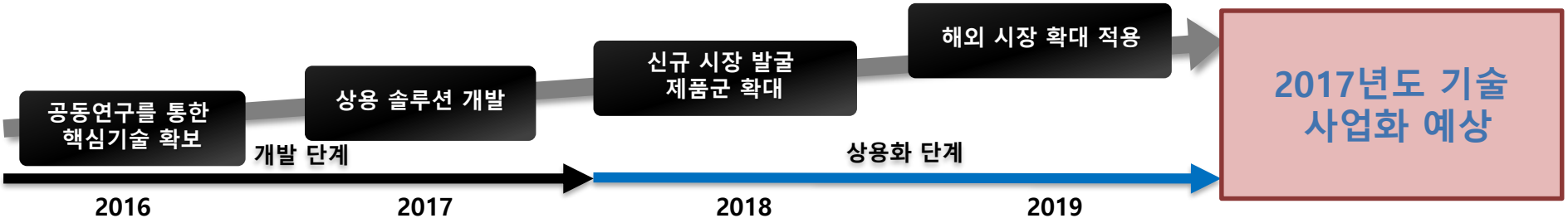
3-2. 상용화 계획

- 공동연구를 통한 SDN 기반 보안 기술 확보
- 보유 기술인 SDN/NFV 기술과 본 과제를 통해 확보된 기술을 융합
- SDN/NFV 플랫폼 + 보안 VNF -> SDN/NFV 기반 보안 솔루션으로 사업화



SDN/NFV 기반의
보안 솔루션으로 확장





3-2. 상용화 계획

㈜나임네트웍스

- 공동연구를 통한 소프트웨어 정의 보안 생태계 기술 연동 기술 확보
- 기 보유하고 있는 상용 환경 구축 기술과 본 과제를 통해 확보된 기술을 융합
- 개발을 포함한 SI 사업을 통해 매출 기회 예상

기존 사업영역

SDx Total solution

- 교육 (나임아카데미)
- SDx 컨설팅
- SDDC 플랫폼 검증 /시연/구축
- 테스트 베드
- 개발

본 과제 기술 활용

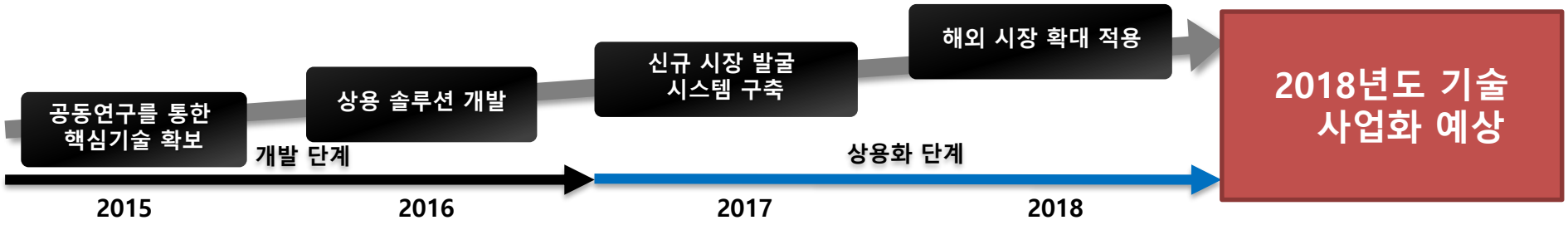
VNC 응용 기술

- SDN 테스트베드 (자사의 Rainbow)
- SDDC 운영 (자사의 Tango)
- 상용 보안기술 연동 컨설팅/개발

융합 기술 기반의 보안 솔루션으로 사업영역 확장

- 확보 VNC 기술 활용 SI 사업 발굴
- VNC 어플라이언스 제품화

자사 솔루션에서 보안 차별성 제공하여 매출확대 기대



3-2. 상용화 계획

㈜랜버드테크놀로지

- 공동연구를 통해 E-SDN HW 플랫폼의 안정화와 성능 극대화를 위한 Data Plane SW 기술 확보
- 확보된 기술을 바탕으로 공동연구 기술과 융합, 시너지를 극대화하여 목표 제품의 경쟁력 향상
- 급변하는 서비스 환경과 요구사항에 민첩하게 대응할 수 있는 SDN/NFV 기반 서비스 장비 개발

기존 사업영역

EPC
PDG
ACR
IBCF

40G이하의 집중화된 네트워크 서비스 장비

- ✓ **40G**이하 멀티코어 또는 **X86** 서버 기반
- ✓ 집중형 프로그램 구조

본 과제 기술 활용

- 고성능(200G이상) 하드웨어
  - ✓ E-SDN 데이터 플레인 소프트웨어
  - ✓ 가상기능(LVF)

◆ **Smart SDN Switch** 시장 진입

◆ **200G**이상의 **SDN** 기반 분산형 네트워크서비스 장비 개발

매출규모 : 2억원(신규) 5억원(기존) 20억원(R&D 결과 일부 적용) 50억원(R&D 결과 상용화)

목 차

4. 맺음말

- SDN 기반 동적 네트워크 은닉 기술
  - → IP 네트워크의 개방성 이슈
  - → 경계 기반 공격 차단 기술에서 변혁적인(Game-changing) 기술로 진화
  - → SDN 기반으로 악의적 사용자의 공격에 대한 예측불가능성 (Unpredictability), 불확정성(Uncertainty) 및 비용(Cost) 증가 기술 개발

- 핵심 요소 기술 개발 현황
  - → RRM, RHM, VNC, E-SDN 기술 개발 및 성능 개선

- 상용화 계획
  - → Atto Research: RHM/RRM
  - → 나임 네트웍스: VNC
  - → 랜버드 테크놀로지: E-SDN


감사합니다
Smart & Green Technology Innovator
ETRI