**연구현황 및 개발요구 목록**

**NAME**: 이종태 **Revision Date**: 2023.08.18

|  |  |  |
| --- | --- | --- |
| **[공식 확인 일정]** | | |
| 순번 | 세부 일정 | 마감 일자 |
| 1 | 과제 제안서 마감 | 23.03.17 |
| 2 | Kick-off 미팅 (아주대학교, 수원) | 23.04.13 |
| 3 | 1차 과제 미팅 (아주대학교, 수원) | 23.07.07 |
| 4 | 중간보고서 마감 | 23.07.31 |
| 5 | 2차 과제 미팅 (국가보안연구소, 대전) | 23.08.04 |
| 6 | 개발 코드 국보연 전달 | 23.08.16 |
| 7 | 10월 위탁과제 합동발표 일정 (확정 아님)  일시: 2023년 10월 24일(화)  시간: 09:30 ~ 17:30  장소: 호텔 인터시티 (대전 유성구) | 23.10.24 |
| 8 | N/A | N/A |
| 9 | N/A | N/A |

|  |  |  |
| --- | --- | --- |
| **[진행 사항]**  세부항목 시작기준: 2023.08.18 | | |
| 순번 | 세부 항목 | 달성여부 |
| **1. 자료조사 및 공부** | | |
| 1 | 주니퍼 라우팅 프로토콜 확인 | **□** |
| 2 | IS-IS 데이터 파악 | **□** |
| 3 | 라우터 NAT 기능 자료조사 및 공부 | **□** |
| 4 | N/A | N/A |
| **2. 시나리오 분석** | | |
| 1 | EVE-ng 내 명령어를 통한 네트워크 시나리오 분석/파악 | **▣** |
| 2 | **(~를 위한)** EVE-ng version 업데이트 | **□** |
| 3 | EVE-ng xml 백업 데이터 규격 확인 **(백업데이터가 뭔지 간단하게 적어주세요)** | **□** |
| 4 | N/A | N/A |
| **3. 데이터 파싱 코드 개발** | | |
| 1 | 기본 데이터 파싱 설계 | **▣** |
| 2 | 국보연 중간코드 전달을 위한 병합처리 (GitHub) | **▣** |
| 3 | ARP 오류 알고리즘 수정 **(어떤 오류인지 써주세요)** | **□** |
| 4 | Logical System 구분 파싱 (2차 파싱) | **□** |
| 4 | N/A | N/A |
| **4. 네트워크 분석 알고리즘** | | |
| 1 | Logical System 별도 표기 방안 구상 | **□** |
| 2 | N/A | N/A |
| **5. 개발 코드 검증 및 점검** | | |
| 1 | 네트워크 확장에 따른 파싱 도구 및 알고리즘 검증 **[~N/A]** | **□** |
| 2 | N/A | N/A |

|  |  |
| --- | --- |
| **[항목별 세부 사항 & issues]** | |
| 카테고리 | 세부 내용 |
| **Issue #1**  **\*\*\*\***  **Issue 마감\*\*\*\*** | **<Logical System 파싱, 23.08.18, 작성자: 이종태>**   * 논리적 시스템에 대한 정보 추가 관련하여, “R1-R3-R1”등의 파일에 대한 분석 진행 * 현재, 논리적 시스템 정보에 대한 추가 파일이 존재 (i.e., R3-R3-R1\_arp.xml, R3-R3-R1\_route.xml) * 다만, R3에 물리적으로 정의된 포트번호 및 routing-table 정보와 R3-R3-R1 파일에 저장 되어있는 Logical System의 포트번호 및 routing-table 정보는 서로 상이함. * 이에 따라, Logical System에 대한 정보는 별도로 디바이스 (“Device Name”)으로 분리시켜 저장할 필요가 있음. * 다만, 현재까지 추출된 데이터와 구조적 혼란이 해결되지 않아 코드 수정이 막힘. * **현재 가장 필요한 개념은 “기존 4가지 파일에서의 interface 정보와 R3-R3-R1에서의 interface 정보 구별”이 필요하다.** * 예시는 아래 그림과 같다. *(ge-0/0/4 내부의 ge-0/0/4.1, ge-0/0/4.0)*      * **즉, 전체적인 네트워크 분석** (특정 라우터의 인터페이스 구조와 그 내부의 logical system에서의 인터페이스 포트번호 및 구조 등)**에 대한 정보가 제공해주면 수월 (네트워크 맵 혹은 라우터 별 인터페이스 구조** (logical 별도) **정리된 표)** * 해당 항목 정리되면 기반으로 logical system을 라우터 내부에 별도로 저장하도록 변경할 예정 * (+) 세부적인 Logical Router 별도 표기를 위한 데이터는 2차 파싱에서 진행하고, 1차파싱에서는 별도로 고려하지 않기로 구상. |
| **Report #1** | **<1차 파싱 코드 변경 요약, 23.08.31, 작성자: 장희연>**   * **Parsing\_main.py** (희연 코드의 data\_process.py 역할과 같음)   라우터 번호만이 아닌, 파일 종류별로만 sort   * **parse\_xml\_conf.py**   각 hostname의 인터페이스 읽어와서 key로 추가  Conf 파일에 logical-systems 태그 있으면 파싱 결과 파일에 ‘logical-systems’ 키 만들고, 이에 대한 value로 리스트 만듦 (여러 개의 logical system 있을 수 있기 때문에)  파싱 결과 파일에 logical system 객체 만들고, logical system 여부 ‘\*’로 표기  logical system 객체에 인터페이스 정보 추가  logical system이 있으면 이에 대응하는 xml 파일 logical\_systems 폴더 만들어서 여기로 전달   * **parse\_xml\_interface.py**   네임스페이스 파싱  인터페이스 추가  수정하고자 하는 부분 : 만약 parsing\_result.json에 조회하는 인터페이스가 없는 경우에도 인터페이스 추가  호스트가 logical system 가지고 있으면 리스트 조회하여,  인터페이스가 logical system의 인터페이스에 해당하는지 확인하고  인터페이스 정보 추가   * **parse\_xml\_arp.py**   네임스페이스 파싱  호스트가 logical system 가지고 있는 경우, 먼저 호스트에서 인터페이스가 arp에 해당하는지 확인, 해당하면 arp list에 추가  다음에 logical system에 접근하여 인터페이스가 arp에 해당하지는 확인, 해당하면 logical system의 arp list에 추가  Host가 logical system 가지고 있지 않은 경우 인터페이스가 arp에 해당하는지 확인하고, 해당하면 logical system의 arp list에 추가   * **parse\_xml\_route.py**   네임스페이스 파싱  라우트 테이블 조회하고  호스트가 logical system 가지고 있으면 logical-systems 폴더에서 해당 logical system의 route 파일 읽어와서 정보 추가하기  끝나고 그냥 호스트에 해당하는 라우트 정보추가  호스트가 logical system 가지고 있지 않은 경우에 대한 라우트 정보 추가 |
| **report #2** | **<1차 파싱 코드 병합, 23.08.31, 작성자: 이종태>**  1차 파싱 코드 병합처리 완료  GitHub main branch에 병합 완료 [ main branch < branch\_jt ]  (동기화 진행하거나 모르겠으면 Branch, 메인 복제해서 파드릴께요 말씀주세요)  **<확인사항>**  - 일부 코드 수정, 코드 구조 동결 (향후 기타 기능만 넣고 코드 구조는 변경하지 말 것)  - 2차 파싱은 “sub\_parse” 폴더에서 진행  : [알고리즘 코드 + 해당 알고리즘을 위한 2차 파싱 도구 코드] 패키지  : 한 패키지 당 sub\_parse 폴더 내 새로운 폴더로 저장하여 경로 참조시킬 것  - 모든 참조는 header.py로 통일 저장하였으며, 전역 딕셔너리인 parsing\_data도 header에 선언되어 있음, 사용을 위해서는 header 참조 후 header.parse\_data로 참조하면 됨  - 중간 분기 때 테스트로 구성했던 analysis\_data 코드는 사용 시 수정해야함 (데이터 구조가 변경되어 동작 불가)  - **Logical System의 Routing 파일에 대한 처리가 필요함, 또한 parse\_xml\_route는 변경되지 않았음**  - 코드 확인 후 9월 1주차까지 1차 파싱 작업 마무리, 기말보고서 및 발표에 보여주기 위한 연결성 분석 알고리즘 2~3개와 그를 통해 시각화된 결과물까지 뽑아두는 것이 좋을 것 같아 학기 바빠지기 전에 빠르게 처리하고 자료 정리 진행 필요  - 향후 Switch 추가 여부에 대해서 확장성 고려해야 함.  (추가적인 1차파싱 코드 생성 필요 예상) |
| **Issue #N/A** | <~세부내용 타이틀~, 날짜, 작성자: 이름, 논의/확인/검토 등 필요여부>  ~세부 내용 작성~ |