

결과 파일: 0802_analysis.txt

1. 프로토콜/응답 포트별 연결 수 Top 10 (Protocol/Resp_Port)

462269 tcp 443
15 udp 443

2. 서버 이름별 연결 수 Top 10 (SSL/TLS Server Name)

150564 cdn.muni.cz
104745 www.muni.cz
13660 www.skm.muni.cz
13509 www.econ.muni.cz
13094 www.fss.muni.cz
8596 webcentrum.muni.cz
8197 poradna.fss.muni.cz
7859 it.muni.cz
6927 www.ics.muni.cz
6049 www.recetox.muni.cz

3. 시간대별 활동량 시각화 (Hour vs. Count)

[00] 23168 *****
[01] 21740 *****
[02] 19754 *****
[03] 21129 *****
[04] 20272 *****
[05] 19199 *****
[06] 16200 *****
[07] 13622 *****
[08] 11105 *****
[09] 10038 *****
[10] 10078 *****
[11] 10721 *****
[12] 11443 *****
[13] 13685 *****
[14] 14399 *****
[15] 19508 *****
[16] 25964 *****
[17] 29236 *****
[18] 24842 *****
[19] 25670 *****
[20] 25053 *****
[21] 24894 *****

[22] 26637 *****

[23] 23927 *****

4. 비정상 종료 연결 상태 Top (SF: 정상 종료 제외)

189569 RSTR
45101 RSTO
24694 OTH
3747 SH
3149 S1
922 RSTRH
728 SHR
189 S0
62 S2
47 REJ
2 RSTOS0

5. 데이터 전송량 Top 10 (Total/Client Tx/Server Tx - 단위 자동 변환)

Total Size	Resp_IP	Client Tx (Orig)	Server Tx (Resp)	TS (Timestamp)
2.00GB	10.0.0.1	517B	2.00GB	1627891600.051613
1.75GB	10.0.0.1	517B	1.75GB	1627891339.971053
1.57GB	10.0.0.1	116B	1.57GB	1627869726.177797
1.29GB	10.0.0.1	1.47KB	1.29GB	1627894789.525116
1.12GB	10.0.0.1	1.27KB	1.12GB	1627915166.007358
1010.80MB	10.0.0.1	517B	1010.80MB	1627891339.702077
932.32MB	10.0.0.1	2.40KB	932.31MB	1627915163.929020
846.52MB	10.0.0.2	1.39KB	846.51MB	1627915167.698752
838.20MB	10.0.0.1	1.37KB	838.20MB	1627915166.307764
751.28MB	10.0.0.1	517B	751.27MB	1627891339.697682

6. 서버 응답량 분포 Top 10 (MB 단위)

454922 0MB
4446 1MB
1220 2MB
556 3MB
327 4MB
244 5MB
143 6MB
95 7MB
67 10MB
54 8MB

7. 평균 연결 지속 시간 (Average Duration)

평균 연결 지속 시간: 21.4951 초

=====

1. 트래픽 환경 및 기본 특징

- cdn.muni.cz: 150,564건 (CDN 서버)
- www.muni.cz: 104,745건 (메인 웹사이트)
- www.skm.muni.cz: 13,660건
- www.econ.muni.cz: 13,509건
- www.fss.muni.cz: 13,094건
- 기타 서브 도메인 다수 확인

2. 시간대별 활동 패턴

- ****피크 시간대****: 17시(29,236건), 22시(26,637건), 16시(25,964건)에 최고치 기록
- ****활동 집중 시간****: 00~05시 새벽 시간과 15~23시 오후/저녁 시간대에 집중
- ****특징****: 일반 업무 시간(08~14시)에는 상대적으로 낮고, 오후~심야에 트래픽 급증
→ 업무 종료 후 사용량 증가 및 자동화 작업 혼재로 추정

3. 연결 상태 및 실패율

- ****비정상 연결 다수 발생****
 - RSTR (클라이언트 측 강제 종료): 189,569건
 - RSTO (서버 측 강제 종료/타임아웃): 45,101건
 - OTH (기타 상태): 24,694건
 - SH, S1 등 기타 비정상 상태 다수
- ****원인 추정****: 클라이언트 요청 중단 또는 서버 과부하로 인한 강제 종료
- ****평균 연결 지속 시간****: 21.5초로 긴 편

4. 데이터 전송 부하 분석 (Top 10)

- ****전송량 규모****: 751.28MB~2.00GB의 대규모 데이터 전송 발생
- ****전송 방향별 특징****
 - 서버 → 클라이언트: 2.00GB, 1.75GB, 1.57GB 등 대용량 다운로드 집중
→ 거의 모든 Top 10 연결이 서버에서 클라이언트로의 대용량 전송
 - 클라이언트 전송량: 대부분 1KB 미만으로 매우 작음 (최대 2.40KB)
- ****특징****: 단방향 대용량 다운로드 패턴이 명확함

5. 서버 응답량 분포

- ****대부분 소용량****: 454,922건(98.4%)이 0MB대 응답
- ****중대용량 응답****: 1~10MB 범위 응답이 7,152건 정도 분포
- ****특징****: 소량의 연결에서 대용량 전송이 집중됨