

결과 파일: 0804_analysis.txt

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

446388 tcp 443
8 udp 443

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

135588 cdn.muni.cz
105100 www.muni.cz
13329 www.fss.muni.cz
13039 www.econ.muni.cz
8297 poradna.fss.muni.cz
7793 it.muni.cz
7212 www.ics.muni.cz
6268 webcentrum.muni.cz
5380 muni.cz
5353 www.skm.muni.cz

3. 시간대별 활동량 시각화 (Hour vs. Count)

[00] 22601 *****
[01] 23552 *****
[02] 22443 *****
[03] 21515 *****
[04] 18096 *****
[05] 18527 *****
[06] 15855 *****
[07] 13596 *****
[08] 12062 *****
[09] 11448 *****
[10] 10636 *****
[11] 11598 *****
[12] 11458 *****
[13] 13758 *****
[14] 15040 *****
[15] 17568 *****
[16] 21308 *****
[17] 22895 *****
[18] 22209 *****
[19] 22111 *****
[20] 23714 *****
[21] 27767 *****

[22] 24889 *****

[23] 21750 *****

4. 비정상 종료 연결 상태 Top (SF: 정상 종료 제외)

159847 RSTR
43001 RSTO
26613 OTH
3678 SH
2267 S1
726 RSTRH
554 SHR
133 S0
56 S2
38 REJ
22 S3

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)
3.69GB	10.0.0.1	1.89GB	1.81GB	1628113442.193624
2.00GB	10.0.0.2	232B	2.00GB	1628074666.319874
1.94GB	10.0.0.1	517B	1.94GB	1628105710.640252
1.75GB	10.0.0.1	1.75GB	3.01KB	1628091412.314466
1.66GB	10.0.0.1	675B	1.66GB	1628109790.864159
1.65GB	10.0.0.1	1.65GB	2.89KB	1628095853.180998
1.20GB	10.0.0.1	1.37KB	1.20GB	1628113492.041947
1.17GB	10.0.0.1	517B	1.17GB	1628106792.342086
1.01GB	10.0.0.1	1.01GB	9.39KB	1628076482.136346
784.68MB	10.0.0.1	517B	784.68MB	1628105717.659267

6. 서버 응답량 분포 Top 10 (MB 단위)

440322 0MB
3295 1MB
1140 2MB
553 3MB
305 4MB
272 5MB
121 6MB
101 7MB
65 10MB
51 8MB

7. 평균 연결 지속 시간 (Average Duration)

평균 연결 지속 시간: 18.0656 초

=====

1. 트래픽 환경 및 기본 특징

- 전체 44만 6396건 중 446,388건이 TCP 443 포트(HTTPS) 사용 (99.99%), UDP 443 연결 8건
- cdn.muni.cz: 135,588건 (CDN 서버)
- www.muni.cz: 105,100건 (메인 웹사이트)
- www.fss.muni.cz: 13,329건
- www.econ.muni.cz: 13,039건
- 기타 서브 도메인 다수 확인

2. 시간대별 활동 패턴

- 피크 시간대: 21시(27,767건), 22시(24,889건), 20시(23,714건)에 최고치 기록
- 활동 집중 시간: 00~05시 새벽과 16~23시 저녁 시간대에 집중
- 특징: 업무 시간(08~14시)보다 저녁~심야에 트래픽 급증, 특히 21시에 가장 높은 피크
→ 업무 종료 후 사용량 증가 및 자동화 작업 혼재로 추정

3. 연결 상태 및 실패율

- 비정상 연결 다수 발생
- RSTR (클라이언트 측 강제 종료): 159,847건
- RSTO (서버 측 강제 종료/타임아웃): 43,001건
- OTH (기타 상태): 26,613건
- SH, S1 등 기타 비정상 상태 다수
- 원인 추정: 클라이언트 요청 중단 또는 서버 과부하로 인한 강제 종료
- 평균 연결 지속 시간: 18.1초로 긴 편

4. 데이터 전송 부하 분석 (Top 10)

- 전송량 규모: 784.68MB~3.69GB의 대규모 데이터 전송 발생
- 전송 방향별 특징
- 최대 전송: 3.69GB (클라이언트 1.89GB, 서버 1.81GB) → 양방향 대용량 전송
- 서버 → 클라이언트: 2.00GB, 1.94GB, 1.66GB, 1.20GB, 1.17GB 등 대용량 다운로드 다수
- 클라이언트 → 서버: 1.75GB, 1.65GB, 1.01GB 등 대용량 업로드 확인
- 특징: 다운로드와 업로드가 혼재되어 양방향 트래픽 균형적으로 발생

5. 서버 응답량 분포

- 대부분 소용량: 440,322건(98.6%)이 0MB대 응답
- 중대용량 응답: 1~10MB 범위 응답이 5,903건 정도 분포
- 특징: 소량의 연결에서 대용량 전송이 집중됨