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

430890 tcp 443
26 udp 443

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

136413 cdn.muni.cz
105063 www.muni.cz
13026 www.econ.muni.cz
12872 www.fss.muni.cz
7963 poradna.fss.muni.cz
7233 it.muni.cz
6017 webcentrum.muni.cz
5695 www.ics.muni.cz
5087 www.skm.muni.cz
5019 www.recetox.muni.cz

3. 시간대별 활동량 시각화 (Hour vs. Count)

[00] 21159 *****
[01] 21853 *****
[02] 22226 *****
[03] 18822 *****
[04] 18258 *****
[05] 18121 *****
[06] 14397 *****
[07] 13153 *****
[08] 11476 *****
[09] 11352 *****
[10] 12424 *****
[11] 12950 *****
[12] 11003 *****
[13] 13904 *****
[14] 15135 *****
[15] 17356 *****
[16] 21922 *****
[17] 23957 *****
[18] 22466 *****
[19] 21295 *****
[20] 22265 *****
[21] 21158 *****
[22] 22656 *****

[23] 21608 *****

4. 비정상 종료 연결 상태 Top (SF: 정상 종료 제외)

157919 RSTR
41708 RSTO
25098 OTH
3900 SH
2581 S1
504 RSTRH
406 SHR
291 S0
146 REJ
43 S2
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)
5.06GB	10.0.0.1	4.00GB	1.06GB	1628190068.571333
3.12GB	10.0.0.1	3.12GB	0B	1628187268.963408
2.65GB	10.0.0.1	888.84MB	1.78GB	1628187830.848956
2.45GB	10.0.0.1	1.12GB	1.33GB	1628190429.200038
1.88GB	10.0.0.1	1.88GB	54.92KB	1628190814.692561
1.62GB	10.0.0.1	517B	1.62GB	1628192395.920539
1.46GB	10.0.0.1	1.46GB	0B	1628191044.141419
1.38GB	10.0.0.1	1.38GB	80.87KB	1628186966.558773
1.34GB	10.0.0.1	1.39KB	1.34GB	1628163336.092962
1.26GB	10.0.0.1	667B	1.26GB	1628158803.648538

6. 서버 응답량 분포 Top 10 (MB 단위)

424988 0MB
3415 1MB
1043 2MB
497 3MB
232 4MB
210 5MB
134 6MB
102 7MB
61 8MB
51 10MB

7. 평균 연결 지속 시간 (Average Duration)

평균 연결 지속 시간: 18.2412 초

1. 트래픽 환경 및 기본 특징

- 전체 43만 916건 중 430,890건이 TCP 443 포트(HTTPS) 사용 (99.99%), UDP 443 연결 26건
- cdn.muni.cz: 136,413건 (CDN 서버)
- www.muni.cz: 105,063건 (메인 웹사이트)
- www.econ.muni.cz: 13,026건
- www.fss.muni.cz: 12,872건
- 기타 서브 도메인 다수 확인

2. 시간대별 활동 패턴

- 피크 시간대: 17시(23,957건), 22시(22,656건), 20시(22,265건)에 최고치 기록
- 활동 집중 시간: 00~05시 새벽과 15~23시 오후/저녁 시간대에 집중
- 특징: 업무 시간(08~14시)보다 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): 157,919건
- RSTO (서버 측 강제 종료/타임아웃): 41,708건
- OTH (기타 상태): 25,098건
- SH, S1 등 기타 비정상 상태 다수
- 원인 추정: 클라이언트 요청 중단 또는 서버 과부하로 인한 강제 종료
- 평균 연결 지속 시간: 18.2초로 긴 편

4. 데이터 전송 부하 분석 (Top 10)

- 전송량 규모: 1.26GB~5.06GB의 대규모 데이터 전송 발생
- 전송 방향별 특징
- 최대 전송: 5.06GB (클라이언트 4.00GB, 서버 1.06GB) → 초대용량 업로드 주도
- 클라이언트 → 서버: 4.00GB, 3.12GB, 1.88GB, 1.46GB, 1.38GB 등 대용량 업로드 집중
→ 대규모 파일 업로드나 백업 작업으로 추정
- 서버 → 클라이언트: 1.78GB, 1.62GB, 1.34GB, 1.26GB 등 대용량 다운로드도 확인
- 특징: 클라이언트→서버 방향 업로드가 압도적으로 많음, 특히 5GB 이상 초대용량 전송 발생

5. 서버 응답량 분포

- 대부분 소용량: 424,988건(98.6%)이 0MB대 응답
- 중대용량 응답: 1~10MB 범위 응답이 5,745건 정도 분포
- 특징: 소량의 연결에서 대용량 전송이 집중됨