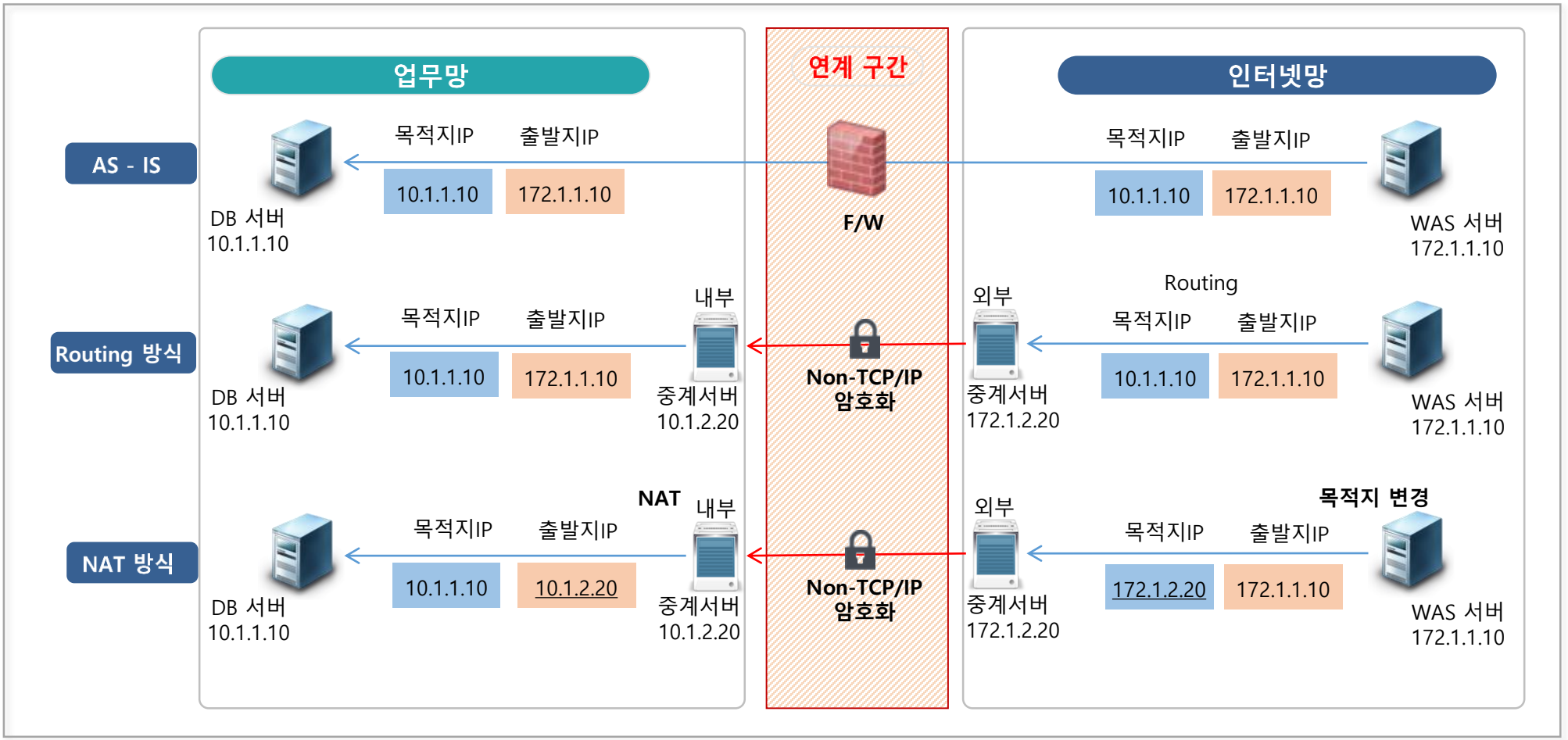
CC인증 GS인증

망간자료전송 솔루션
스트림 연계 매뉴얼

SecureGate는 스토리지 방식과 인피니밴드 방식
그리고 소켓 방식 3가지 제품을 제공합니다.

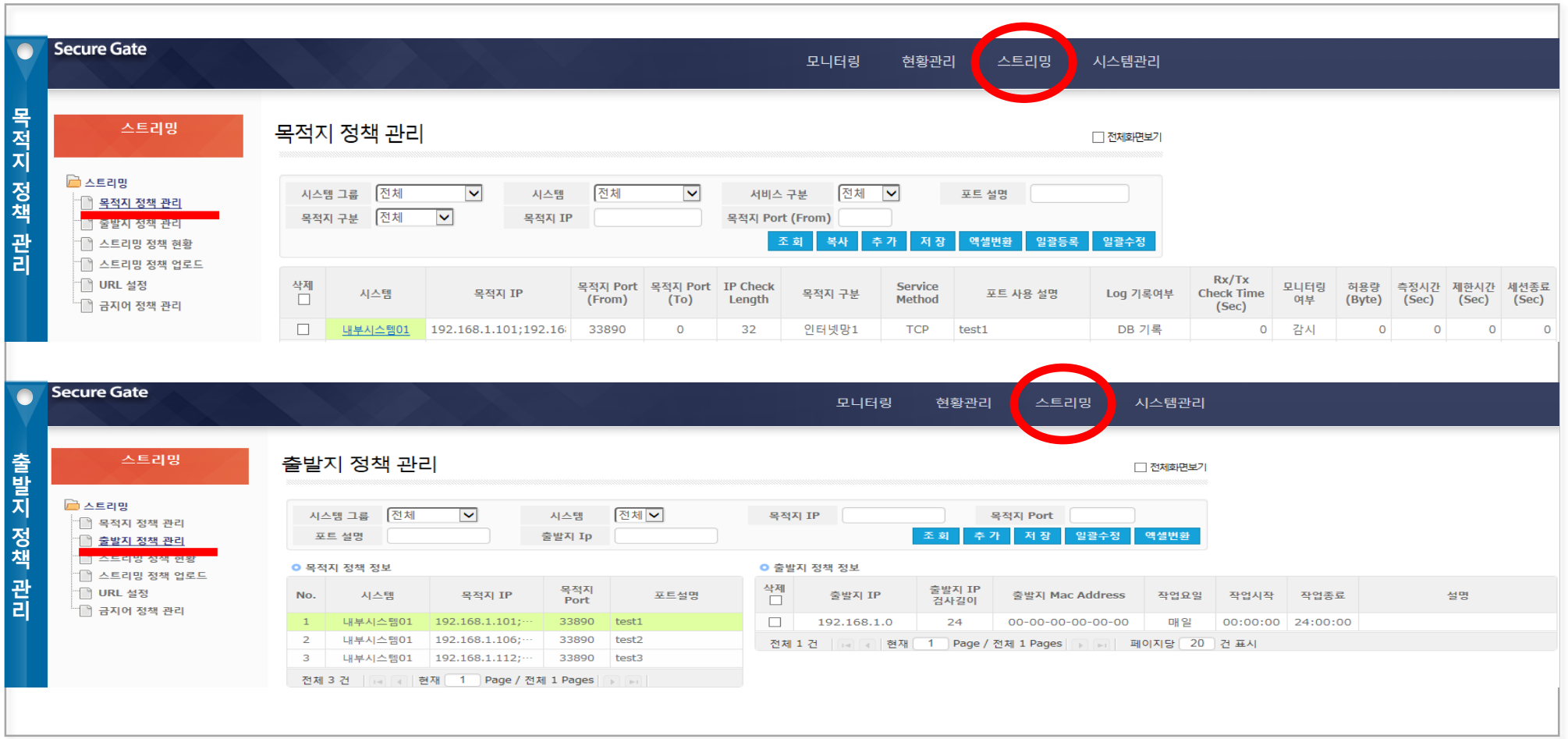
1. 스트림 연계 방식

스트림 연계는 **분리된 업무망과 인터넷망 구간**을 **Non TCP/IP 기반**의 자체 암복호화과정을 통해 **안전한 데이터 전송 기능**을 제공한다. **스트림 연계 방식**은 **Routing 방식**과 **NAT 방식**으로 구분된다.



2. 스트림 연계 정책 관리

스트림 연계는 **관리자가 정의한 연계 정책**을 기반으로 서비스를 지원한다. 관리자는 **웹매니저를 이용**하여 **목적지 연계 정책**과 **출발지 연계 정책**을 정의할 수 있다. **"목적지 정책 관리"** 화면은 **스트림 연계가 필요한 목적지의 운영 정책을 등록하는 화면**이며, **"출발지 정책 관리"** 화면은 **등록된 목적지에 접근할 수 있는 출발지 정보를 관리하는 화면**이다.



1. 목적지 정책 등록 [1/2]

관리자는 관리자 웹페이지 **"스트리밍"** 메뉴의 **"목적지 정책 관리"** 화면에서 목적지 연계 정책을 관리한다.

※ 스트림 연계 데이터 로그 기록 시, 대량의 스트림 연계 데이터 발생으로 시스템 장애가 발생 가능함

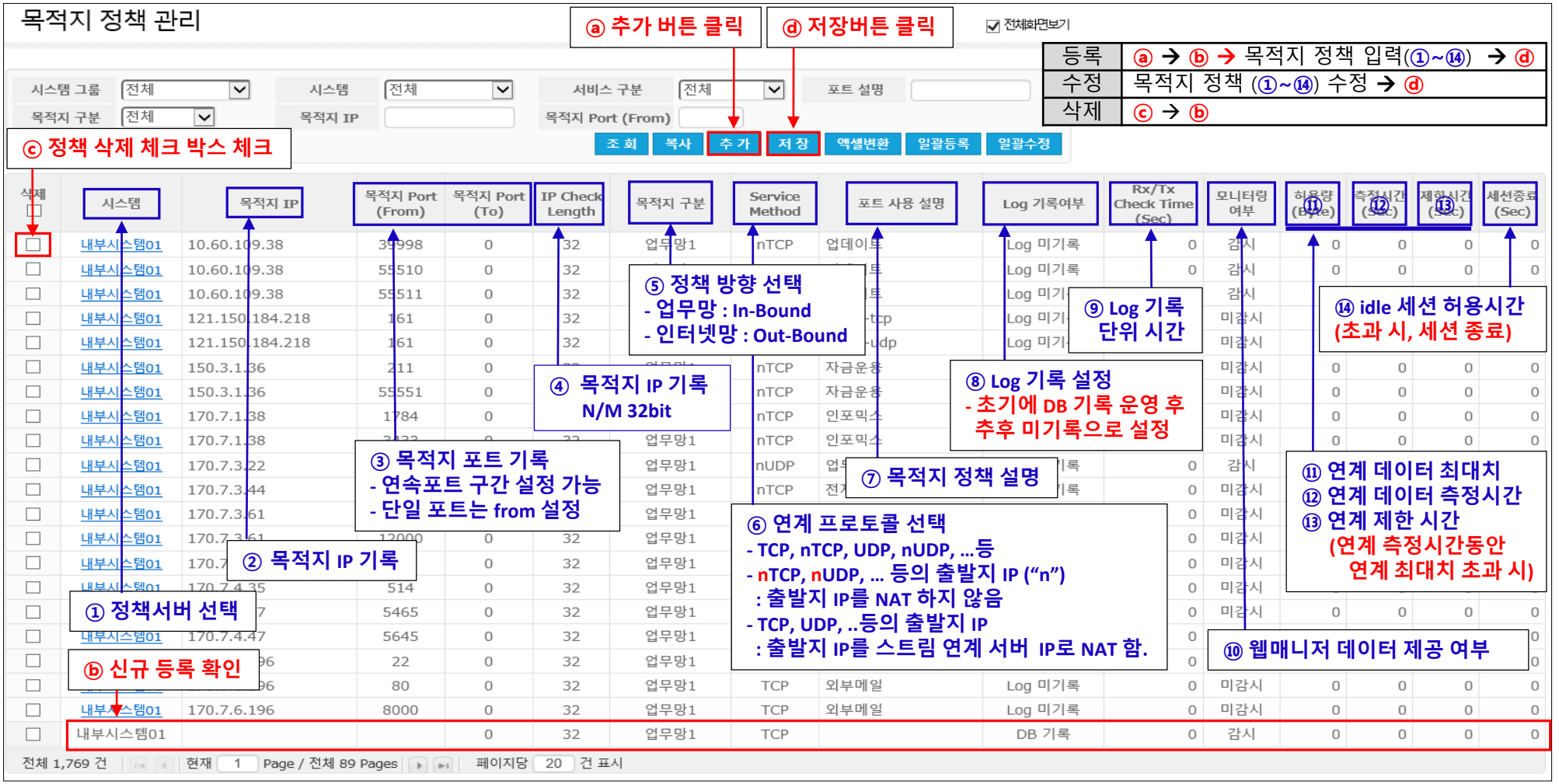
등록	추가버튼 (ⓐ) 클릭 → 목적지 정책 (①~⑭) 입력 → 저장버튼 (ⓑ) 클릭
수정	목적지 정책 (①~⑭) 수정 → 저장버튼 (ⓑ) 클릭
삭제	삭제 체크박스 (ⓒ) 체크 → 저장버튼 (ⓑ) 클릭

▶ 목적지 정책 입력 항목

①	시스템	스트림 연계 정책을 적용할 시스템	
②	목적지 IP	스트림 연계 목적지 IP	
③	목적지 Port	스트림 연계 목적지 Port	**연속 포트구간:** 첫 포트는 from에 마지막 포트는 to에 등록 (**단일 포트는** from 등록)
④	IP Check Length	목적지 NetMask 32bit 설정	
⑤	목적지 구분	연계 방향 설정 (내부망 기준)	**업무망:** In-Bound 연계, **인터넷망:** Out-Bound 연계
⑥	Service Method	연계 정책 프로토콜 타입 (TCP, UDP, SFTP … 등)	
⑦	포트 사용 설명	연계 정책 설명	
⑧	Log 기록여부	Log 기록 방법 (DB/File/Text기록, Log미기록 등)	**※ 스트림 연계 데이터는 대량발생이 가능하므로 기록 시, Disk Full 발생 가능**
⑨	RX/TX Check Time	Log 기록 단위 시간 (초 단위)	
⑩	모니터링 여부	웹매니저 데이터 제공 여부 (감시 미감시)	**감시:** 웹매니저 화면에 데이터 제공, **미감시:** 웹매니저 화면에 데이터 미제공
⑪	허용량	정책 연계 허용량 (Byte)	
⑫	측정시간	정책 연계 허용량 측정 시간 (초단위)	
⑬	제한시간	정책 연계 허용량 초과 시, 연계 차단 시간 (초단위)	연계 차단시간 동안은 스트림 연계를 제공하지 않음.
⑭	세션종료	Idle 세션 최대 허용시간	**idle 세션 최대 허용 시간 초과 시**, 해당 세션 강제 종료함.

1. 목적지 정책 등록 [2/2]

관리자는 연계 목적지 정책 정보를 아래와 같이 등록/수정/삭제한다.



2. 출발지 정책 등록 [1/2]

관리자는 관리자 웹페이지 **"스트리밍"** 메뉴의 **"출발지 정책 관리"** 화면에서 목적지 정책에 대한 출발지 연계 정책을 관리한다.

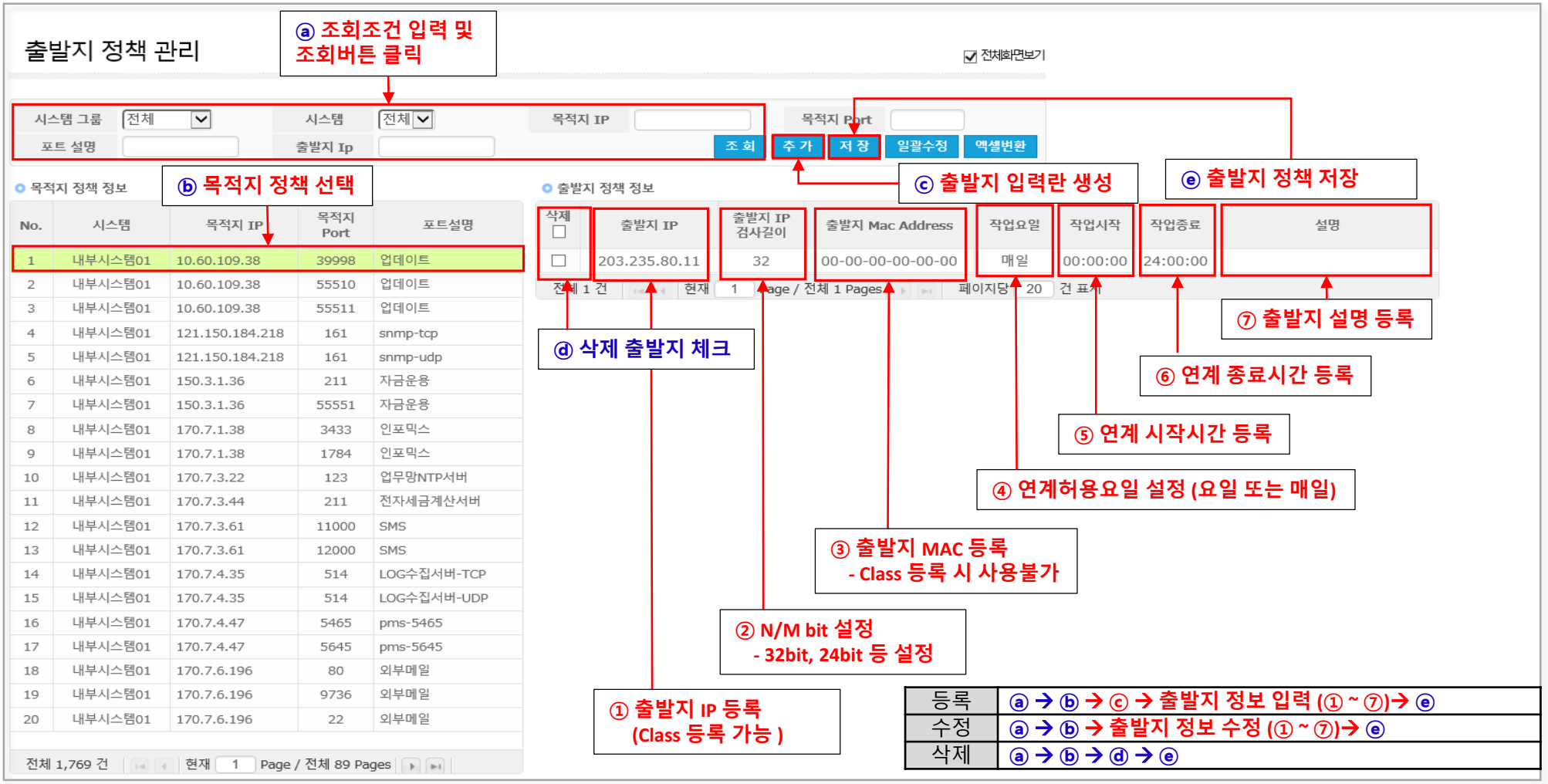
등록	출발지를 등록할 목적지 정책 조회 (ⓐ) → 목적지 선택 (ⓑ) → 추가버튼 (ⓒ) 클릭 → 출발지 정책 (①~⑦) 입력 → 저장버튼 (ⓔ) 클릭
수정	출발지를 등록할 목적지 정책 조회 (ⓐ) → 목적지 선택 (ⓑ) → 출발지 정책 (①~⑦) 수정 → 저장버튼 (ⓔ) 클릭
삭제	출발지를 등록할 목적지 정책 조회 (ⓐ) → 목적지 선택 (ⓑ) → 삭제할 출발지 리스트 체크박스 (ⓓ) 체크 → 저장버튼 (ⓔ) 클릭

▶ 출발지 정책 입력 항목

①	출발지 IP	목적지에 접속을 인가할 IP (IP 또는 IP 대역)
②	출발지 IP 검사길이	NetMask bit 설정
③	출발지 Mac Address	출발지 Mac Address
④	작업요일	매일, 일요일, 월요일, 화요일, 수요일, 목요일, 금요일, 토요일
⑤	작업시작	스트림 연계 시작시간
⑥	작업종료	스트림 연계 종료시간
⑦	설명	출발지 정책 설명

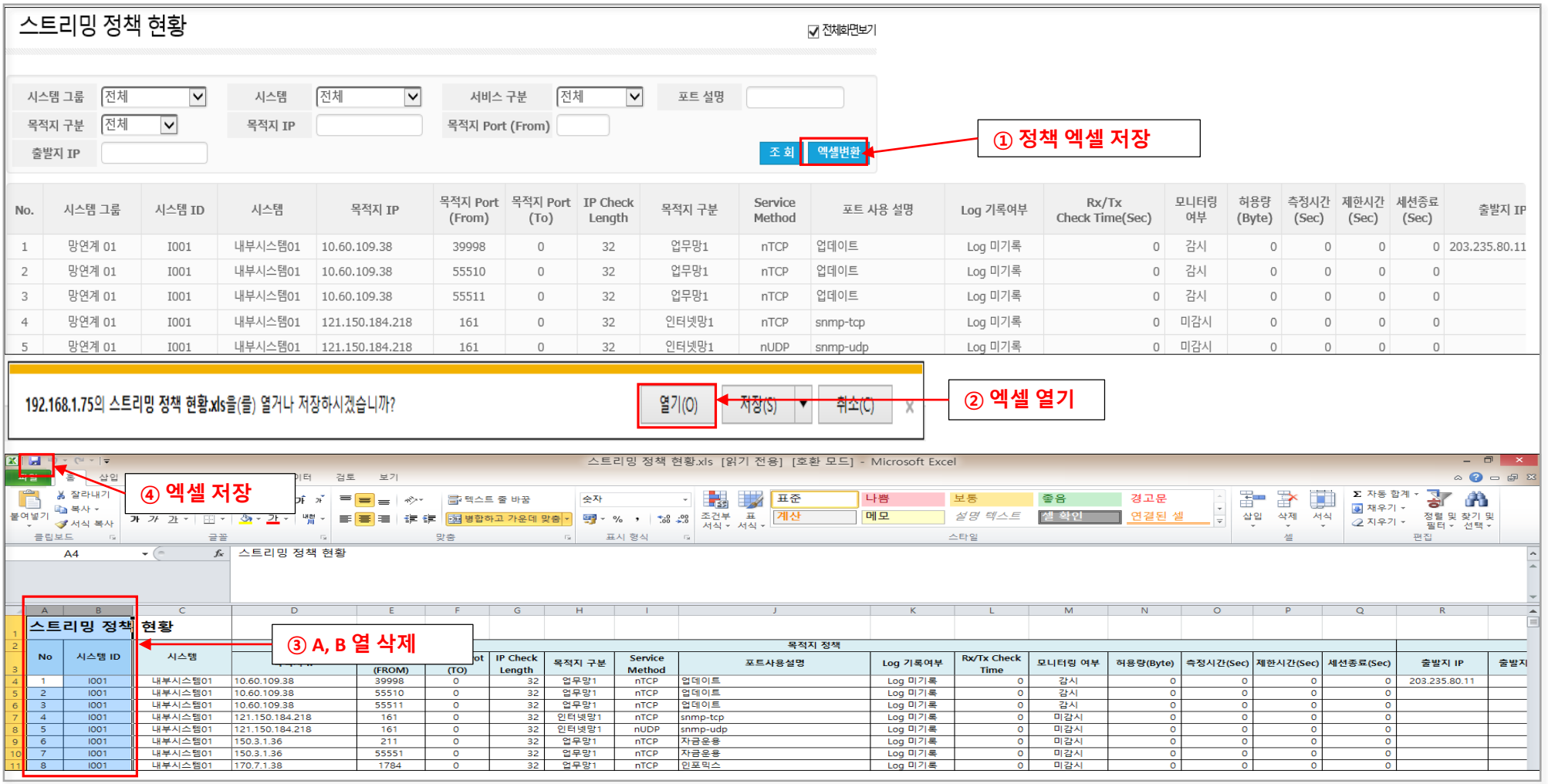
2. 출발지 정책 등록 [2/2]

관리자는 연계 목적지에 인가할 출발지 정책 정보를 아래와 같이 등록/수정/삭제한다.



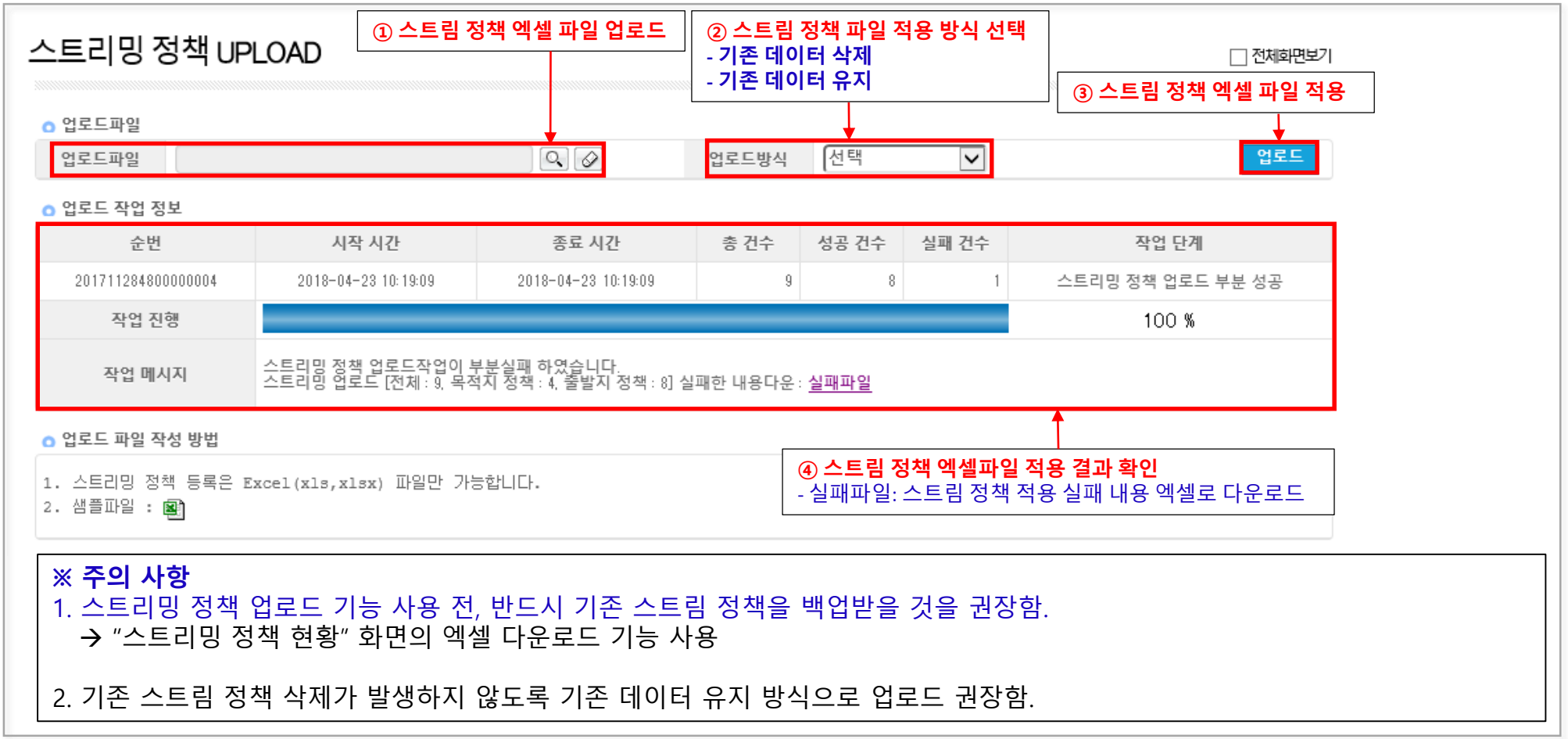
3. 스트림 연계 정책 다운로드

관리자는 관리자 웹페이지 **"스트리밍"** 메뉴의 **"스트리밍 정책 현황"** 화면에서 스트림 연계 정책을 엑셀파일로 다운로드할 수 있다.



4. 스트림 연계 정책 업로드

관리자 웹페이지 **"스트리밍"** 메뉴의 **"스트리밍 정책 UPLOAD"** 화면에는 관리자가 스트림 정책을 Excel 파일로 작성할 수 있도록 **스트림 정책 작성 샘플 파일**을 제공한다. **관리자는 다운로드 받은 엑셀파일에 스트림 정책을 작성**하고 "스트림 정책 UPLOAD" 화면을 에서 **엑셀파일을 업로드**하여 **스트림 정책을 적용**할 수 있다.



※ 주의 사항

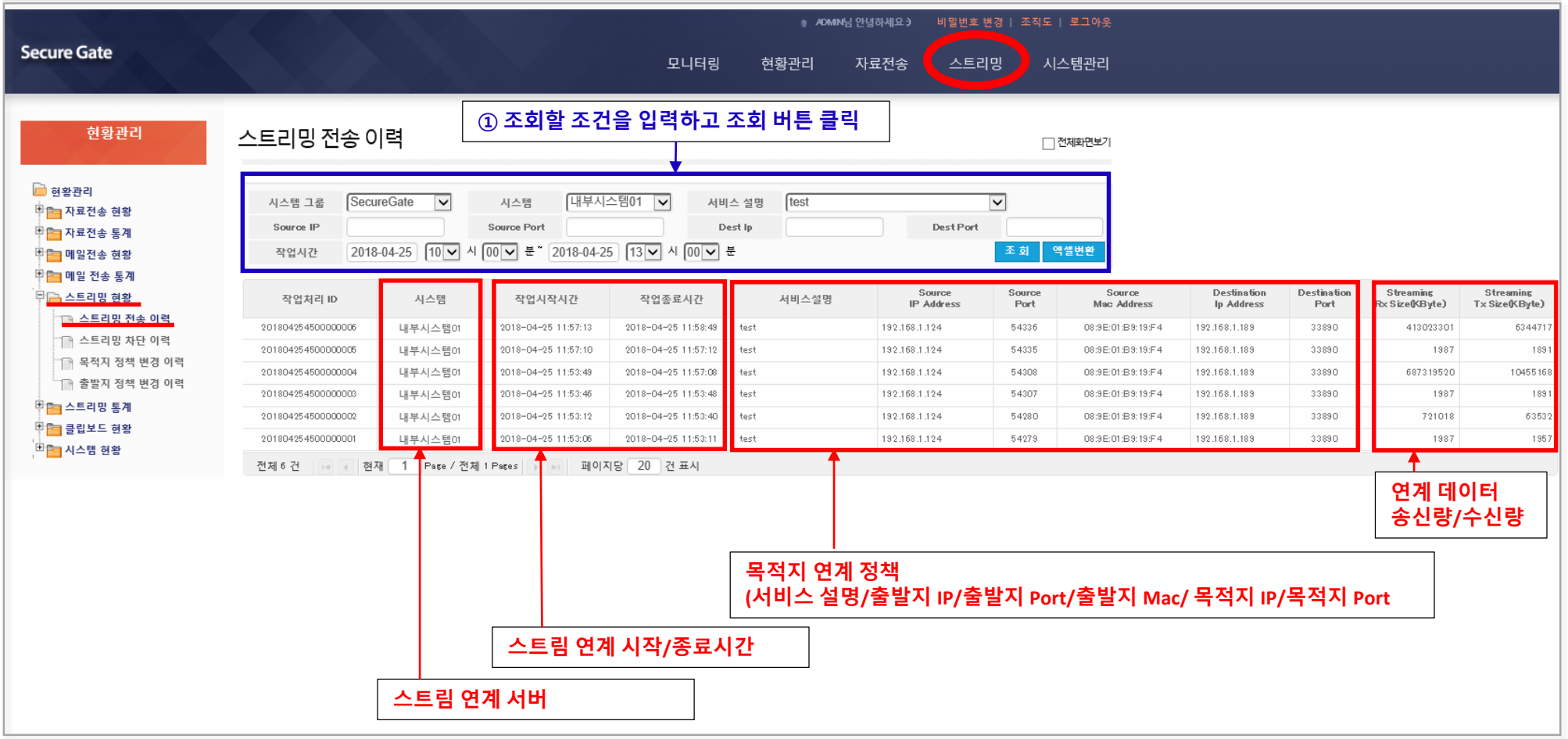
1. 스트리밍 정책 업로드 기능 사용 전, 반드시 기존 스트림 정책을 백업받을 것을 권장함.
   → "스트리밍 정책 현황" 화면의 엑셀 다운로드 기능 사용

2. 기존 스트림 정책 삭제가 발생하지 않도록 기존 데이터 유지 방식으로 업로드 권장함.

1. 연계 확인: 웹매니저 [1/3]

관리자 웹페이지 **"현황관리"** 메뉴의 **"스트리밍 현황"** 과 **"스트리밍 통계"** 에서 제공하는 화면에서 스트림 연계 데이터를 확인할 수 있다. 아래 화면은 **"스트리밍 현황"** 메뉴의 **"스트리밍 전송 이력 "** 화면을 예로 보여준다.

※ 스트리명 현황 데이트는 "목적지 정책 관리"의 "Log 기록여부"을 "DB기록"으로 설정해야 생성된다.
(Log 기록 저장은 시스템 용량에 많은 영향을 주며, 연동 확인 후 반드시 "Log 기록여부"을 "Log 미기록"으로 저장하도록 한다.)



2. 연계 확인: 콘솔접속 tsmon [2/3]

관리자는 **스트림 연계 서버 콘솔**에 접속하여 **tsmon (스트림 연계 실시간 모니터링 프로그램)**을 이용하여 스트림 연계 현황을 실시간으로 모니터링할 수 있다. (단, tsmon 기동은 단일 접속만 허용한다.)

root@securegate-in:~

```
[root@securegate-in netlog]# tsmon
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Hanssak Netstream Console. MultiVER 2.3.7 Mar 25 2018 11:47:52
Site Version: 0 IN
ARP Ver:0
NSC> p
  TCP 정책  현황          목적지                                          현재연결  접속거부   수신패킷       송신패킷
================ ================================================ ======= ======= ========== ==========
20180418420000001  192.168.001.189:33890 / 192.168.001.089:33890          1       0 12883521 18.185GB   5204171 283.426MB
20180419420000057 ~010.001.008.010:0 ------------------------------       0       0        0 0         0 0
20180419420000045 ~010.001.010.061:23                                     0       0        0 0         0 0
20180420420000027 ~010.001.010.061:23 ------------------------------       0       0        0 0         0 0
20180419420000046 ~010.001.010.061:35400                                  0       0        0 0         0 0
20180420420000028 ~010.001.010.061:35400 --------------------------       0       0        0 0         0 0
20180419420000026 ~010.001.010.061:35410                                  0       0        0 0         0 0
20180420420000007 ~010.001.010.061:35410 --------------------------       0       0        0 0         0 0
20180419420000039 ~010.001.010.061:45001                                  0       0        0 0         0 0
20180420420000020 ~010.001.010.061:45001 --------------------------       0       0        0 0         0 0
20180420420000044 ~172.016.000.162:25                                     0       0        0 0         0 0
20180420420000039 ~010.001.008.010:0 ------------------------------       0       0        0 0         0 0
20180420420000026  192.168.001.189:33890 / 192.168.001.089:33890          0       0        0 0         0 0
20180420420000045 ~192.168.001.188:5201 / 192.168.001.092:5201 ----       0       0   168843 9.118MB    994250 1.502GB
NSC>
```

① 스트림 연계 서버 콘솔 접속하고 tsmon 입력

② 정책별 데이터 송/수신량 출력 명령 입력

③ 목적지별로 현재연결 수/접속거부 / 수신패킷 / 송신패킷 출력

주요 명령어

- **s: 스트림 연계 환경정보**
  - ① 내/외부 스트림 연계 환경 (Link Up 정상)
  - ② 스트림 쓰레드 데이터 처리 양
  - ③ L4/gateway 정보
  - ④ 스트림 운영 설정 정보
- **a: 전체 트래픽 처리 실시간 모니터링**
  - ① 실시간 모니터링 중 "a" 입력하면 중지됨
- **p: 연계 정책별 송/수신량 출력**
- **r : 스트림 연계정책 출력**
- **d : 스트림 연계 디버깅 파일 생성**
  - ① 생성위치: /hrx/log/hrxlog/netlong에서 생성
  - ② d 입력하면 디버깅 프로토콜 출력
  - ③ d 프로토콜 입력하면 파일 생성시작. (예, d tcp)
  - ④ d 프로토콜 재입력하면 파일 생성종료 (예, d tcp)

NSC> d DBLOG

DBLOG on

NSC> d DBLOG

DBLOG off

3. 연계 확인: 콘솔접속 tcpdump [3/3]

관리자는 **스트림 연계 서버 콘솔**에 접속하여 **tcpdump 명령어를** 이용하여 사용하여 스트림 연계 패킷데이터를 모니터링 할 수 있다. 아래의 예는 아웃바운드 정책 (내부 서버 → 내부 스트림 연계 서버(192.168.1.189/33890) → 외부 스트림 연계 서버 → 외부 서버 (192.168.1.89/33890)의 예이다. (tcpdump 명령은 root 계정에서만 사용할 수 있다.)

[내부 스트림 연계 서버] 스트림 연계 서버(192.168.1.189)의 33890 포트로 들어 패킷을 덤프함.

```
[root@securegate-in ~]# tcpdump -nni bond0 host 192.168.1.189 and port 33890
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bond0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:46:12.590309 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [S], seq 2674918410, win 8192, options [mss 1460,nop,wscale 2,no
p,nop,sackOK], length 0
09:46:12.592826 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [S.], seq 2615330632, ack 2674918411, win 8192, options [mss 146
0,nop,wscale 8,nop,nop,sackOK], length 0
09:46:12.593354 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [.], ack 1, win 16425, length 0
09:46:12.593996 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [P.], seq 1:20, ack 1, win 16425, length 19
09:46:12.599646 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [.], ack 20, win 256, length 0
09:46:12.599650 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [P.], seq 1:20, ack 20, win 256, length 19
09:46:12.800205 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [.], ack 20, win 16420, length 0
09:46:14.859984 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [P.], seq 20:146, ack 20, win 16420, length 126
09:46:14.863386 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [P.], seq 20:845, ack 146, win 256, length 825
09:46:14.866003 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [P.], seq 146:472, ack 845, win 16214, length 326
09:46:14.875399 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [P.], seq 845:904, ack 472, win 254, length 59
09:46:14.877840 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [P.], seq 472:557, ack 904, win 16199, length 85
09:46:14.881111 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [P.], seq 904:1149, ack 557, win 254, length 245
09:46:14.884394 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [P.], seq 557:1394, ack 1149, win 16138, length 837
09:46:14.888687 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [P.], seq 1149:1490, ack 1394, win 251, length 341
09:46:14.890204 IP 192.168.1.124.54918 > 192.168.1.189.33890: Flags [F.], seq 1394, ack 1490, win 16425, length 0
09:46:14.892794 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [.], ack 1395, win 251, length 0
09:46:14.892797 IP 192.168.1.189.33890 > 192.168.1.124.54918: Flags [R.], seq 1490, ack 1395, win 0, length 0
```

[외부 스트림 연계 서버] 외부 최종 목적지(192.168.1.89)의 33890 포트로 나가는 패킷을 덤프함.

```
[root@securegate-ex ~]# tcpdump -nni bond0 dst 192.168.1.89 and port 33890
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bond0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:46:12.284860 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [S], seq 2674918410, win 8192, options [mss 1460,nop,wscale 2,nop
,nop,sackOK], length 0
09:46:12.287912 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [.], ack 2615330633, win 16425, length 0
09:46:12.288538 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [P.], seq 0:19, ack 1, win 16425, length 19
09:46:12.494875 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [.], ack 20, win 16420, length 0
09:46:14.554509 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [P.], seq 19:145, ack 20, win 16420, length 126
09:46:14.560541 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [P.], seq 145:471, ack 845, win 16214, length 326
09:46:14.572385 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [P.], seq 471:556, ack 904, win 16199, length 85
09:46:14.578920 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [P.], seq 556:1393, ack 1149, win 16138, length 837
09:46:14.584878 IP 192.168.1.188.12302 > 192.168.1.89.33890: Flags [F.], seq 1393, ack 1490, win 16425, length 0
```

주요 명령어

- **tcpdump –nni bond0 host IP1 and port PORT1**
  → 본딩 인터페이스에서 host IP IP1 의 PORT1 포트로 발생하는 패킷을 덤프
- **tcpdump –nni bond0 dst IP1 and port PORT1**
  → 본딩 인터페이스에서 목적지IP IP1 의 PORT1 포트로 발생하는 패킷을 덤프
- **tcpdump –nni bond0 src IP1 and port PORT1**
  → 본딩 인터페이스에서 출발지 IP IP1의 PORT1 포트로 발생하는 패킷을 덤프
- **tcpdump –nni bond0 src IP1 or dst IP2 and port PORT1 or port PORT2**
  → 본딩 인터페이스에서 출발지 IP IP1 또는 목적지 IP IP2이고 포트가 PORT1이거나 PORT2에서 발생하는 패킷을 덤프
- **tcpdump –nni bond0 host IP1 and not host IP2 and port PORT1 and not port PORT2**
  → 본딩 인터페이스에서 호스트 IP 가 IP2를 제외한 IP1이고 포트는 PORT2를 제외한 PORT1에서 발생하는 패킷을 덤프