
방화벽교육자료

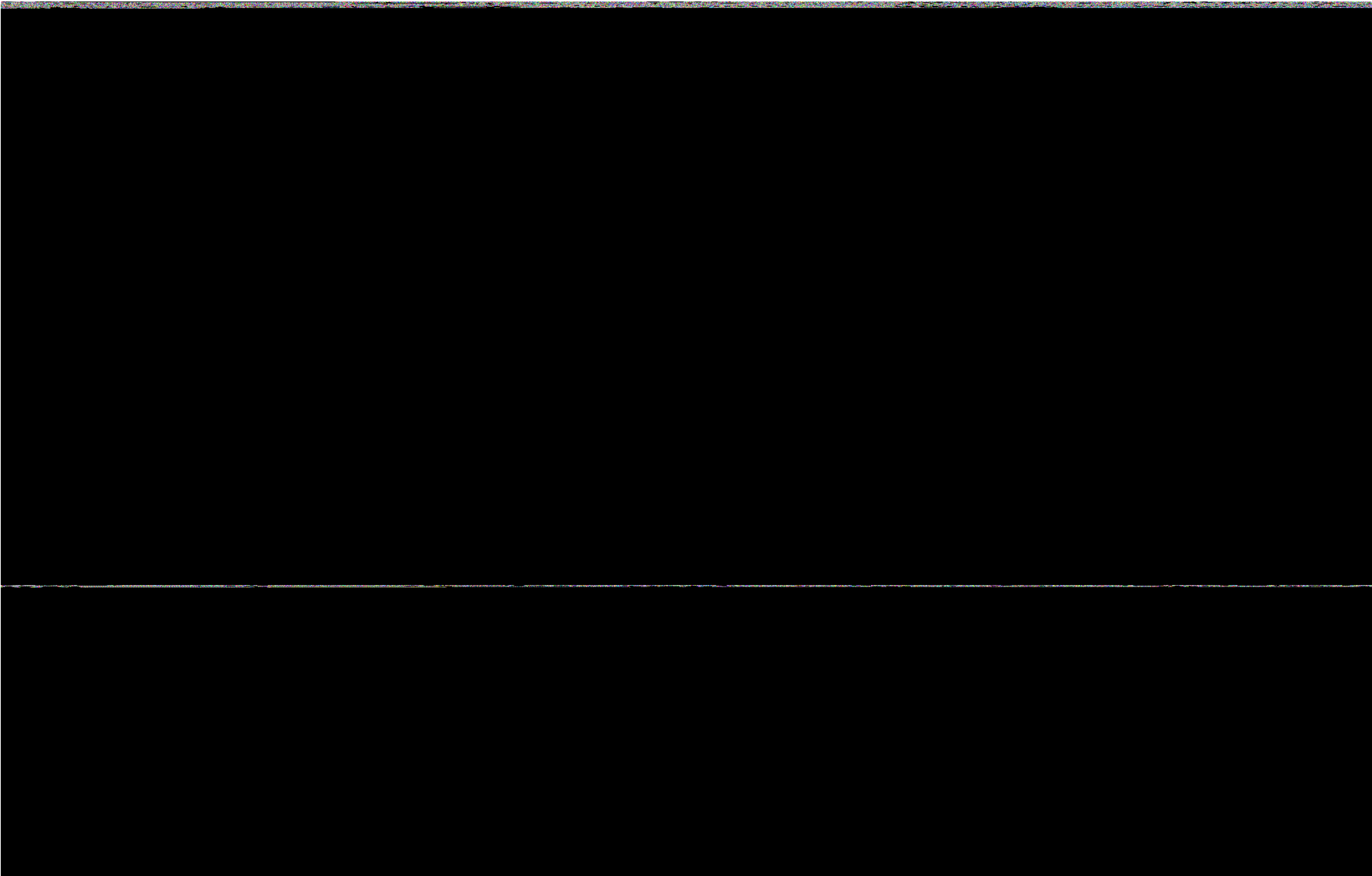
AhnLab TrusGuard

2024. 09

목차

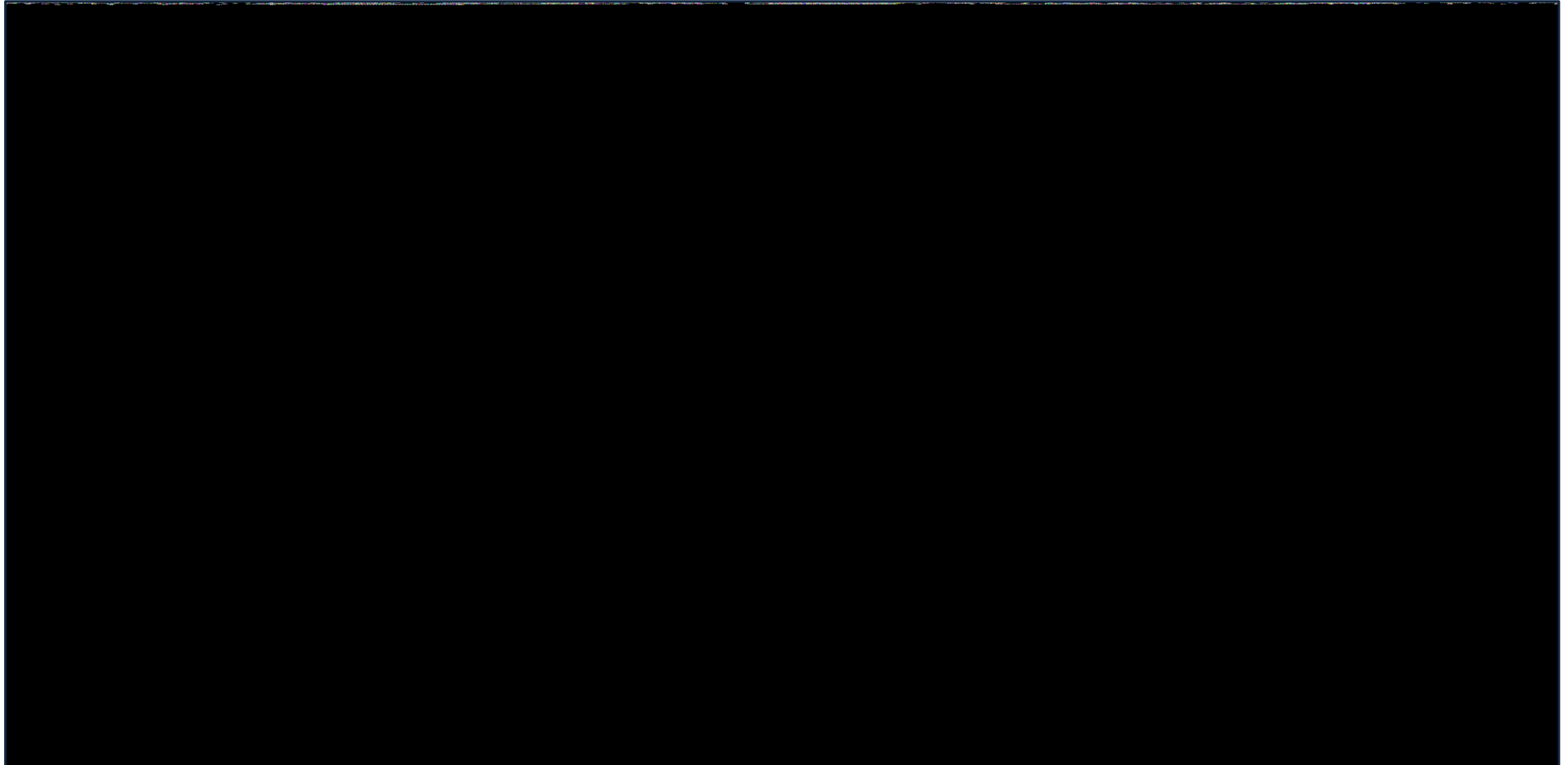
- TrusGuard – 제품 소개
 - TrusGuard – 장비 접속
 - TrusGuard – DashBoard
 - TrusGuard – Network
 - TrusGuard – Object
 - TrusGuard – System
 - TrusGuard – Policy
 - TrusGuard – VPN
 - TrusGuard – Log & Report
 - TrusGuard – 설정적용 및 동기화
 - TrusGuard – 장애 대응
-

제품 소개



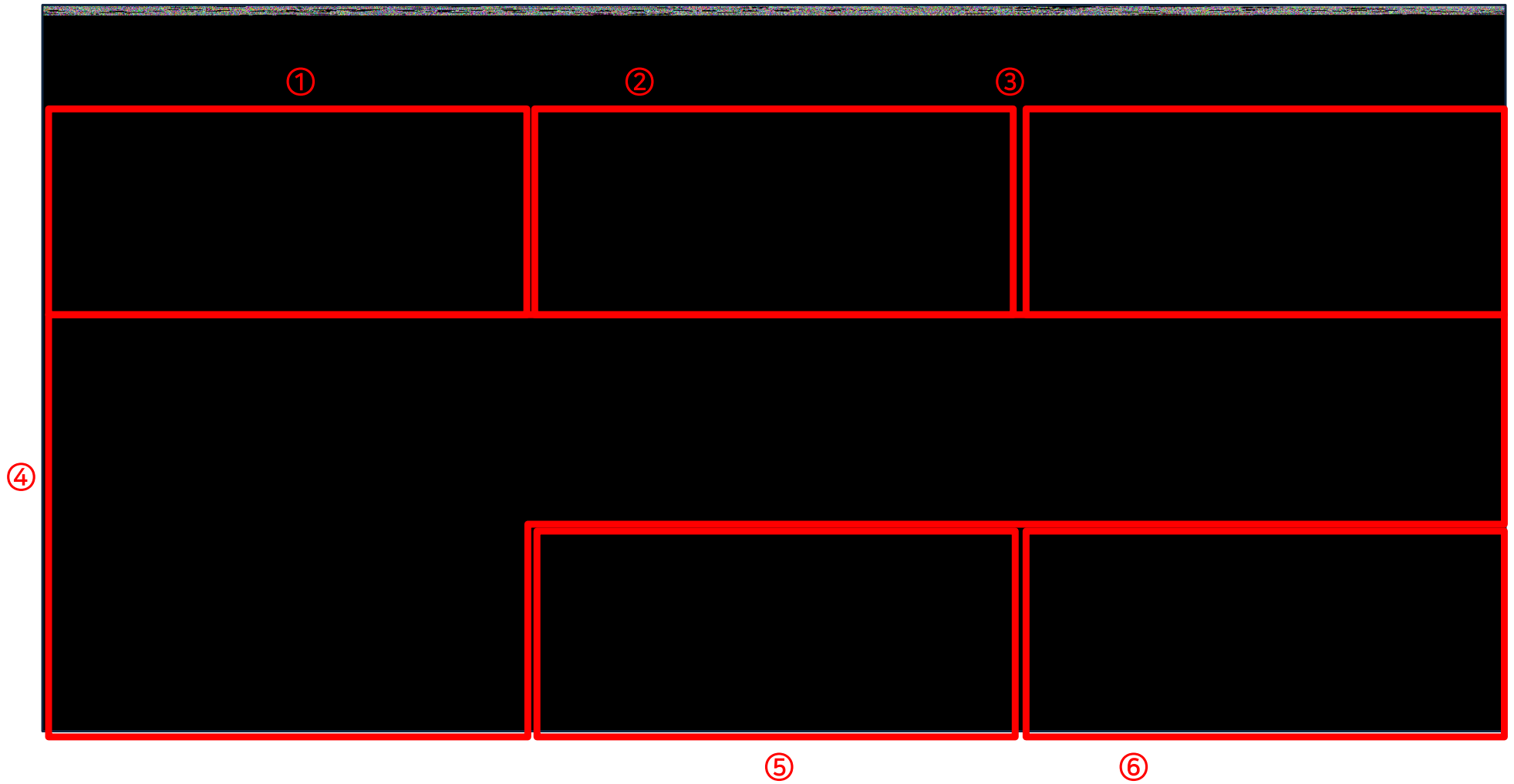
장비 접속

- ❖ 브라우저 주소 창에 https://[장비 IP]:50005를 입력하고 접속
- ❖ "이 웹사이트를 계속 탐색합니다(권장하지 않음)." 클릭 후 장비 접속



- 로그인 화면이 나타나면 아이디와 비밀번호를 입력하고 로그인을 클릭
- 로그인 정보 잘못 입력할 시 계정 잠김 주의

DashBoard

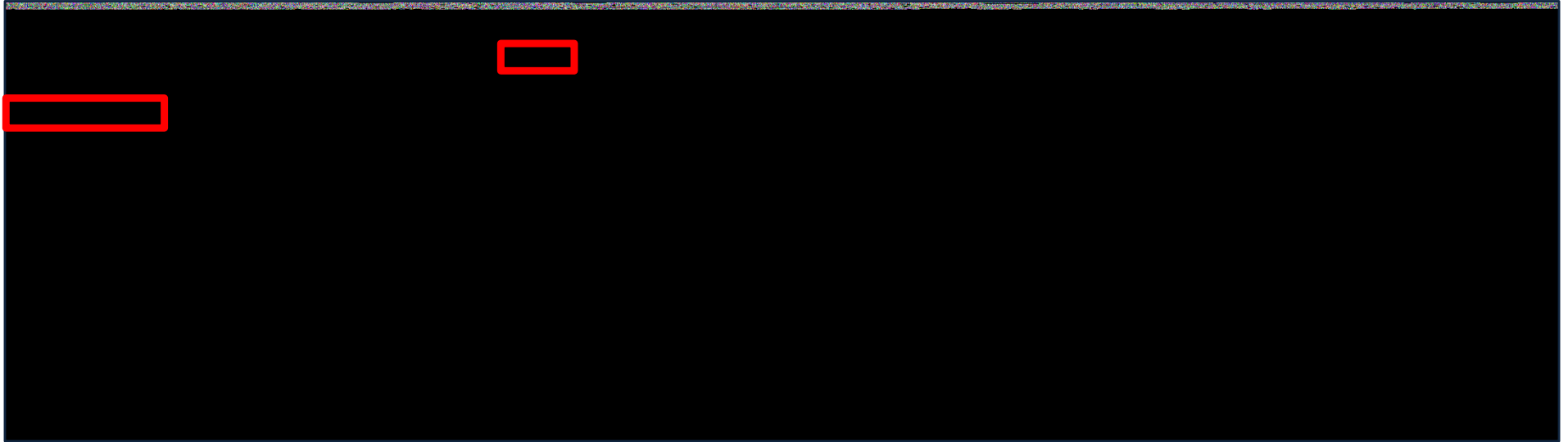


DashBoard

- ① 시스템 정보 : 장비 Host name, 방화벽 라이선스, 라이선스 기반 업데이트 정보, 펌웨어 버전, HA 사용 여부에 대한 정보 확인
- ② 네트워크 포트 : 실시간 물리적 장비 Link 상태 확인
- ③ 시스템 리소스 : 실시간 CPU, 메모리, Disk 사용량 확인 및 경보 조건 메뉴에서 사용량 임계치 지정 가능
- ④ 트래픽 : 포트별, 프로토콜별 시간별 트래픽 확인
- ⑤ 이벤트 로그 : 실시간으로 가장 최근에 수집된 이벤트 로그 현황 표시
- ⑥ 관리자 접속 정보 : 장비에 접속한 관리자 현황 확인
HA로 구성된 장비일 경우, 별도 표시

Network

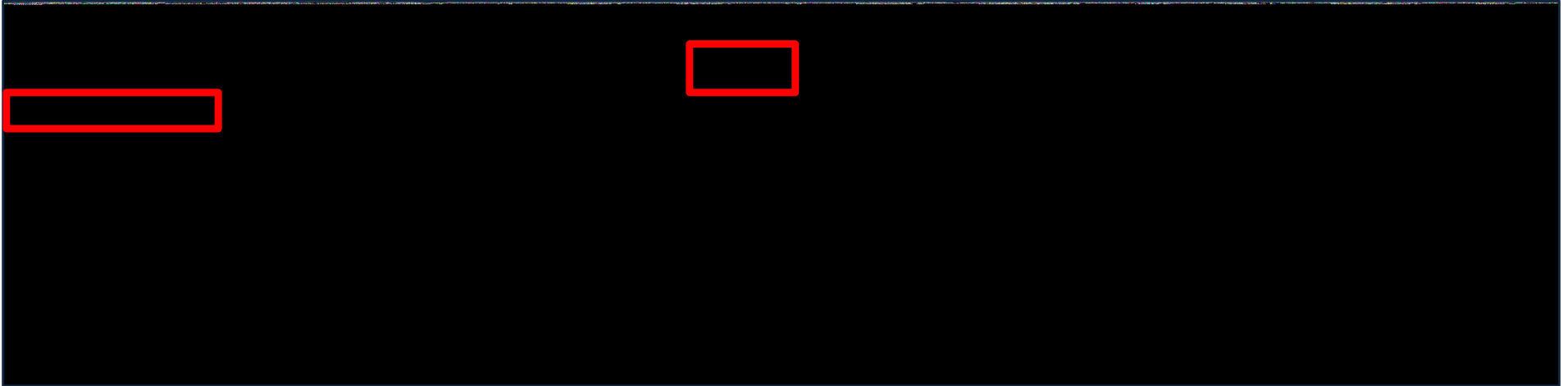
❖ Network → 인터페이스



- 시스템을 운영할 네트워크의 구성과 특성을 고려하여 네트워크 인터페이스를 구성
- 장비 Interface 설정
- 수정 버튼을 클릭 후 해당 Interface 의 IP 정보, Prefix 및 유형 설정
- Interface Duplex/Speed 와 장비 접속 프로토콜, ICMP 허용 여부 등 설정
- 포트 링크 상태와 트래픽의 대략적인 정보 확인 가능

Network

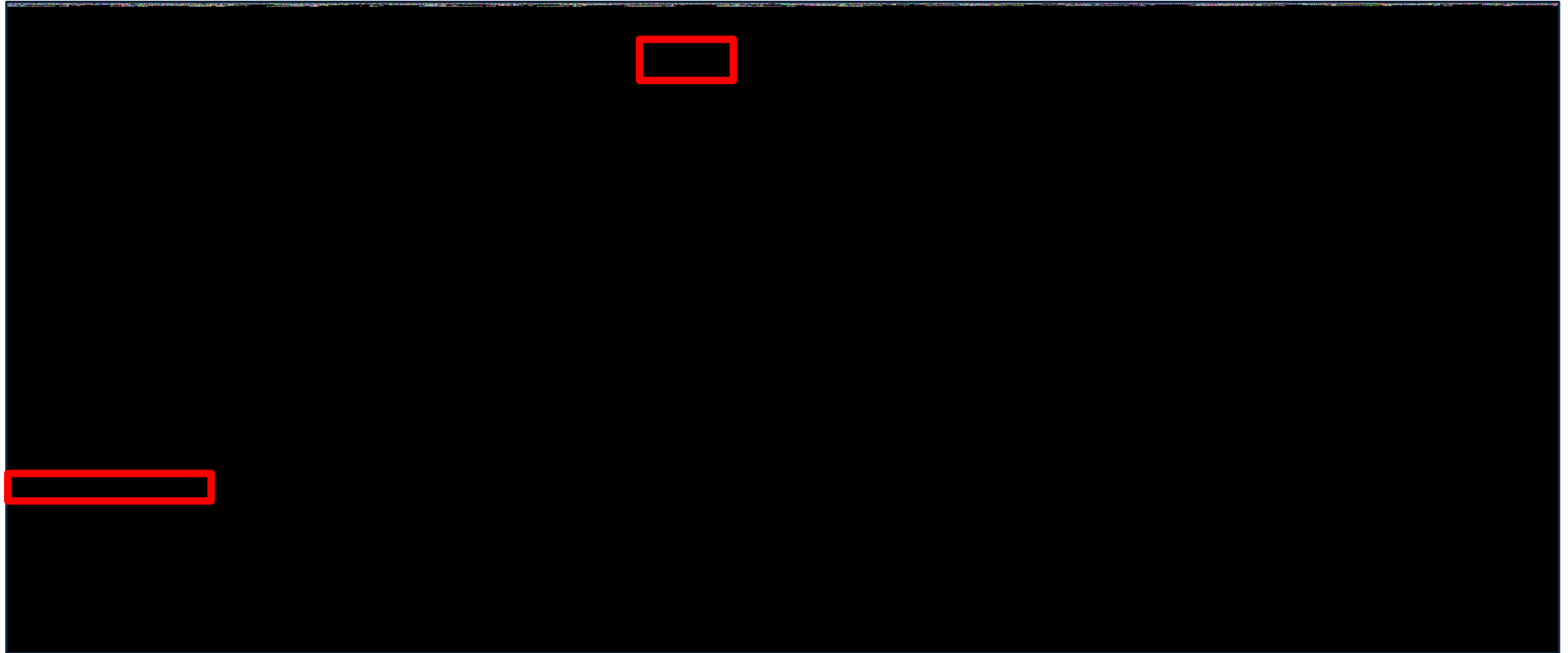
❖ Network → 라우팅 → IPv4 라우팅



- 라우팅 추가, 확인 및 검색 가능
- 기본 라우팅(Default Gateway), 목적지 라우팅, 출발지 라우팅, 정책 기반 라우팅 설정 가능
- 출발지 IP 주소, 게이트웨이, 목적지 IP 주소, 네트워크 포트 별 설정 내역 검색 가능

Network

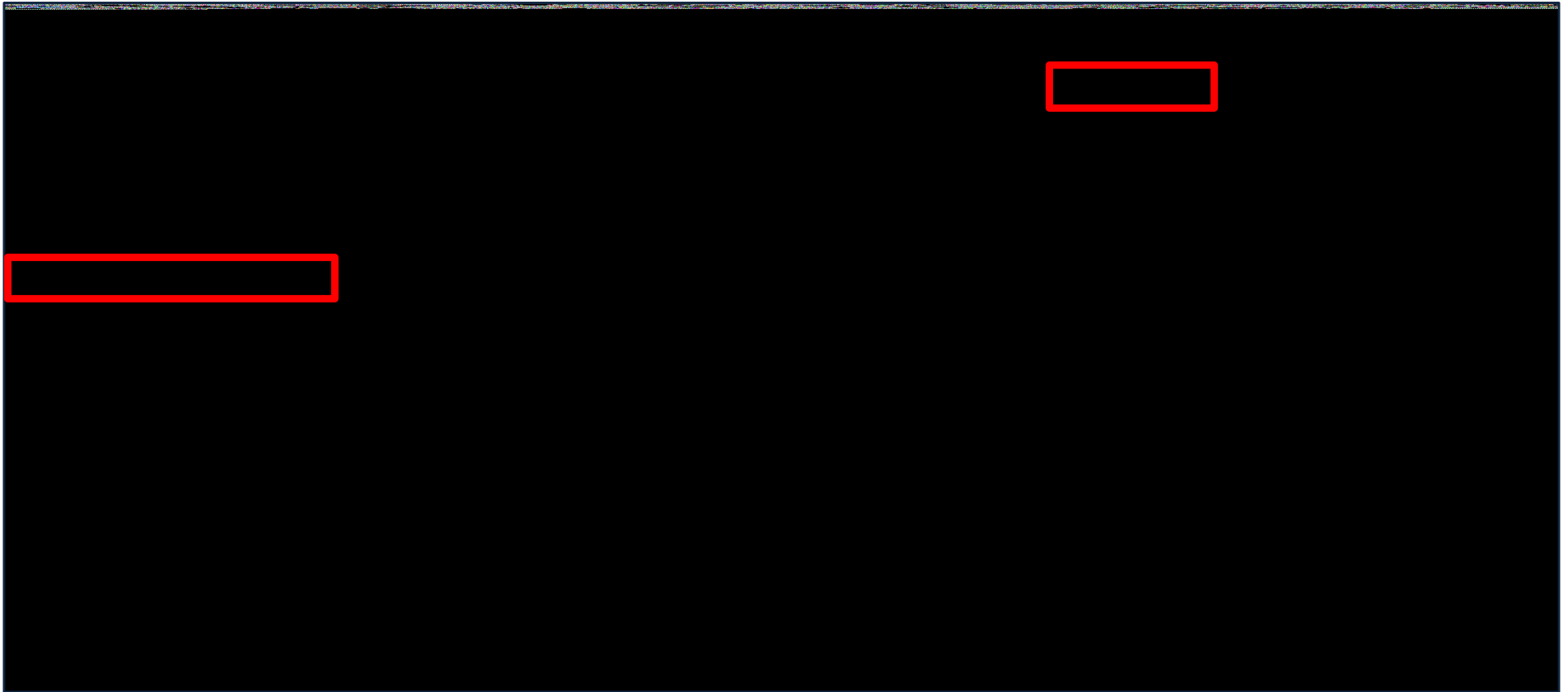
❖ Network → HA → HA 인터페이스



- HA 서비스에 사용할 네트워크 인터페이스를 구성
- 동일한 그룹 아이디를 할당 받은 HA 구성원끼리 장애 대응
- HA 작동 상태 확인 가능

Network

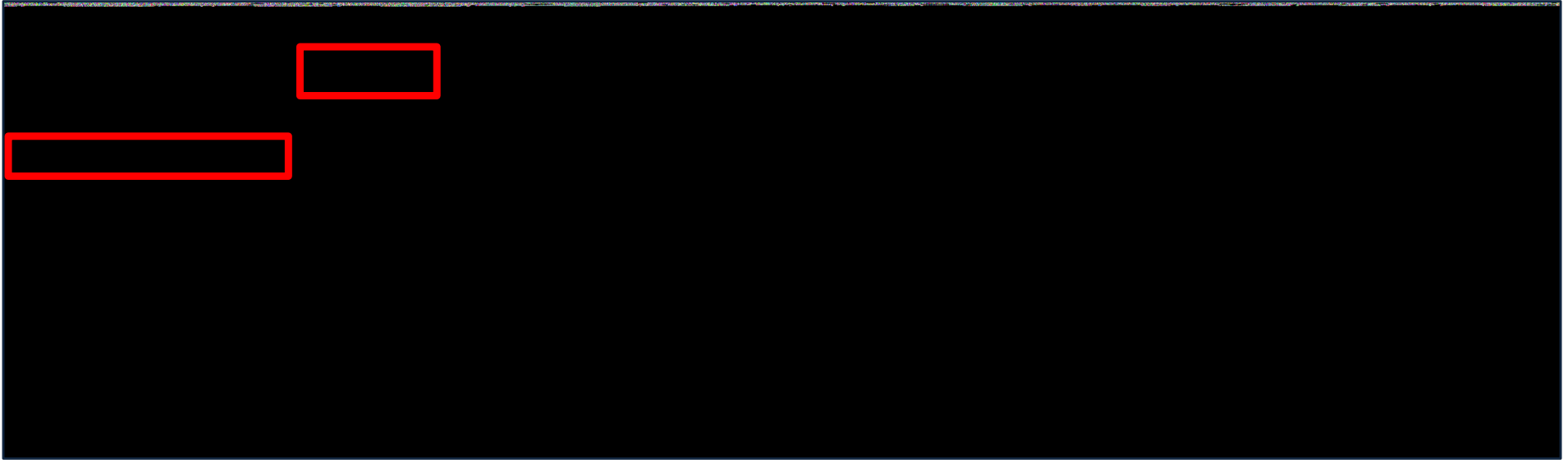
❖ Network → HA → HA 설정



- 이중화 된 2대의 장비 정책 등의 동기화를 위해 사용
- 우선 순위 숫자가 작은 쪽이 Master, 큰 쪽이 Slave 구성
- 일반적으로 별도 포트를 사용하여 다이렉트로 연결

Object

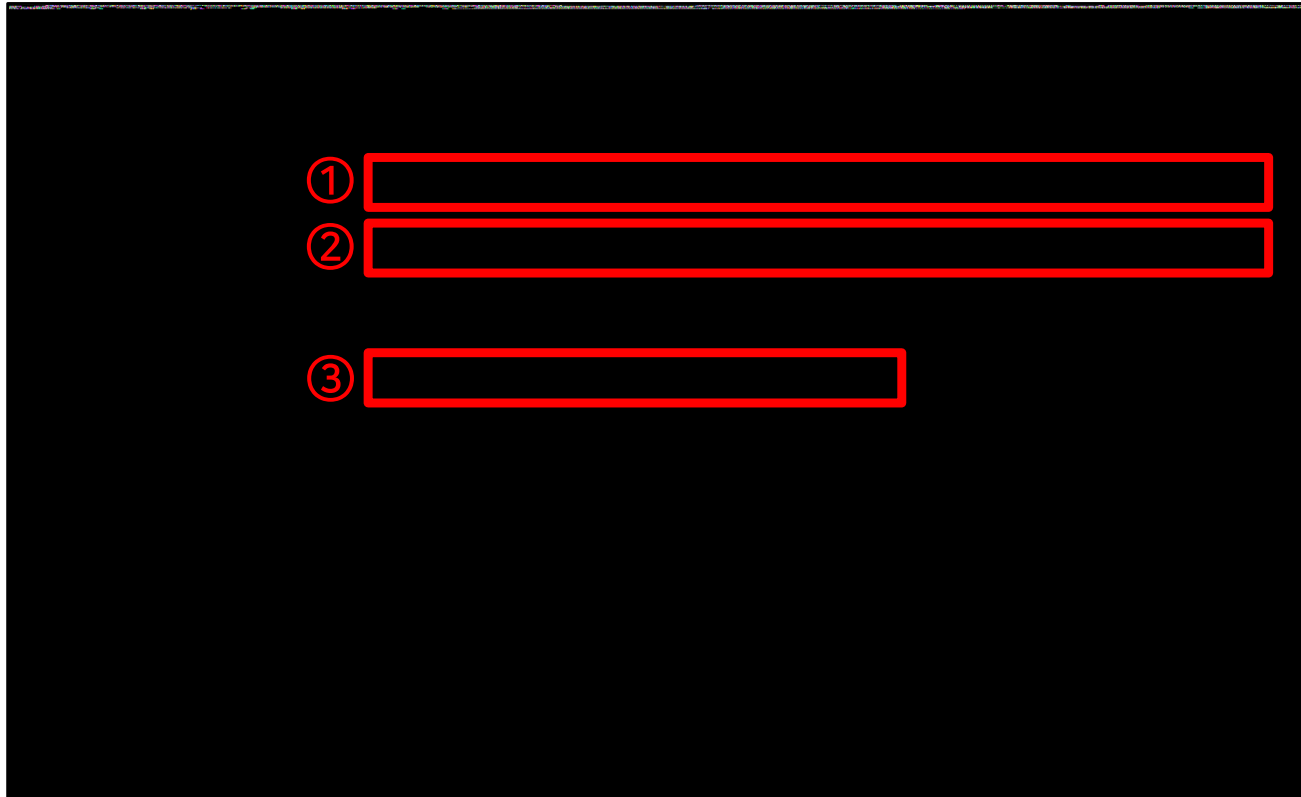
❖ Object → IPv4 주소 → IPv4 주소 목록



- 방화벽 정책, NAT, 정책 예외, VPN에 들어갈 IP 객체 생성 (좌측 "+" 버튼 클릭)
- 단일 IP, 네트워크 대역, 구간 별로 IP 생성 가능
- 만들어진 IP 객체들을 이름, 종류, IP 주소, 네트워크 포트, 보안 등급 별로 검색 가능

Object

❖ Object → IPv4 주소 → IPv4 주소 객체 추가



①

②

③

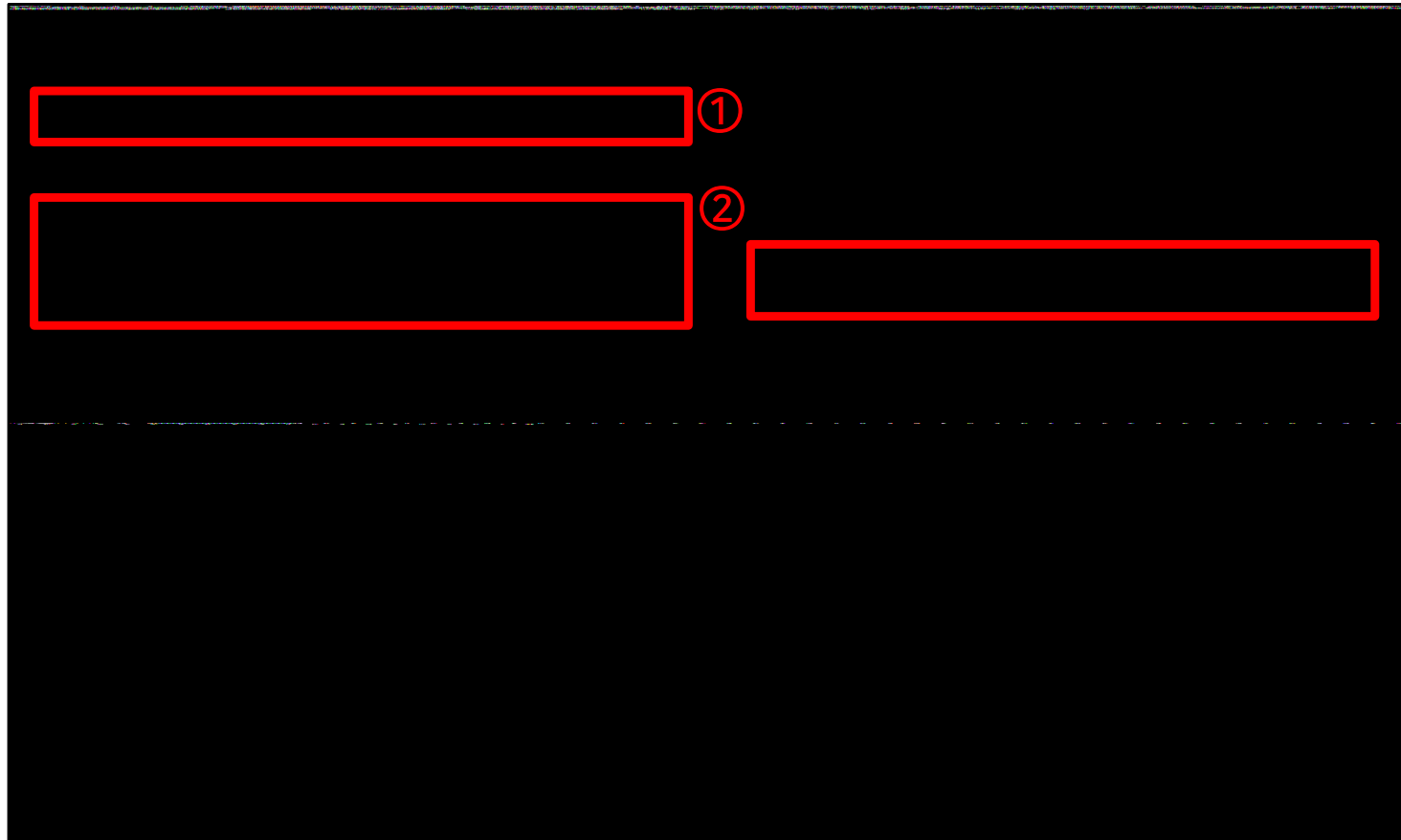
① 이름 : IP 객체 이름 지정

② IPv4 주소 : 단일 IP (10.10.10.1/32), IP 범위 시작과 끝 (10.10.10.1-10.10.10.10), 네트워크 ID와 Subnetmask 설정 (10.10.10.0/24)

③ 인터페이스 : 방화벽 기준 해당 객체가 있는 interface 구간 선택 (all 선택)

Object

❖ Object → IPv4 주소 → IPv4 주소 그룹



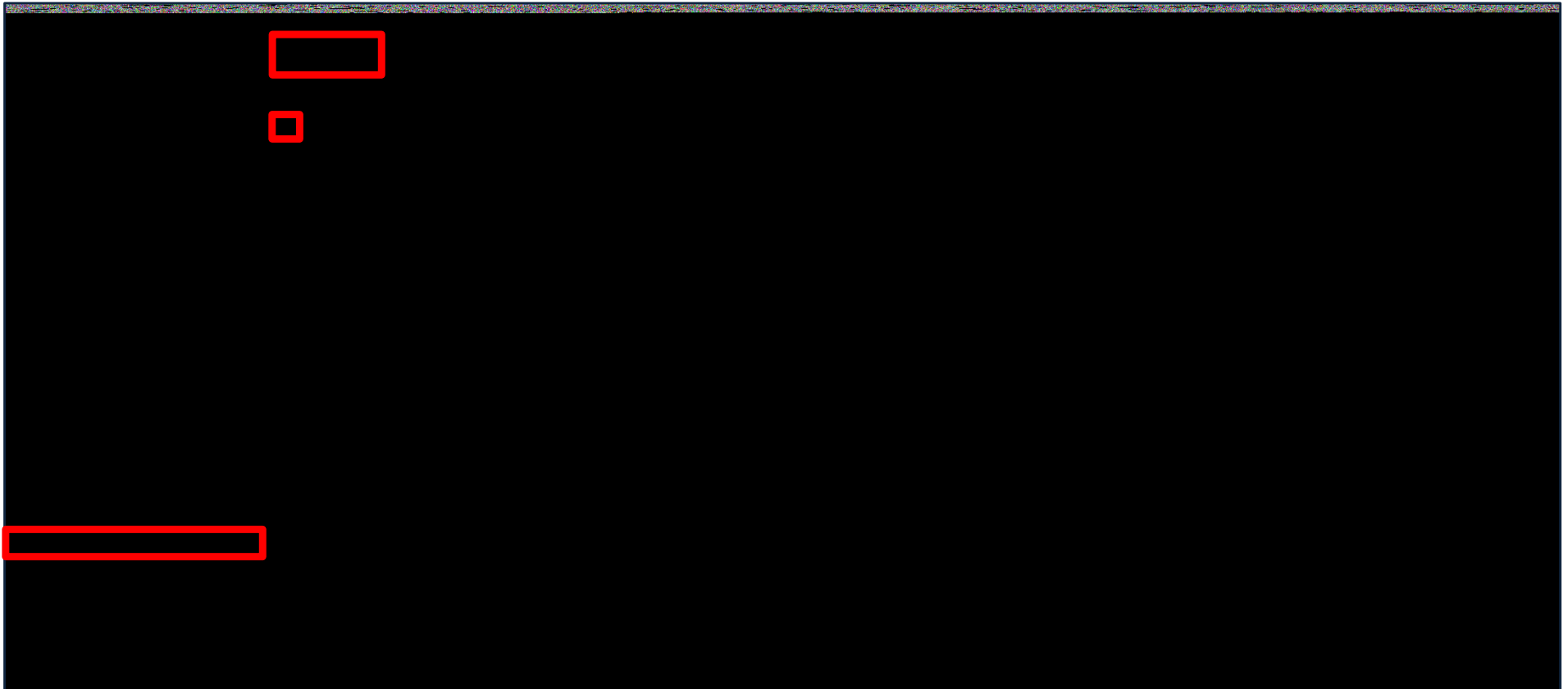
- 할당 된 IP 객체를 그룹으로 묶는 설정

① 그룹 이름 : 원하는 그룹 이름 지정

② 그룹 구성 : 그룹으로 묶을 객체 선택 후 화살표 아이콘 선택하여 구성원으로 추가

Object

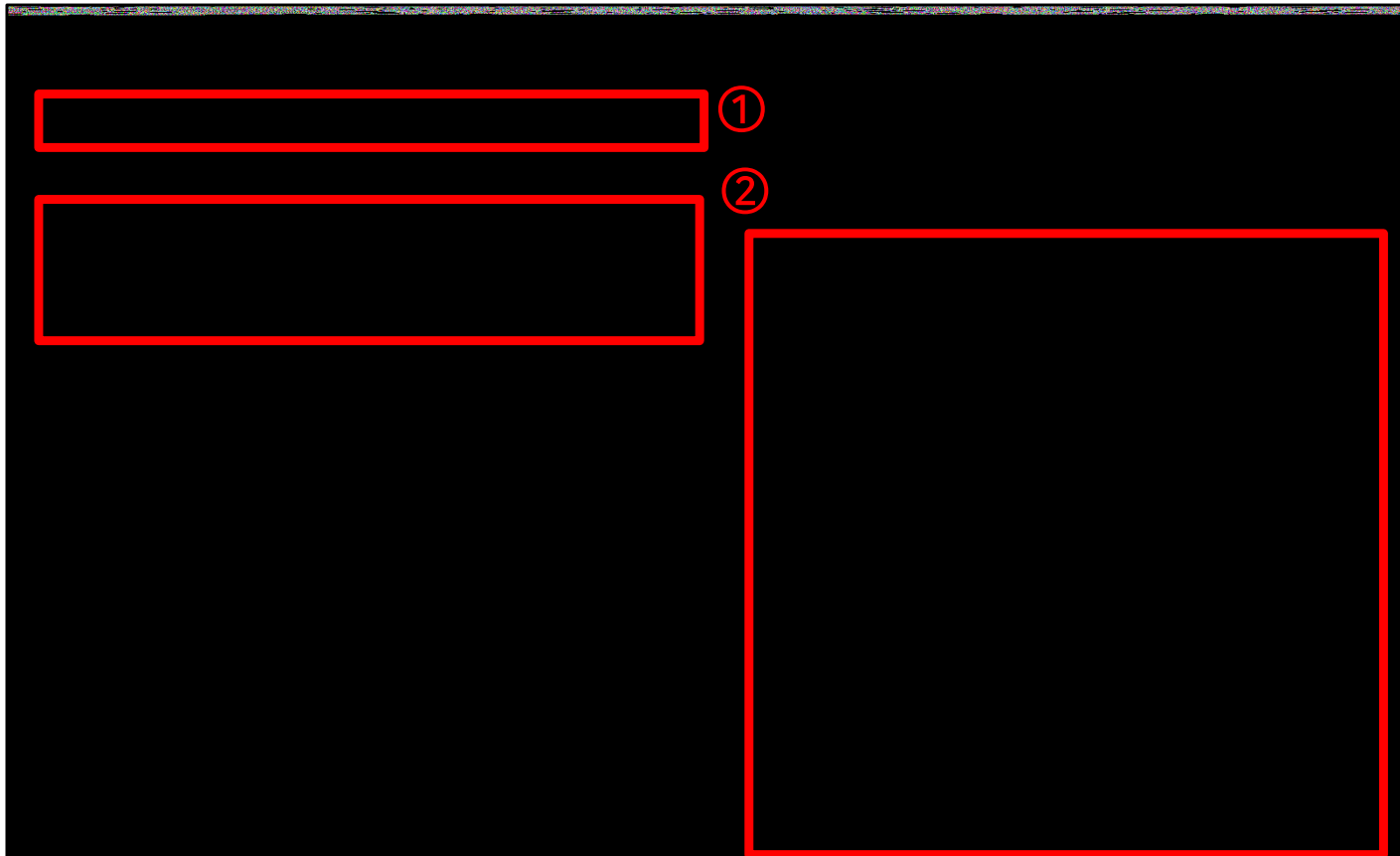
❖ Object → 서비스 → 서비스 목록



- 프로토콜, 포트, 세션 타임아웃을 정의하는 객체 생성
- 포트번호 1-65535 설정 가능, 세션 타임아웃 (TCP : 1800초, UDP : 30초, ICMP : 30초, IP : 600초)
- 좌측 "+" 버튼 클릭 후 방화벽 정책, IPS 규칙에 들어갈 서비스 객체 생성

Object

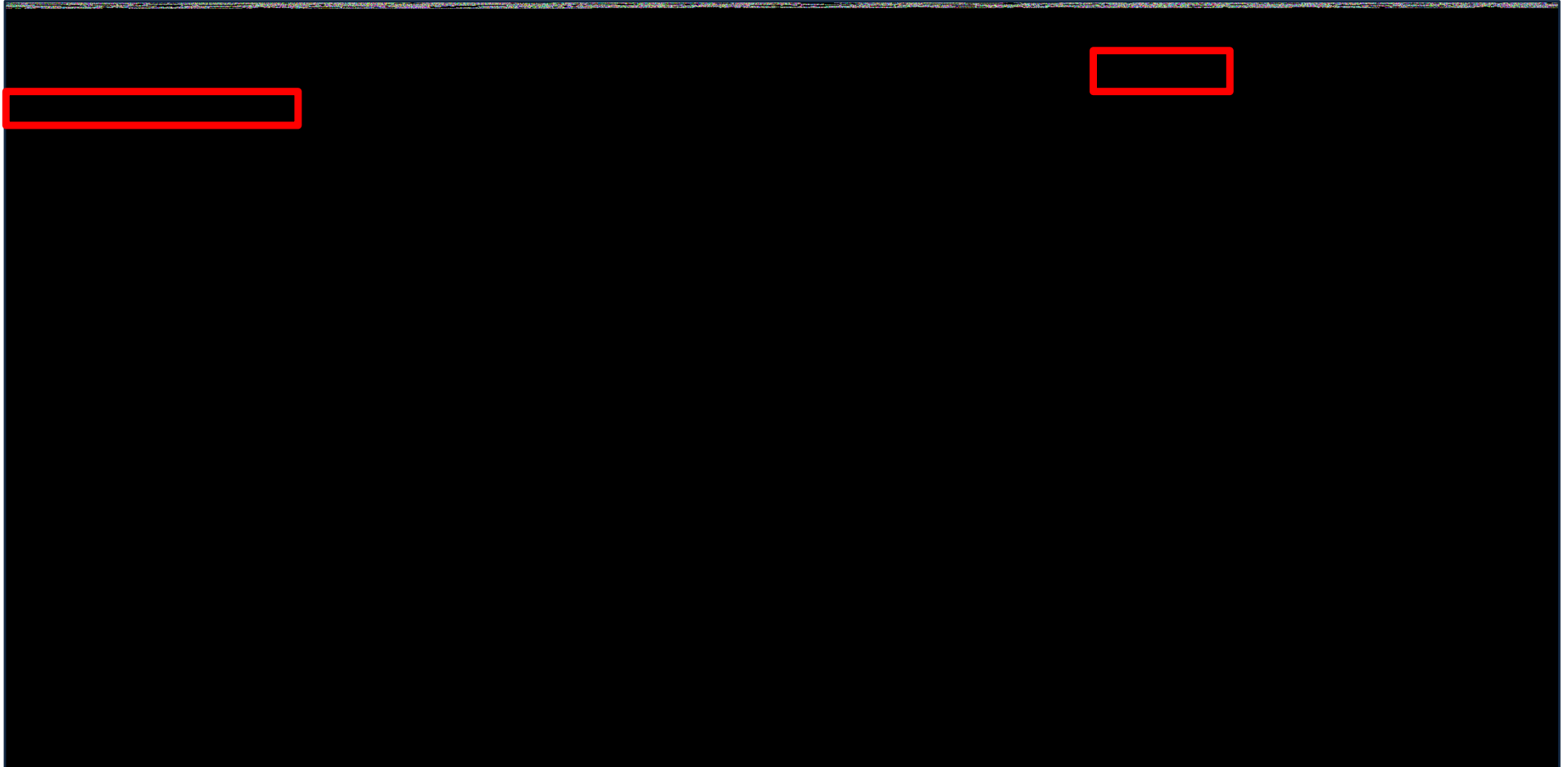
❖ Object → 서비스 → 서비스 그룹



- 할당 된 서비스 객체를 그룹으로 묶는 설정
- ① 그룹 이름: 원하는 그룹 이름 지정
- ② 그룹 구성: 그룹으로 묶을 객체 선택 후 화살표 아이콘 선택하여 구성원으로 추가

System

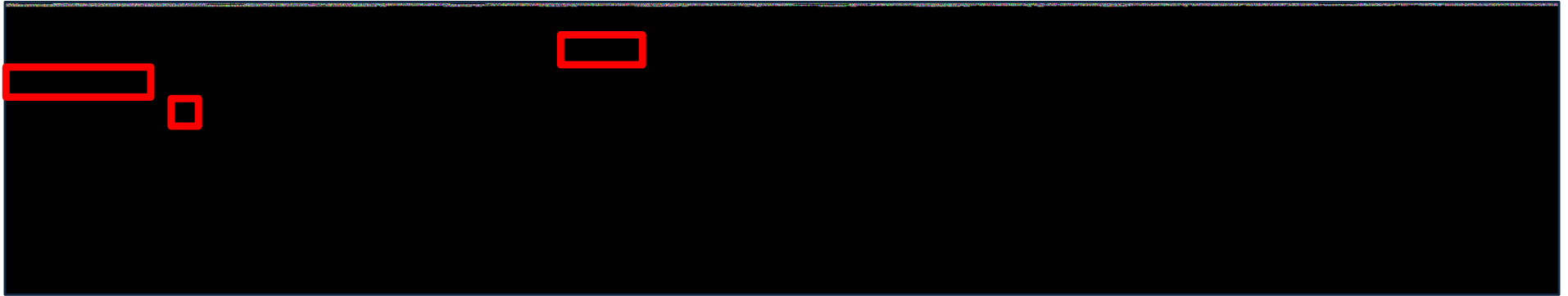
❖ System → 시스템 정보 → 호스트 이름



- 호스트 이름 수정, 시스템 시간 확인 및 NTP 서버 동기화 (설정 후 하단 저장 클릭)
- 동기화 시간은 로그 서버의 로그 기록 시간으로 표시
- 동기화 자동 업데이트 시간 설정

System

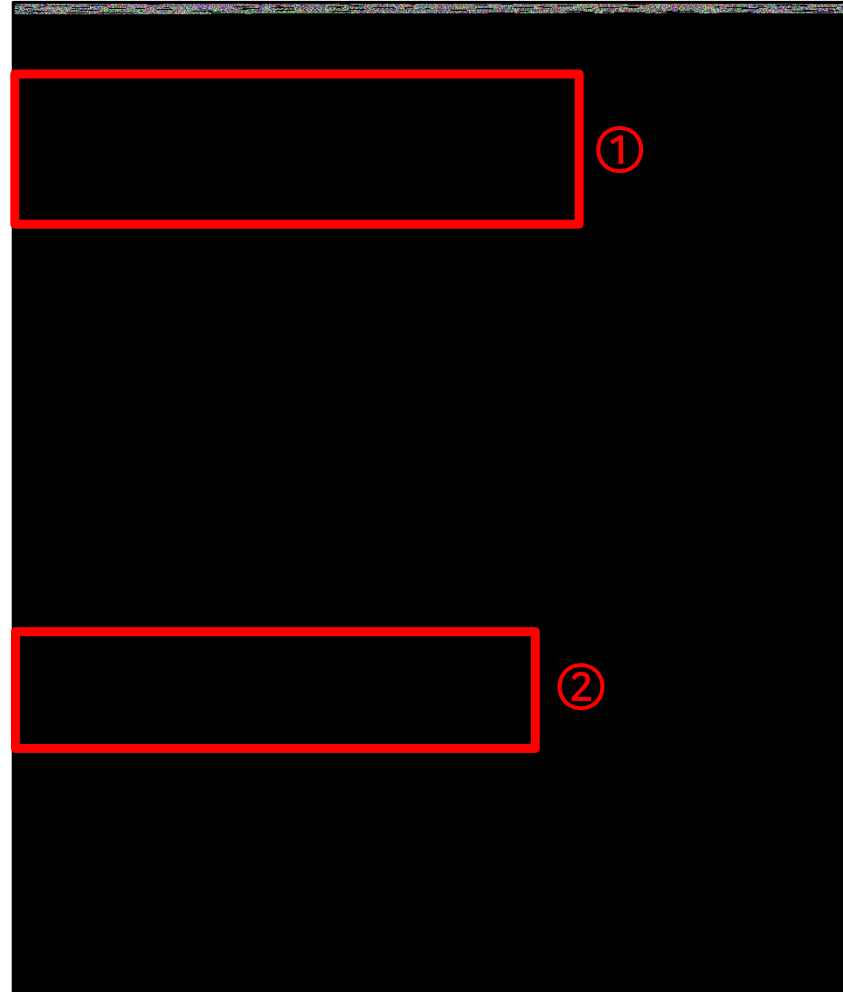
❖ System → 관리자 → 관리자 계정



- 장비에 로그인할 수 있는 계정 등록 및 관리 (기본계정 : admin)
- 계정 유형, 인증 방법, 마지막 로그인 시간, 계정 상태, 유효기간 등 확인 가능
- 권한에 따라 시스템 관리자 (모든 권한), 읽기 관리자 (읽기 권한), 정책 관리자 (선택한 정책에 대해서만 읽기, 추가, 수정, 삭제 등 권한)
- 좌측 "+" 버튼 클릭 후 관리자 계정 추가 가능

System

❖ System → 관리자 → 관리자 계정 추가

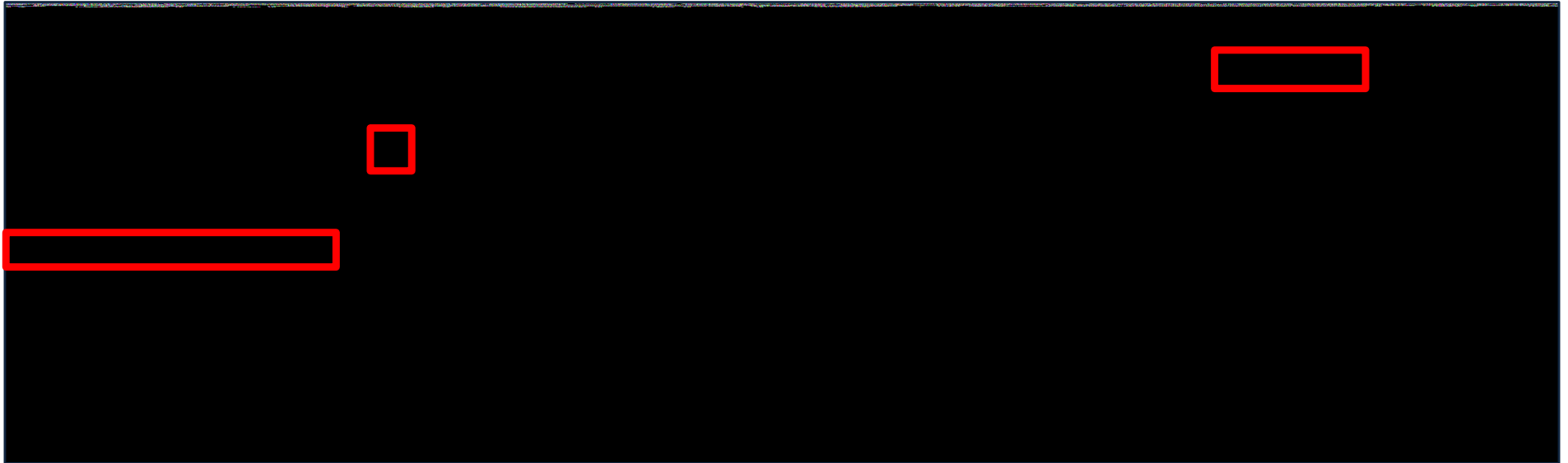


① 아이디, 비밀번호, 변경 주기, 계정 유형, 로그 허용 횟수, 잠금 시간 등 설정
(변경 주기 0일 설정 시 변경 불필요, 허용 회수 및 잠금 시간 : 기본 3회 / 5분)

② 로그인 허용 IP 설정 시 해당 IP 외 접근 불가

System

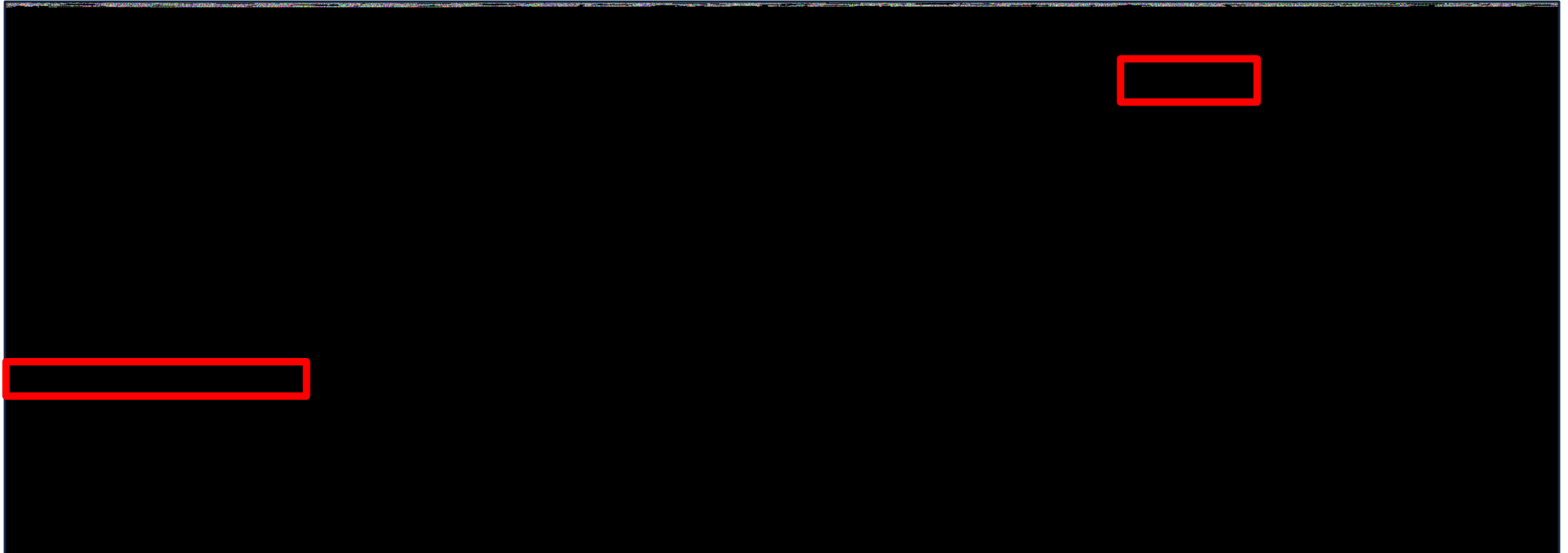
❖ System → 관리자 → 관리자 IP 주소



- 관리자 접근 가능 IP 주소 수정 및 추가
- 방화벽 접근 허용 단일 IP 주소 및 Network 주소 입력
- 좌측 "+" 버튼을 눌러 방화벽 접근 가능한 IP 추가

System

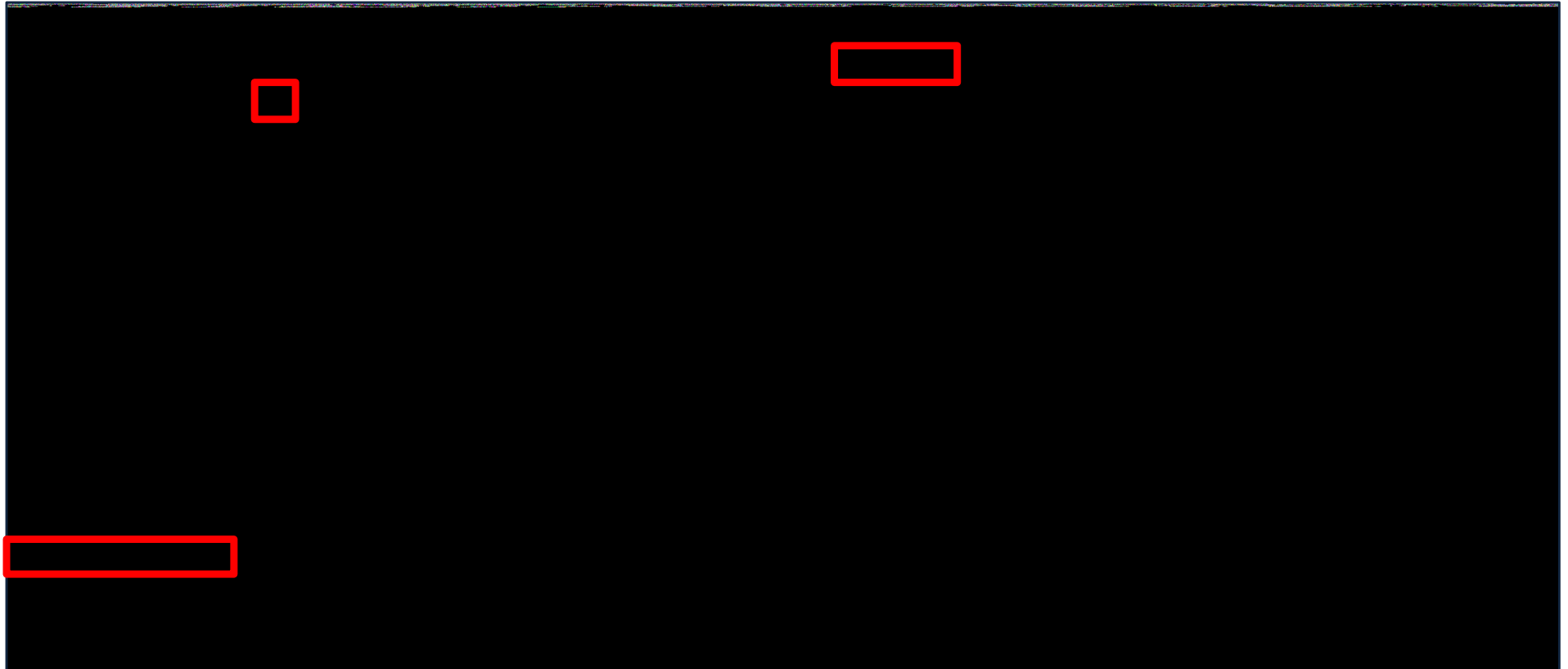
❖ System → 관리자 → 접속 관리



- 웹 화면 및 터미널 접속에 대한 접속 포트, 세션 타임아웃 시간 설정
- 웹 접속 포트 50005(기본), 터미널 접속 포트 22(기본)
30000-39999(설정 가능 포트)
- 웹 세션 타임아웃 600초(기본), 터미널 세션 타임아웃 1800초(기본)
60-86400초(설정 가능 시간)

System

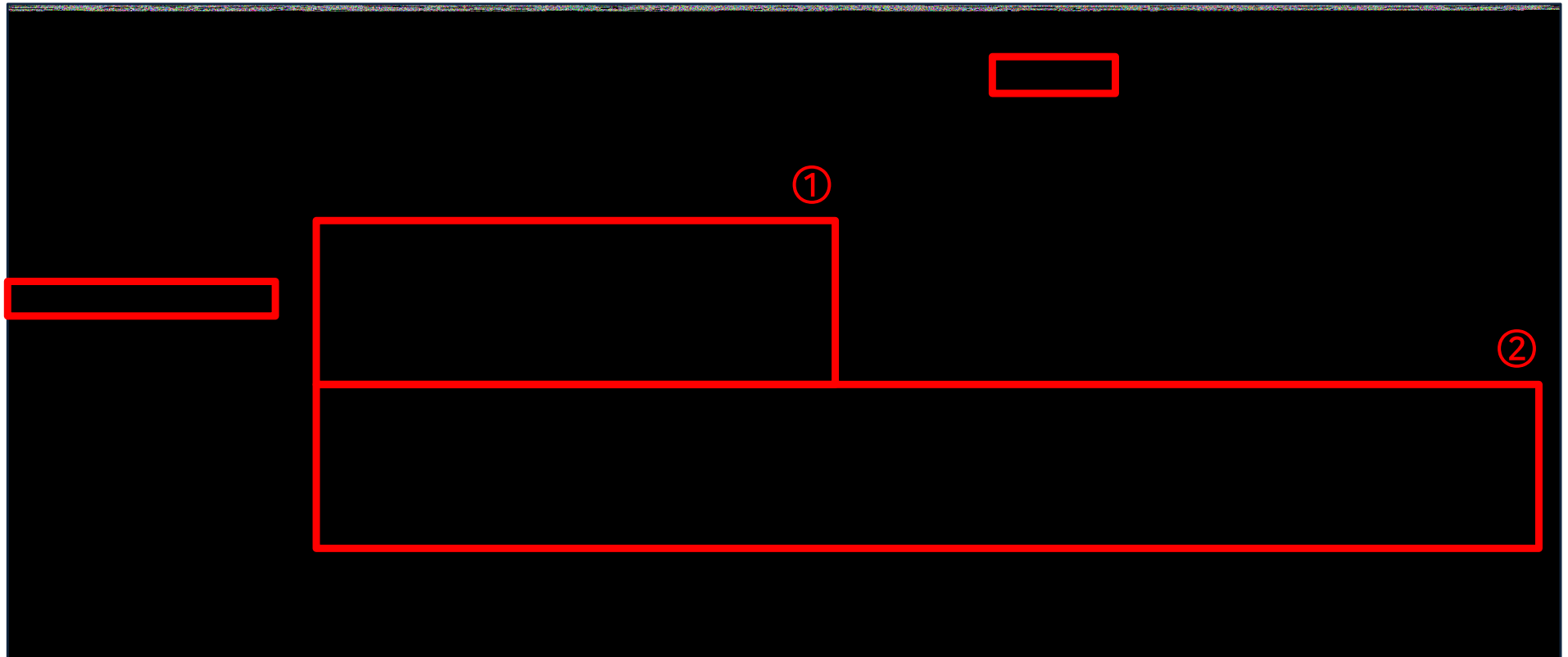
❖ System → 로그 서버



- 로그 정보 전송 할 로그 서버 IP 및 포트번호 (514) 추가
- 전송 하고자 하는 로그 정보 선택 및 해제 가능
- 좌측 "+" 버튼 클릭 후 로그 서버 추가 가능

System

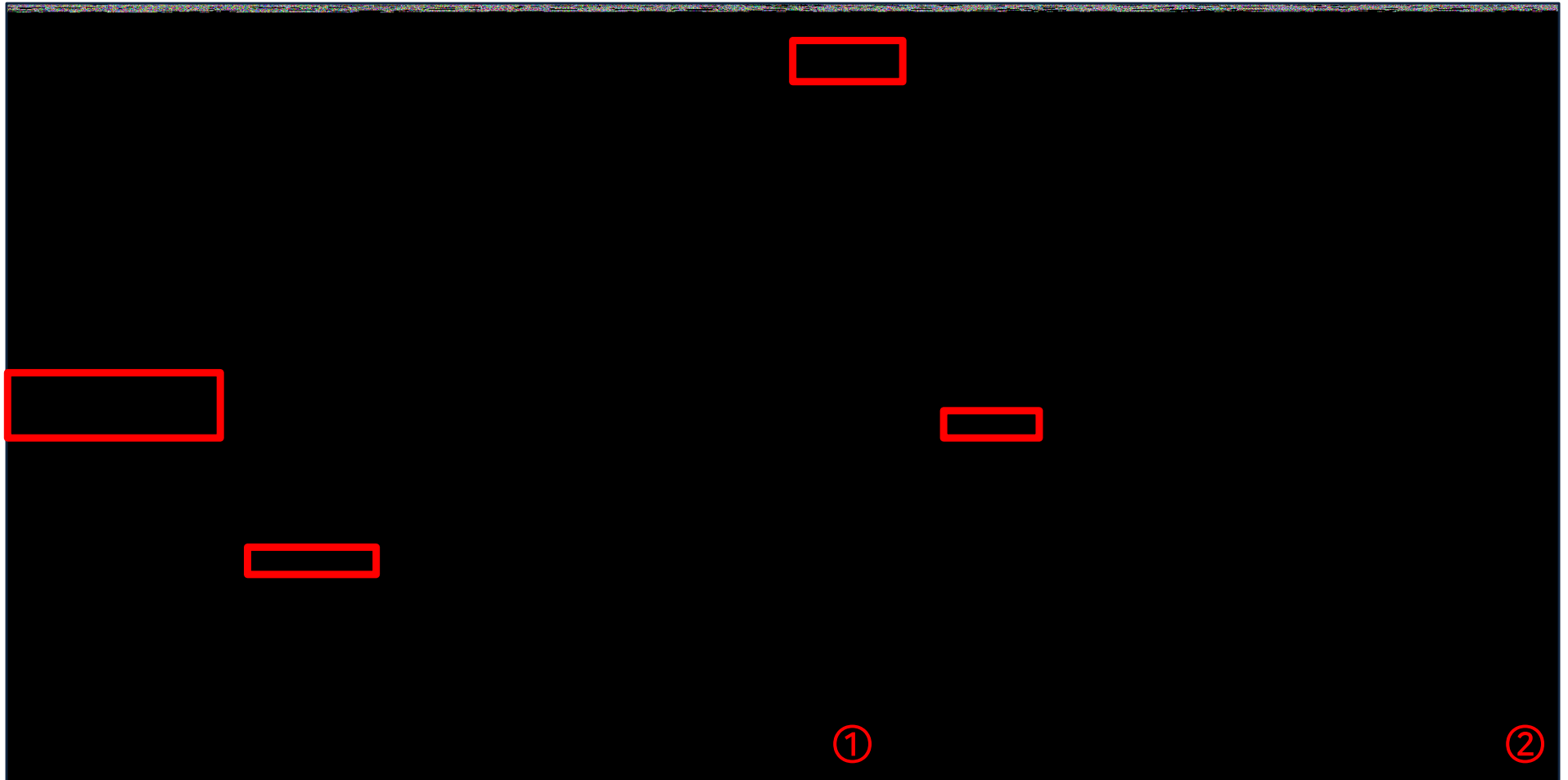
❖ System → SNMP



- 네트워크 모니터링을 목적으로 원격 로그서버에 방화벽을 연결할 때 SNMP를 설정해 두면 방화벽 정보를 쉽게 관리 가능
- ① SNMPv1, SNMPv2를 지원하는 NMS 서버와 통신하려면 SNMP 커뮤니티만 등록 (SNMP 커뮤니티 이름과 IP/CIDR 입력)
- ② SNMPv3를 지원하는 서버와 통신하려면 SNMPv3 사용자 설정

System

❖ System → 백업/복원

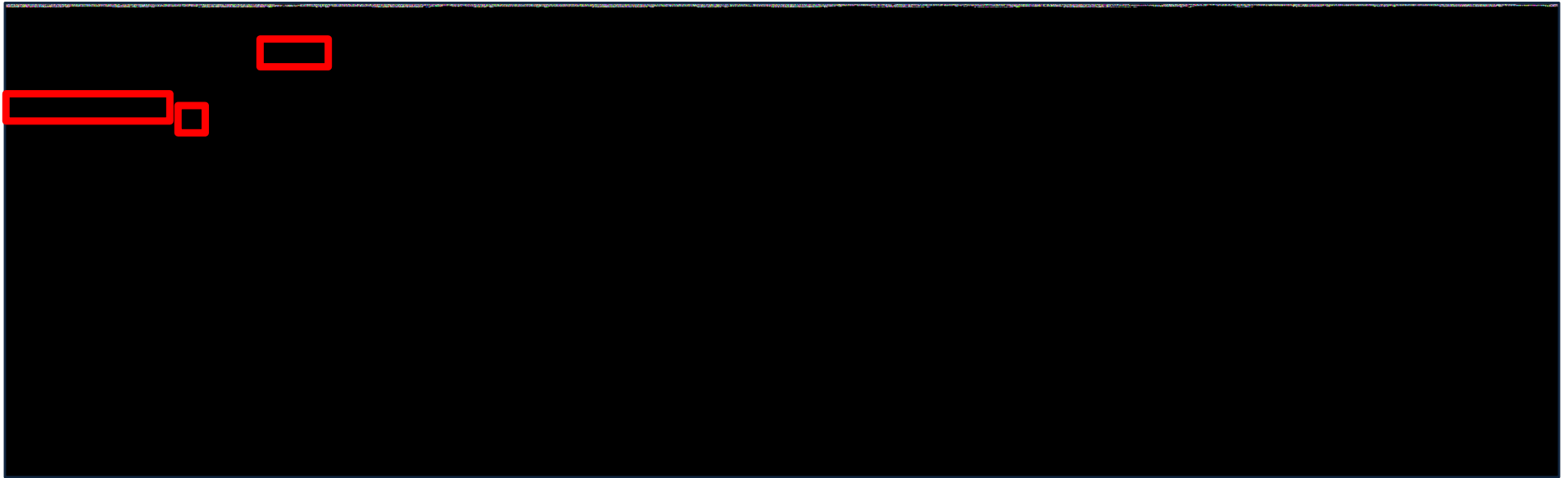


① 백업 : 현재 시점의 시스템 설정 및 정책을 저장
“현재 설정 다운로드” 선택 후 비밀번호 입력 시 시행

② 복원 : 장비 백업 파일을 복원, 백업 시 설정한 비밀번호 알아야 수행 가능

Policy

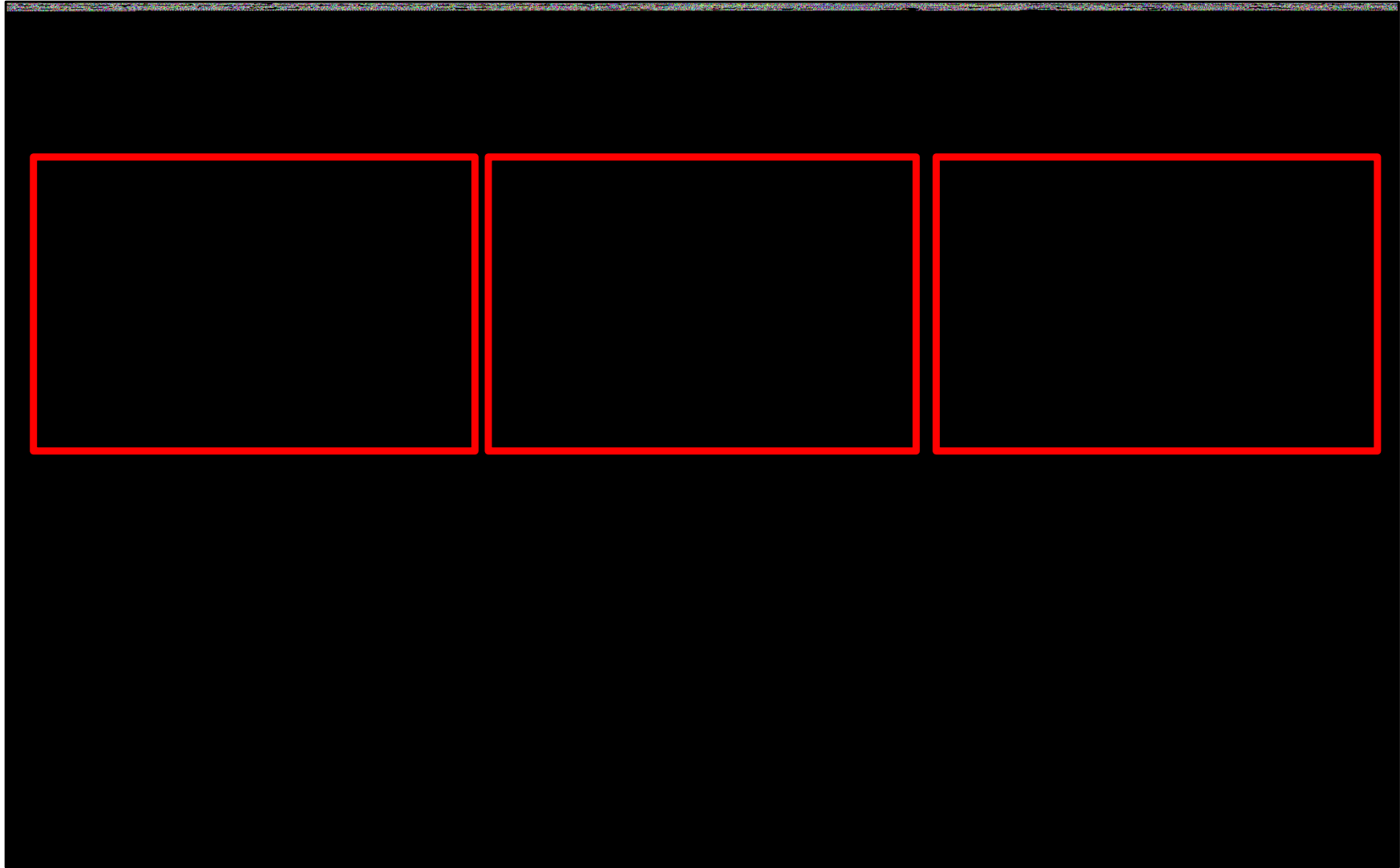
❖ Policy → 기본 정책 → IPv4 정책



- 방화벽 기본 기능 및 IPS 애플리케이션 제어, 안티 바이러스 등 보안 프로파일들과 연계하여 다양한 공격에 대응
- 사용 여부, 출발지 IP, 목적지 IP, 서비스, 처리 방법, 일정, 로그/로그 ID 등 해당 정보에 대한 검색 가능
- 허용해 주지 않은 정책에 대해서는 마지막 기본 차단 정책으로 전부 차단
- 좌측 "+" 버튼 이용하여 정책 추가

Policy

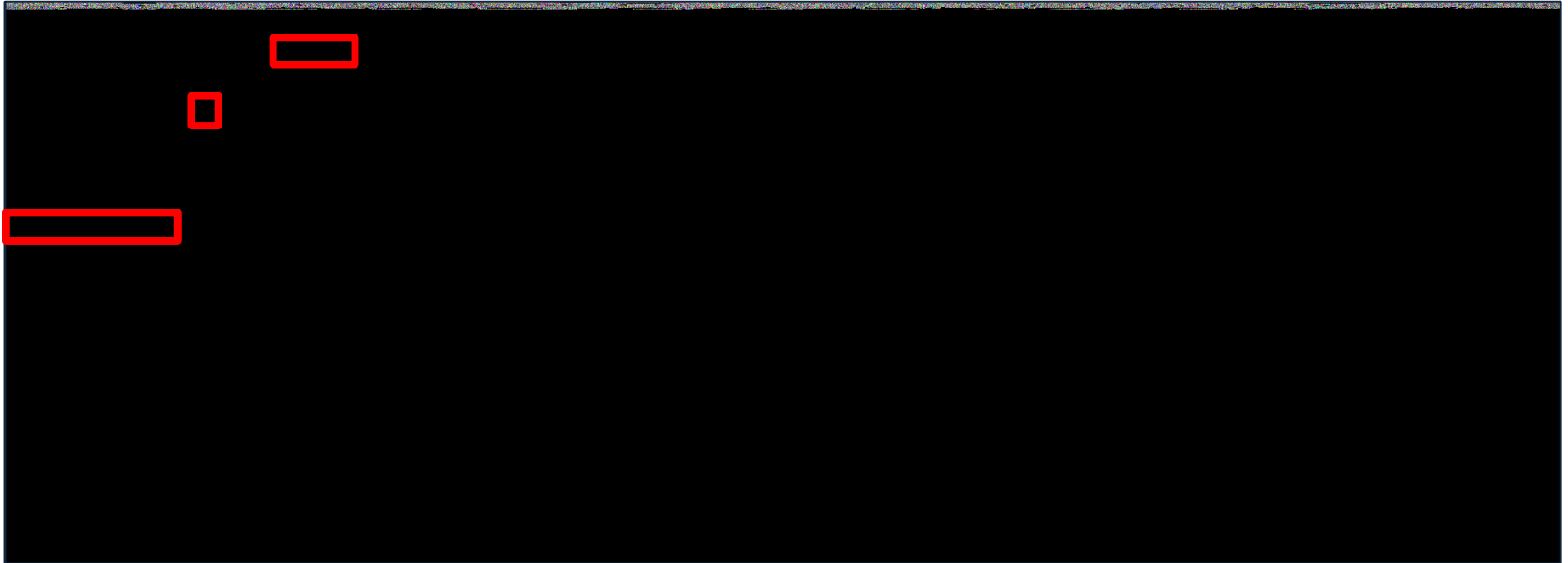
❖ Policy → 기본 정책 → IPv4 정책 추가



- 사용 여부, 출발지 IP, 목적지 IP, 서비스, 처리 방법, 양방향 정책 등 설정

Policy

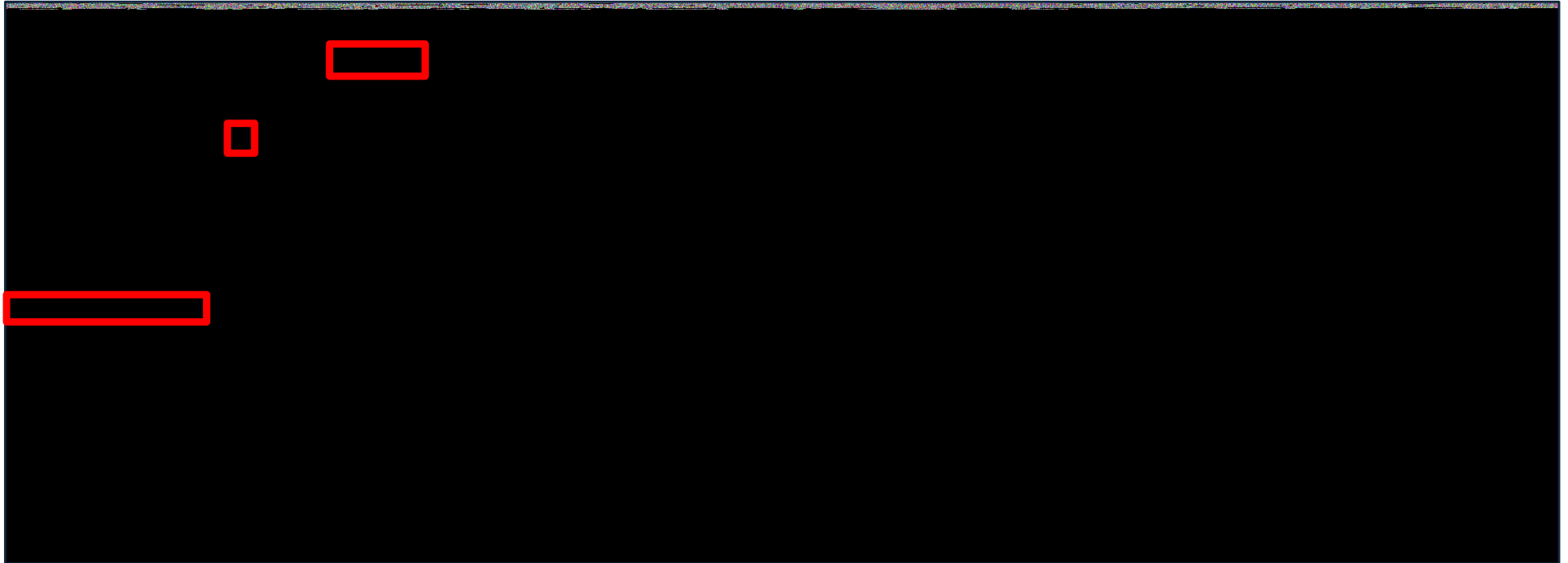
❖ Policy → NAT → 인터페이스 기반 NAT



- 장비를 기준으로 내부와 외부 네트워크를 구분하여 NAT를 설정하는 방식
- Dynamic NAT - 내부에서 외부로 통신 할 때 외부의 출발지 주소로 변경
Static NAT - 외부망에 연결된 인터페이스를 통해 내부의 서버로 목적지 주소 변경
LS NAT - 외부망에 연결된 인터페이스를 통해 DMZ 영역에 있는 서버 그룹에 연결
- 우선순위에 따라 설정 적용
- 좌측 "+" 버튼 이용하여 설정

Policy

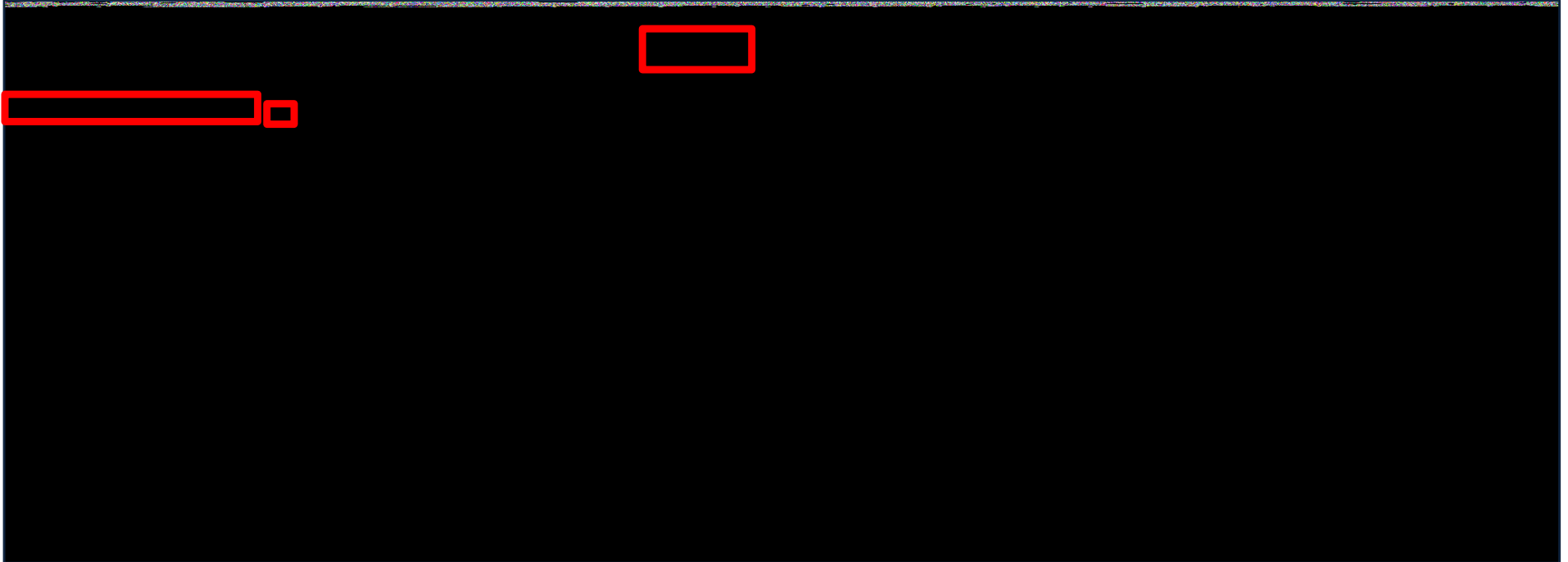
❖ Policy → NAT → 정책 기반 NAT



- IP 객체가 NAT에서 변환될 때, 변환 전/후 IP를 설정하는 방식
- NAT를 통한 통신을 허용하려면, IPv4 정책이 필요
 - IPv4 정책 출발지 : 정책 기반 NAT의 변환 전 출발지
 - IPv4 정책 목적지 : 정책 기반 NAT의 변환 후 목적지
 - IPv4 정책 서비스 : 정책 기반 NAT의 변환 후 서비스
- 좌측 "+" 버튼 이용하여 설정

VPN

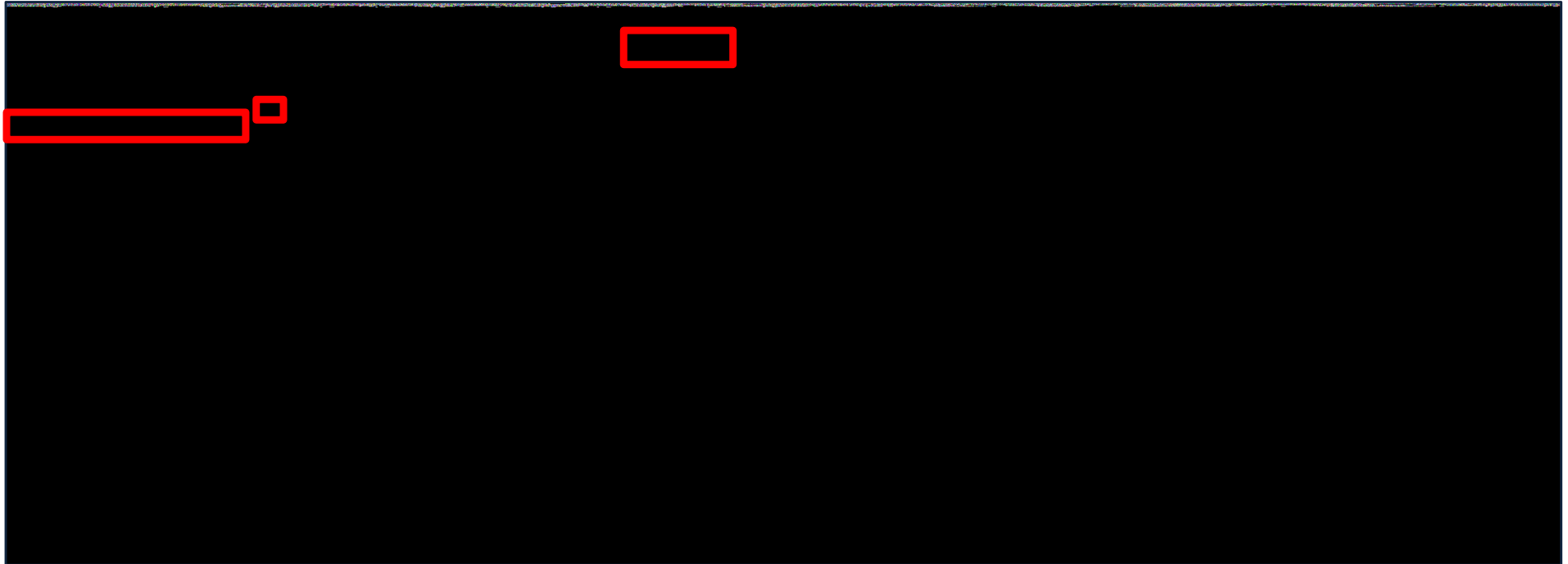
❖ VPN → IPsec VPN → IPsec VPN 정책



- IPsec VPN 연결에 필요한 SA를 지정하고, 로컬/원격 서브네트워크 사이의 터널을 설정하는 방식
- IPsec VPN 정책은 SA, 로컬/원격 게이트웨이, 로컬/원격 서브네트워크 필요
 - SA : IPsec VPN에 사용될 IKE SA, IPsec SA 설정
 - 로컬/원격 게이트웨이 : IPsec VPN 연결에 사용될 로컬 인터페이스, 원격 IP주소
 - 로컬/원격 서브네트워크 : IPsec VPN 터널을 사용할 출발지, 목적지
- 좌측 "+" 버튼 이용하여 설정

VPN

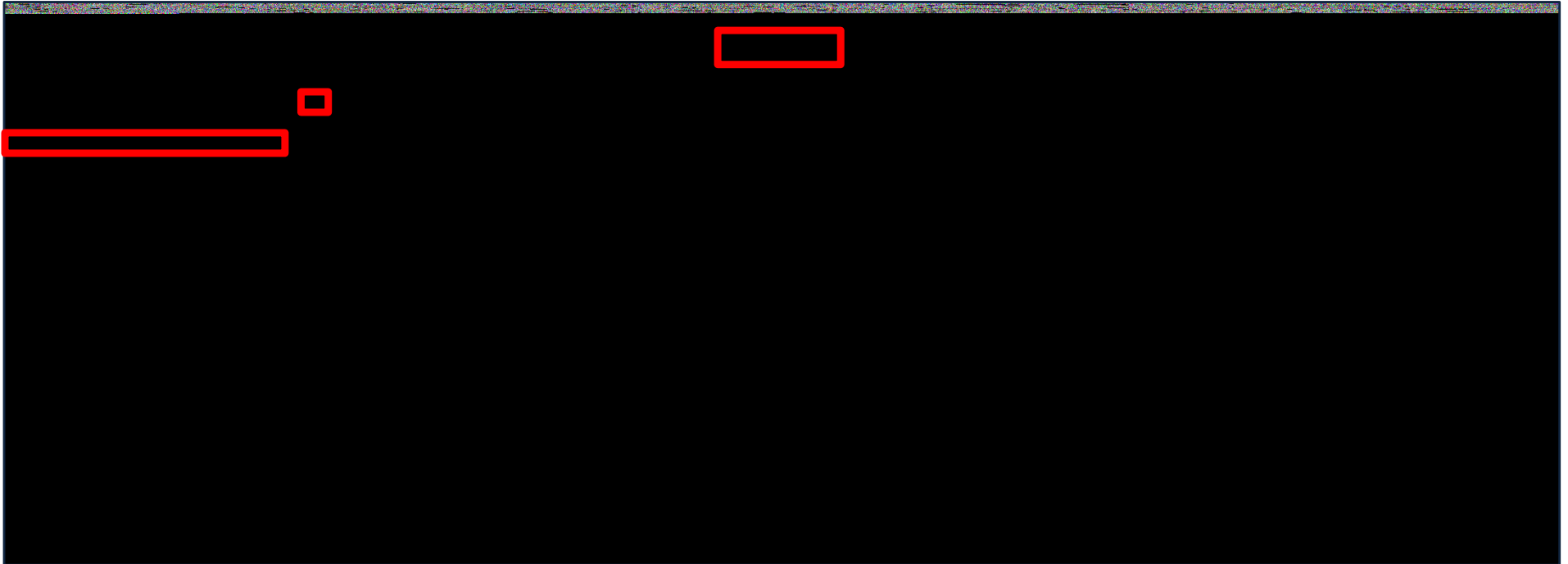
❖ VPN → IPSec VPN → IKE SA



- 두 장비 간의 IPSec VPN 터널 연결 과정에서 Phase 1을 위한 설정으로, Phase 2에서 사용될 IKE 메시지들을 보호하기 위한 마스터키를 설정하고 상호인증 수행
- IKE SA는 IKE 모드, 인증방법(사전공유키), 로컬/원격 게이트웨이 아이디 필요
 - IKE 모드 : IKEv2(IKEv1의 복잡한 통신방식 간소화 및 보안성 향상 버전), IKEv1 메인 모드(보안협상과 키교환 순차적 진행) / 어그레시브 모드(한번에 진행) 중 선택
 - 인증방법(사전공유키) : 인증에 사용할 비밀키 설정
 - 로컬/원격 게이트웨이 아이디 : 상호 식별용 로컬/원격 게이트웨이 문자열 설정
- 좌측 "+" 버튼 이용하여 설정

VPN

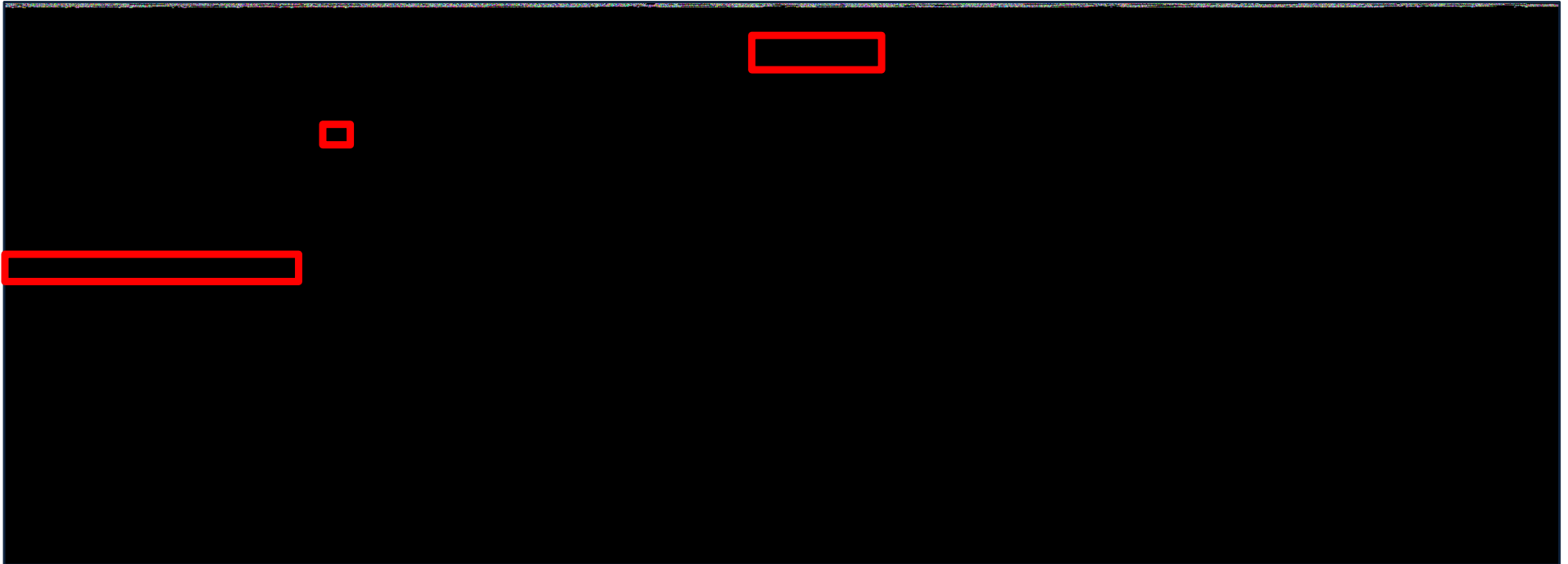
❖ VPN → IPsec VPN → IPsec SA



- 패킷을 암호화하거나, 데이터 처리에 사용할 비밀키의 생성 및 실제 패킷 처리에 필요한 매개변수를 정의
- IPsec SA는 보안 프로토콜, 암호화 알고리즘, 해시 알고리즘 필요
 - 보안 프로토콜 : AH, ESP 중 선택
 - 암호화 알고리즘 : ESP를 사용할 때 페이로드 암호화에 사용할 수 있는 알고리즘
 - 해시 알고리즘 : AH, ESP에서 사용할 수 있는 HMAC 알고리즘
- 좌측 "+" 버튼 이용하여 설정 (기본 생성되어 있는 목록 중에 사용 가능)

VPN

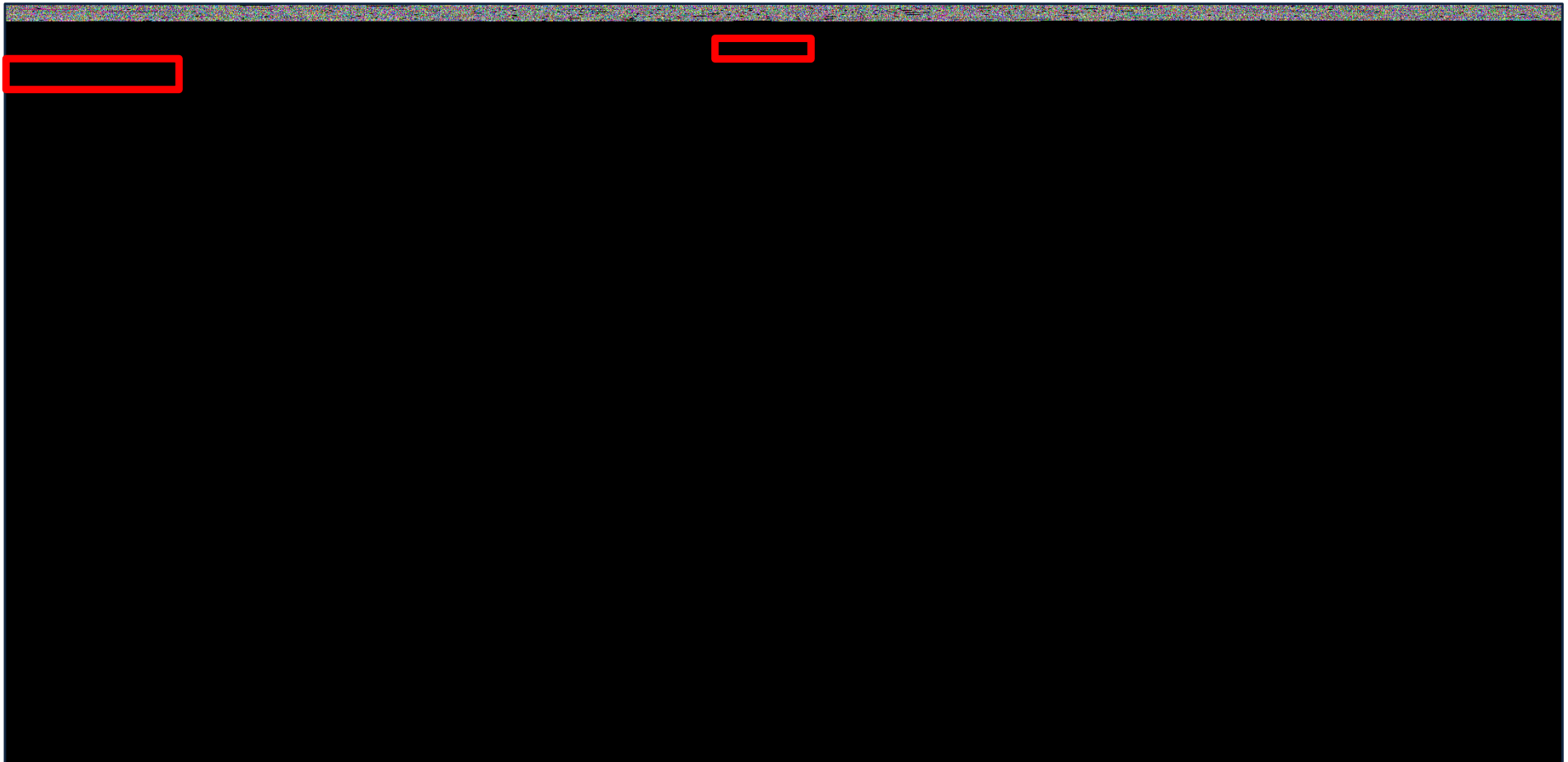
❖ VPN → IPsec VPN → IPsec VPN 설정



- IPsec VPN 실행에 필요한 옵션을 설정
- IPsec VPN 서비스 시작/중지 및 검사 주기, 연결 주기 옵션 선택
 - 검사 주기 및 연결 주기는 기본 설정으로 유지해도 무방하나 사용/중지 변경 시 하단에 저장 클릭 후 설정 필수
 - 주요 통신포트 정보 : NAT-T(터널링 중간에 NAT장비가 있을 시 사용) : UDP 4500
IKE 포트(키교환 서비스) : UDP 500
- “IPsec VPN 사용” 체크 선택하여 사용

Log & Report

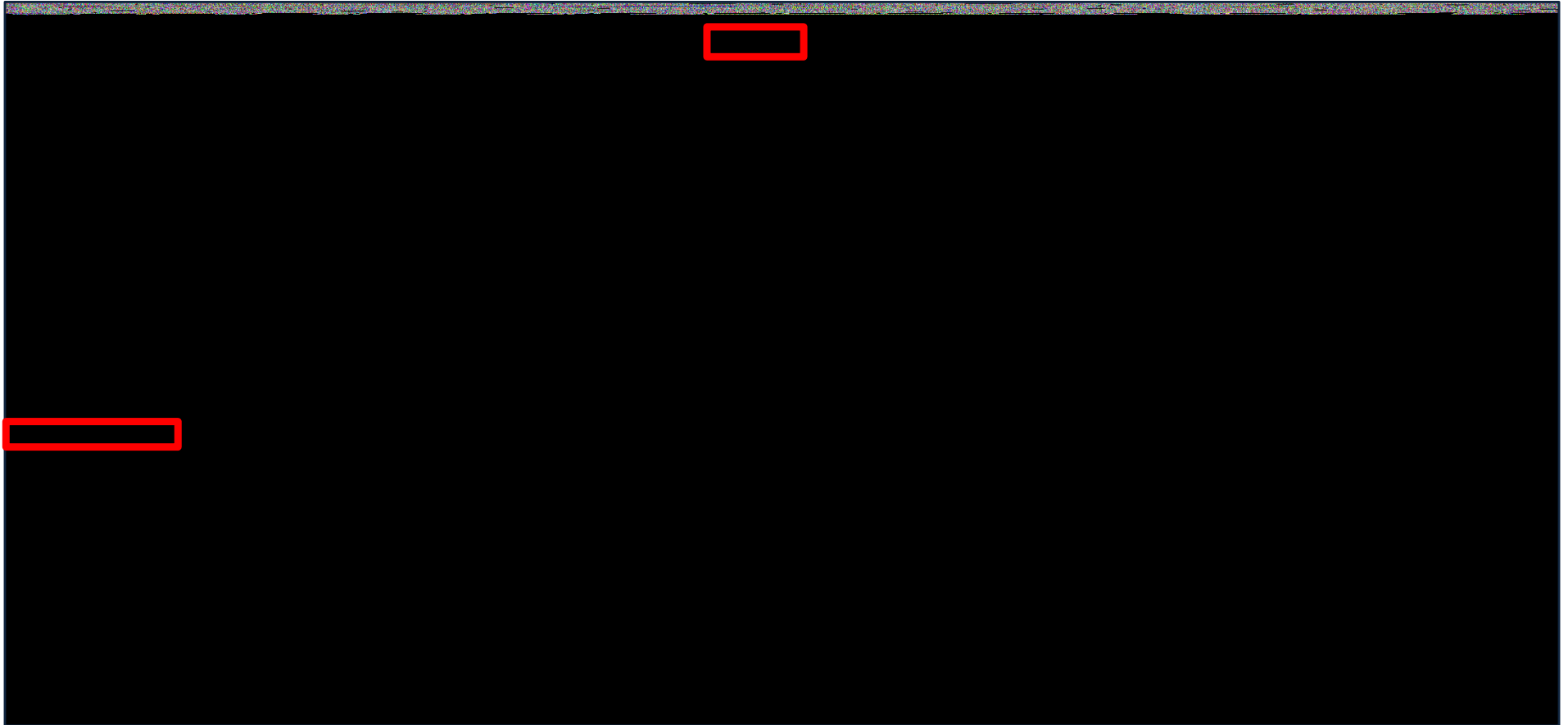
❖ Log & Report → 트래픽 통합 로그



- 제품으로 들어오는 모든 세션에 대해 Policy 하위 기능별 처리 결과를 통합 확인
- 시간, 처리 방법, 정책 아이디, 로그 아이디, IP 주소, 포트번호, 서비스 등 확인 가능하며 검색하여 분리 확인

Log & Report

❖ Log & Report → 이벤트 로그



- 장비에서 발생한 모든 이벤트 로그 확인
(설정/상태 로그, 에러 로그, 관리자 로그, 업데이트 로그, HA 로그 등)
- 생성시간, 로그 중요도, 관리자, IP 주소, 로그 내용 등 표시

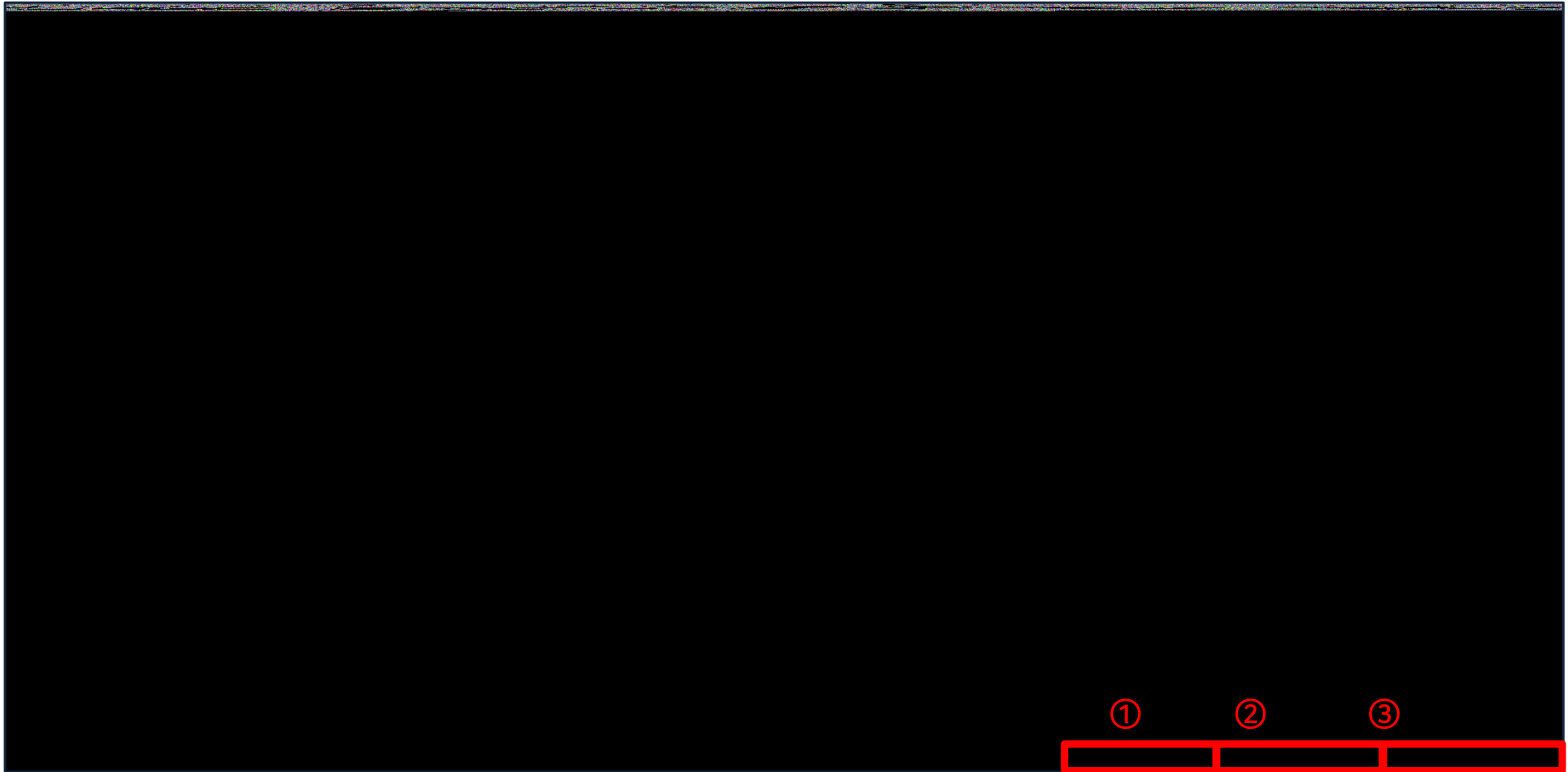
Log & Report

❖ 주요 로그 ID

로그 ID	내용
UTM_ADMINHOST	관리자 IP 주소로 방화벽과 통신한 로그
UTM_DEFAULT	기본 방화벽 정책(모든 트래픽 차단)에 의해 차단된 로그
UTM_HA	HA로 구성된 방화벽 간의 HA 통신 내역 기록
UTM_INVALIDRCP	TCP 유효성검사 활성화 시 TCP 세션 상태가 비정상인 패킷을 차단했을 때 나타나는 로그
UTM_OUTPUT	방화벽이 시작한 통신 내역을 기록 할 때 사용 (PROXY, 시그니처 업데이트)
UTM_PING	방화벽과 호스트 사이에 발생한 ICMP 통신 내역 기록

설정적용 및 동기화

❖ 방화벽 설정적용 / 설정 확인 / 동기화



① 이전 적용 내역 확인 및 복원

② HA 이중화 시 두 장비 설정 및 정책 동기화

③ 방화벽 설정 완료 시 필히 적용 클릭

장애 대응

1. 통신 장애 대응

구분	내용
장애 증상	장비를 통과해서 흐르는 Traffic의 통신 서비스가 정상적으로 이루어 지지 않음
장애 원인	원인 가능성 1 : Software적으로 장비 설정을 잘못된 경우 원인 가능성 2 : H/W적으로 장비에 결함이 있을 경우 원인 가능성 3 : 통신 장애가 있는 구간의 타 장비(서버, 호스트 및 전원 공급장치 포함)에 장애가 있을 경우 원인 가능성 4 : 통신 장애가 있는 구간의 cable에 결함이 있는 경우
대처 방안	1. Network interface 설정, Routing table 설정, IP 객체 설정, 서비스 객체 설정, 방화벽 정책 설정 등에 대해서 확인하여 설정 상의 문제가 없는지 확인하여 잘못된 설정에 대해 수정 2. 장비 전면의 LCD 화면에 정상적인 메시지와 인터페이스에 링크 활성화, 장비 후면의 Power Supply LED 불 등을 확인 - 전면 LCD 메시지가 정상적으로 나오지 않을 경우 장비 리부팅 - 인터페이스 링크가 정상적으로 활성화되지 않았다면 케이블을 교체하고 그래도 동일하다면 장비 교체나 NIC 교체 - Power Supply 2개의 LED 불이 모두 들어오지 않았다면 (전원공급에 문제가 없다면) Power Supply 교체 3. 전원공급장치에 이상이 없다면 통신 장애가 있는 구간을 장비 별로 각각 나누어 ping이나 기타 가능한 서비스 체크 방식으로 확인하여 방화벽을 거치지 않는 장비 구간일 경우 해당 장비를 체크 4. Cable 확인에서 결함이 발견되면 cable 교체

장애 대응

2. 접속 장애 대응

구분	내용
장애 증상	장비에 접속이 되지 않음
장애 원인	원인 가능성 1 : 접속을 시도하는 IP가 관리 IP가 아닌 경우 원인 가능성 2 : 접속을 시도하는 PC에서 장비까지 통신이 되지 않는 경우 원인 가능성 3 : 장비 프로세스에 문제가 있는 경우 원인 가능성 4 : 로그인 실패 횟수 초과(10회)로 Lock이 걸린 경우
대처 방안	1. 장비에 Console Cable 로 연결(Speed: 115200)하여 wizard → adminhost 에서 관리 IP 확인하여 접속 2. 접속을 시도하는 PC에서 장비로 ping check를 하여 통신이 되는지 확인 ping 체크가 안될 경우 네트워크 통신 연결 확인하여 통신 연결 복구 3. 관리 IP나 통신에 문제가 없다면 장비 프로세스에 문제가 있을 수 있으므로 장비를 재가동 하여 확인 4. 로그인 실패 횟수를 초과하여 Lock이 걸렸을 수 있으므로 이 경우에도 장비를 재가동하여 확인

장애 대응

3. H/W 장애 대응

구분	내용
장애 증상	장비 전면 좌측 LCD 창에 불이 들어오지 않거나 메시지가 나오지 않음 장비 port 부분에 링크 불빛이 안 들어오거나 깜빡이지 않음
장애 원인	원인 가능성 1 : 전원이 OFF 된 경우 원인 가능성 2 : 장비 프로세스에 문제가 생긴 경우 원인 가능성 3 : port 연결 불량이나 cable 불량인 경우 원인 가능성 4 : port의 duplex/speed 설정이 맞지 않는 경우
대처 방안	1. 장비 후면 Power Supply LED에 불이 정상적으로 들어와 있는지 확인하여 안 들어와 있을 경우 전원 체크 2. 전원에 이상이 없고 장비 전면 좌측 LCD 창에 메시지가 나오지 않는다면 장비를 재가동한 후 다시 확인 3. 장비 port 링크에 이상일 경우 port와 cable 접촉상태를 확인하고 cable 자체에 결함이 없는지 확인하여 이상이 있을 경우 cable 교체 4. Port의 duplex/speed가 정상적인지 장비에 접속하여 확인 후 Half나 speed가 맞지 않을 경우 상대 장비와 cable, 구성 등을 확인하여 설정을 같게 함

장애 대응

4. 전원 (Power) 장애 대응

구분	내용
장애 증상	장비 후면에서 알람 소리가 나거나 Power Supply LED에 불이 들어오지 않음
장애 원인	원인 가능성 1 : 2개의 Power 중 한 개에 장애가 발생한 경우 원인 가능성 2 : 전원공급이 정상적이지 않을 경우 원인 가능성 3 : Power cable에 결함이 있을
대처 방안	1. 장비 후면에서 알람소리가 난다는 건 2개의 전원 중 한 곳에서 전기를 사용하지 못한다는 것이며 이중화된 전원은 Hot Swap 방식으로 운영 중에도 장애가 있는 Power Supply를 교체 가능 2. Power Supply에 전원을 공급해 주는 멀티탭이나 그 상위 공급장치 장애일 경우 해당 장치들의 장애를 먼저 해결 3. Power cable에 결함이 있을 수 있으므로 Power cable도 교체해서 확인