“FOCS” 방화벽 정책 통합관리 솔루션 제품 소개서

싸이버텍홀딩스 보안사업부

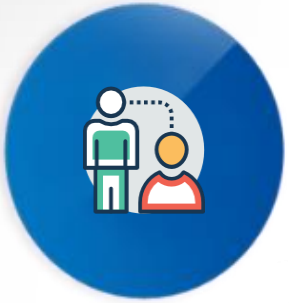
이상현 차장 (010-2396-3106, shlee@cybertek.co.kr)

Leading the Paradigm 싸이버텍홀딩스

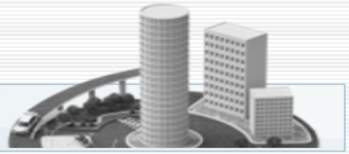
bellock

CONTENTS

방화벽 정책관리 솔루션 시장현황



단순 정책관리 및 감사 솔루션에서 → 방화벽 통합운영 관리 솔루션으로 발전



1세대 솔루션 모니터링

- ✓ 정책분석 및 감사 기능 수행
- ✓ 외산 감사용 솔루션 장비 도입

2세대 솔루션 신청+운영

- ✓ 신청 및 설계/적용 기능 국내 개발 제품 등장
- ✓ 외산 장비(운영) + 국내 개발 협업 시작

3세대 솔루션 통합관리

- ✓ 통합운영 및 관리 솔루션으로 발전
- ✓ 보안업무 자동화 기능 구현 및 상시 감사 수행

방화벽보안정책 관리의 위협 요소

정책관리 필요성

- 강화되는 보안규정 및 감사
- 수기/인력에 의한 정책 운영/관리 어려움
- 보안정책의 관리운영 전문기술 인력부족

당면한 정책관리 위협

- 보안규정 실시간 준수여부 확인 불가
- 방화벽 및 보안정책 증가
- 보안 정책 운영 관리 리소스 증가
- 보안 규정 위배 정책의 적용
- 중복 및 사용 만료 정책을 통한 해킹 공격

휴먼 오류 장애 발생 및 불필요한 보안정책 누적으로 보안 위협 증가

도전과제

당면한 정책관리 위협을 해결하고, 정책 관리의 효율성을 향상시켜야 함

'신청, 설계, 적용, 감사' 및 정비에 이르는 업무 자동화 확립

'Compliance 실시간 준수여부 확인'

솔루션 도입의 필요성

1. 방화벽 정책 수준 제고로 보안 강화
2. 보안업무 자동화로 업무 혁신
3. Compliance 준수

* 방화벽 운영업무 개선방안 및 정합성 있는 설계, 보안규정과 실시간 감사 체계필요

표준화

업무표준 프로세스 수립

- 이기종 방화벽의 중복 및 취약 정책 신청 예방
- 신청자와 운영자의 업무 자동화
- 방화벽 정책신청 업무 간소화
- 이기종 방화벽의 공통 신청양식 및 이력관리 제공
- 담당자의 불필요한 중복 업무 제거

효율성

업무효율 및 생산성 증대

- 자동화된 정책분석으로 업무 효율 향상
- 방화벽 정책의 최적화, 자동분석,이력관리를 통한 라이프 사이클 관리
- 사용자 중심의 관리 운영 페이지 제공
- 신청 / 결재 / 적용 프로세스의 전산 및 자동화

보안성

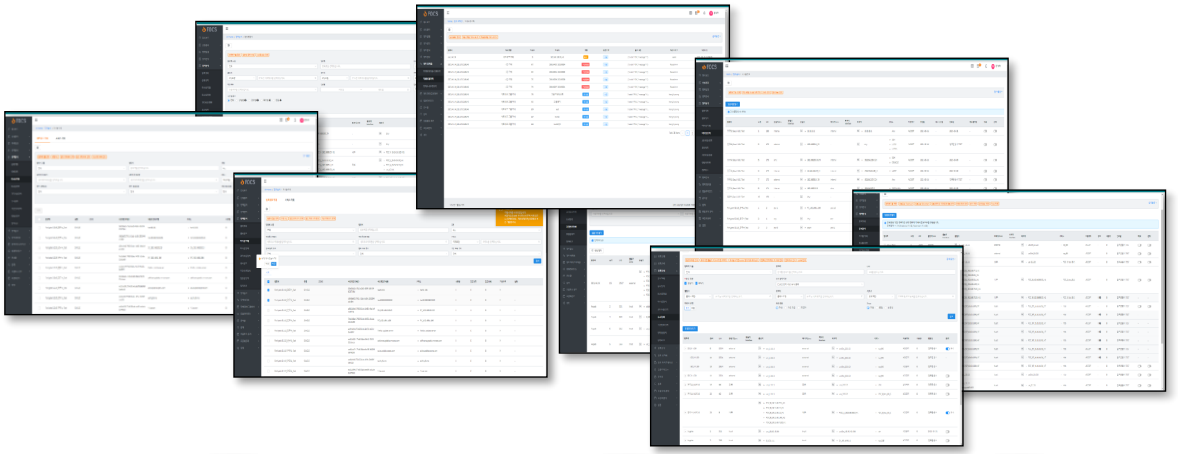
상시 보안감사 수행

- 규정준수 관리의 시스템화
- 상시적 규정준수 및 감사 대응
- 내부 보안규정에 따른 정책 자동 필터링 제공
- 다수의 이기종 방화벽 설비의 실시간 로그 확인

서비스를 잘 모르는 사람도 망설임 없이 편하게 사용할 수 있도록

사용 편리성

신청 관리 프로세스 제공



누구나

IT서비스 경험이 익숙하지 않은 사용자 및 관리자

쉽고 편하게

원하는 기능을 쉽고 편하게 확인 및 사용 할 수 있도록

사용할 수 있게

전문가의 도움없이 빠른 이용이 가능 하도록

방화벽 정책의 라이프사이클을 체계적으로 관리하는 국내 환경에 최적화된 국산 "방화벽 정책통합 관리솔루션"


신청/결재


설계적용(자동화)


정책관리


관리감사

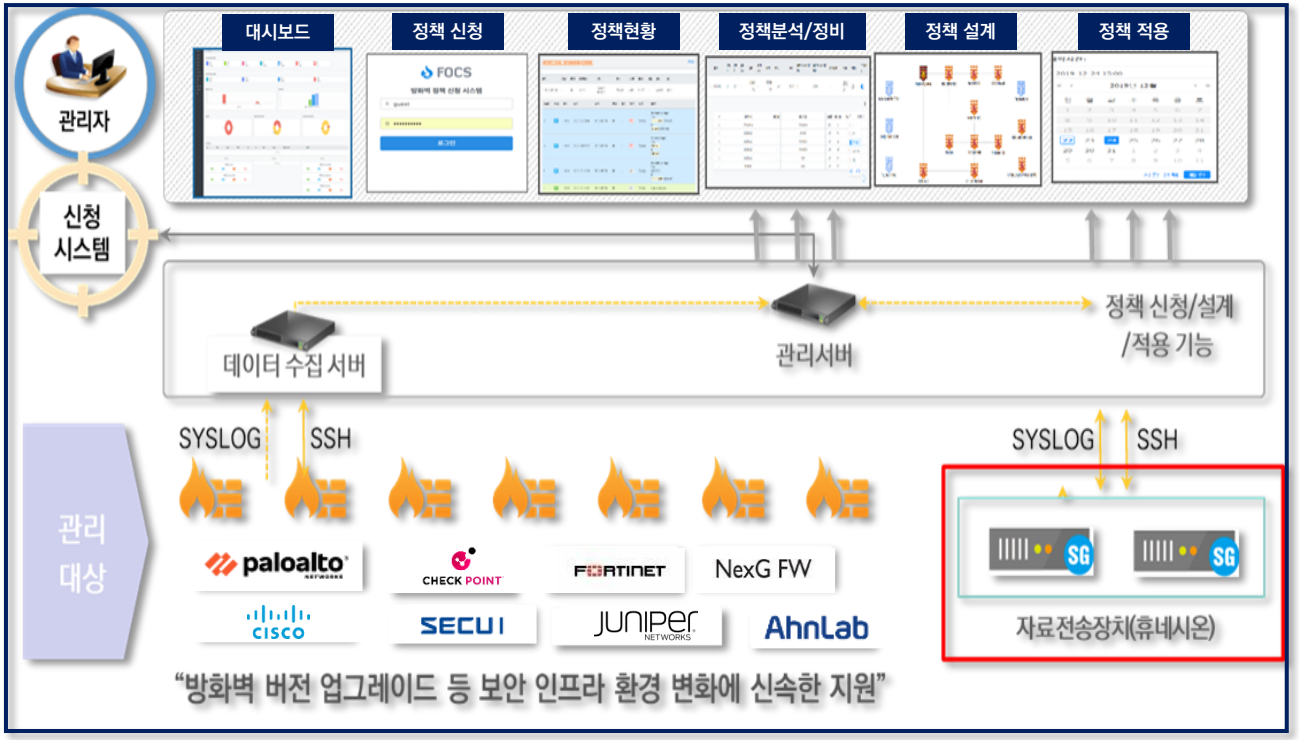
대시보드	정책분석	자산연동
정책현황	정책설계	정책신청
정책적용	DB	결재관리

기능별 모듈화 구현
각 모듈의 유기적 연결 내부 논리 구성으로
최적의 성능 및 안정성 보장

Point ▸▸▸▸ ONE

Vendor & One Key

- One Vendor 제품으로 Process 구현 가능
- One Key 연계된 정책관리 및 이력관리
- 신속한 기술대응 및 서비스 제공 고객만족도 향상



FOCS 는 특허받은 대용량 시스로그 처리방법론을 기반으로 하여 정책 신청에서 분석/정비/설계/적용까지 신뢰성 높은 데이터를 제공하여 효율적으로 방화벽정책관리 업무 지원

차별화

특장점 01	TECHNOLOGY	핵심기술지원	특허받은 방화벽 정책 대용량 시스로그 처리 정책설계가이드 / TCP Flag 분석 • 신청/분석/적용까지 정확한 정책관리 운영업무 지원	딥러닝 학습 데이터 기반 ✓ 방화벽 정책에 대한 신뢰도 있는 분석 데이터 제공 ✓ 사용률 분석을 통한 과다 허용 세분화 정책지원 정책현황분석 / 경유지 토폴로지 맵
특장점 02	PROCESS	정책통합관리 프로세스	방화벽 정책의 신청, 설계, 적용 및 감사에 대한 운영 신청 → 분석 → 적용 • 신청/분석/적용까지 정확한 정책관리 운영 업무 지원	아키텍처 연동 자산 DB연동 / 인사 DB연동 • 유기적인 내부 로직 구성을 통한 데이터 연동지원
특장점 03	OPERATION	자동화운영지원	365일 무중단 정책관리 서비스 제공 • 정책의 신청, 설계 적용 및 결재가 솔루션을 통해 자동화 함으로써, 보안담당자의 업무 효율성 증대 • 방화벽 및 정책관리 전문 기술인력을 통한 상시 기술 지원 제공	정책자동적용 • 신청 내역 결재 완료 시 경유지 방화벽 자동 분석 및 적용 기능 제공 • 자동 적용 내역에 대한 상세 결과 신청자/운영자/관리자 즉시 알림 기능 제공

Point ▸▸▸▸ 딥러닝 기능을 통한 " 데이터 정합성 및 상세분석 " 기능

- ☑ 상세 TCP Flag 분석 데이터 제공
- ☑ 학습을 통한 자동 토폴로지 맵 구현

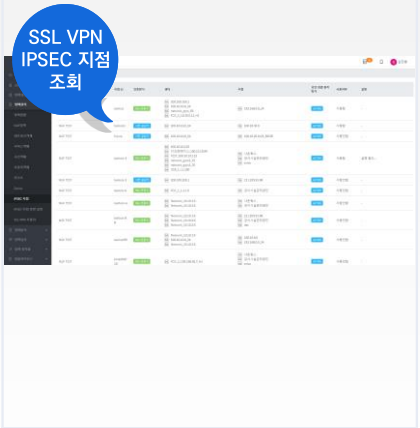
타시스템분석기법	FOCS분석기법
기존 ZONE 정보에 대하여 수동등록진행 (인터페이스, Zone정보 등)	Syslog 및 트래픽 수집 후 딥러닝 기능을 통한 정책설계 추천가이드 제공 상세 TCP Flag분석 데이터 제공
Syslog 및 트래픽 정보 수집 후 정확한 데이터 제공 (추측할 수 있는 데이터 기반 가이드 제공)	기존 Zone 정보에 대하여 자동매칭
SNMP방식을 통한 토폴로지 맵 구현시 방화벽 장비에 리소스 지원이용으로 방화벽 부하 발생	딥러닝 기술을 통한 자동 토폴로지 맵 구현 (딥러닝 학습을 통한 맵 구성)
SNMP Pulling / Pulling 방식을 통한 정책 적용시 암호화 및 명령어 보호(캡슐화)에 대한 이슈	Rest API를 사용하여 방화벽 연동 (암호화 키값을 토대로 SHA256등의 암호화 방식에 의거 명령어 전달 및 수행)

VS

Point ▸▸▸▸ VPN 관리

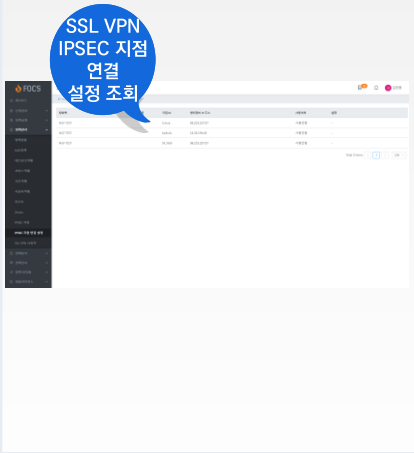
- IPSEC VPN 지점의 인증 및 연결 동작 조회
- IPSEC VPN 지점 연결 관리
- SSL VPN 사용자 관리

IPSEC 지점



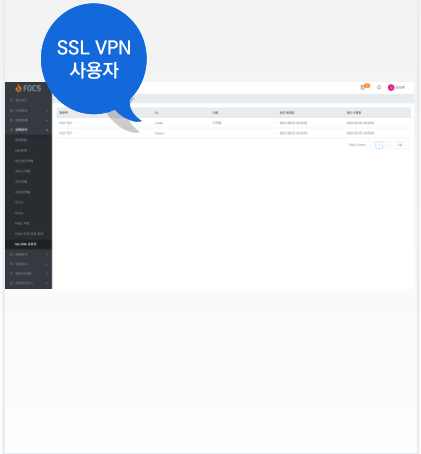
- VPN 에 등록된 IPSEC 조회

IPSEC 지점 연결 설정



- VPN 에 등록된 IPSEC 지점 연결 설정 조회

SSL VPN 사용자



- SSL VPN 사용자 현황 조회

Point ▸▸▸▸ 인증 및 특허

- 관련 특허 3건 보유
- GS인증서 보유

1등급 GS인증(1등급)

조달등록제품

비동기 데이터 전송을 위한 채널 할당 관리 방법, 비동기 데이터 전송 방법 및 상기 방법을 이용하는 장치

- 본 발명은 비동기 데이터 전송을 위한 채널 할당 관리에 관한 것으로, 본 발명에 따른 비동기 데이터 전송을 위한 채널 할당 관리 방법 및 데이터 로그 수집 방법론

패킷 라우팅 방법 및 장치

- 패킷 라우팅에 관한 것으로, 이웃 노드별 이웃 노드 테이블 업데이트 주기 내의 손실 비컨 프레임 수를 이용하여, 주기적으로 상기 각 아웃 노드에 대한 링크 안정성 산출하여, 상기 이웃 노드 테이블 내에 업데이트하고, 수신된 임의의 패킷에 대해 자신이 목적지 노드가 아니면, 자신 보다 목적지 노드에 더 가깝게 위치한 이웃노드를 파악하고, 상기 임의의 패킷을 상기 파악한 이웃 노드로 전송하는 기술

네트워크에 연결된 디바이스간에 이벤트 정보 전송 방법 및 장치와 그 저장 매체

- 본 발명은 네트워크에 연결된 디바이스간에 다양한 형태의 이벤트 리소스를 전송할 수 있는 이벤트 정보 전송 방법 및 장치와 그 저장 매체에 관한 것

Point ▸▸▸▸ 국내ICT환경에최적화된기능제공

현업 담당자의 니즈를 바탕으로 기능 구현

국내 정보보안업무에 필수적인 요소

신청관리	신청 정책에 대한 네트워크 경로 또는 중복정책 여부 점검 기능
정책감사	공통 표준 컴플라이언스(ISMS-P,PCI DSS 등)위반여부 점검 기능 제공
정책현황	방화벽 전체 정책 및 정책 상세 정보를 조회할 수 있으며, 정책별 이력 및 근거 문서 자동 매핑
정책분석	정책 현황정보, 정책 미사용, 중복, 과다허용, 기간만료 정책 분석 후 정책 정비 프로세스 제공
설계/적용	정합성 있는 방화벽 및 정책/객체 추천하여 운영자의 정책설계/적용 업무를 효율적으로 지원
토폴로지	실 트래픽 및 syslog 기반으로 FOCS만의 노하우 기술력을 통한 토폴로지 분석 기능 제공
보고서	전체 이력관리 및 현황을 한눈에 볼수있는 보고서 기능 제공

신청관리 | 결재관리 | 정책설계 | 정책적용 | 정책관리 | 정책최적화 | 보고서

신청관리

신청자

- 신청자 편의성을 갖춘 자산 내역 검색을 통한 신청 제공
- 신청 내역에 대한 중복, 감사 검증 기능을 통해 최적의 신청 가이드

특화 기술: 자산 등록 및 검색 반영 기능

결재관리

단계별 알림기능

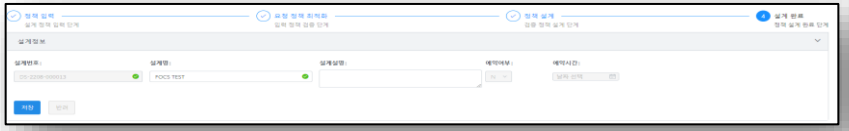
- 신청 내역에 대한 알림을 통해 즉각적인 결재 요청 사항을 알 수 있으며 신청 내역의 정합성 여부 확인 기능 제공

특화 기술

- 메신저
- Mail
- SMS

정책설계

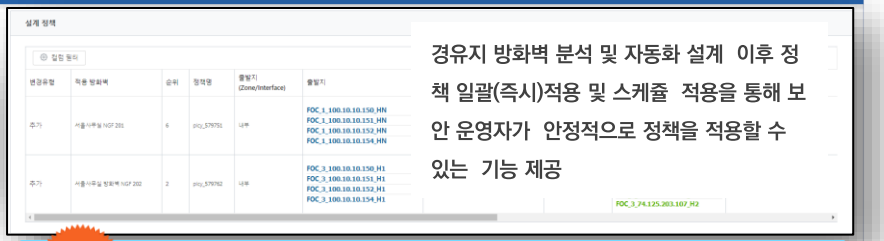
정책 입력 → 요청 정책 최적화 → 정책 설계 → 설계 완료



- 자동화 설계 기능을 통해 경유지 방화벽 분석 및 경유지 방화벽 내 오브젝트 설계 제공

특화 기술
- 트래픽 딥러닝을 통해 정확한 경유지 방화벽 분석 및 설계 기능
- 상세 설정 기반의 설계 자동화

정책적용

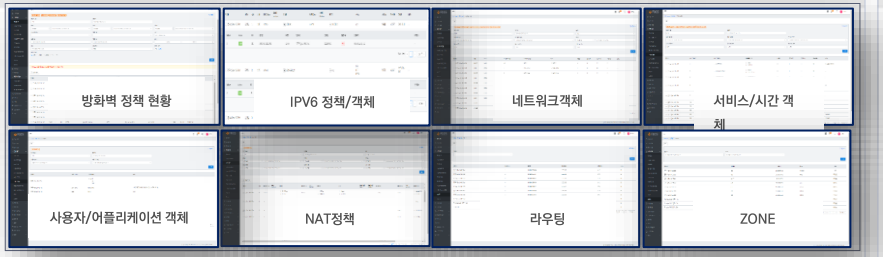


경유지 방화벽 분석 및 자동화 설계 이후 정책 일괄(즉시)적용 및 스케줄 적용을 통해 보안 운영자가 안정적으로 정책을 적용할 수 있는 기능 제공

특화 기술: FOCS 특화 기술 : 즉시, 스케줄 등의 차등 적용 기능과 오브젝트 표준화(오브젝트명 표준화) 기능

신청관리 | 결재관리 | 정책설계 | 정책적용 | **정책관리** | **정책최적화** | **보고서**

정책관리



정책 및 객체 별 상세 사용률 분석 및 각 정책이 사용되는 트래픽까지 상세 분석이 가능

정책최적화

☑ 정책/객체 최적화 가이드 제공
→ 보안정책 최적화 기능

특화 기술

정책, 객체 등에 대한 분석 및 실제 최적화(삭제) 기능 제공

최적화 적용

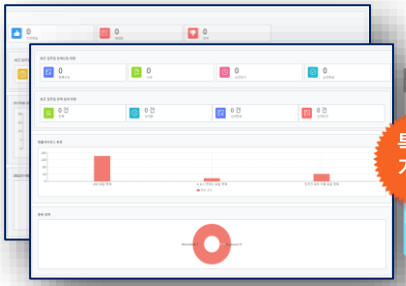
정책/객체

분석/설계

변경/삭제

보안 정책 최적화

보고서



☑ 신청/결재자의 편의성 제공 및 신청 정책에 대한 네트워크 경로 or 중복정책 여부 점검 기능

특화 기술

ITSM 보고서를 통해 일일 요약 보고서 제공

FOCS 기술 발전 방향

FOCS(Firewall Policy Orchestration Center Solution)

보안 대응 자동화(SOAR)를 목표로 방화벽 외 IT 전반의 보안시스템의 플랫폼 지향 및 개발 中

☑ AS –IS : 망연계솔루션 정책현황/분석/감사 연계 완료 (설계 적용중)
향후 :취약점분석시스템 / VPN등과 연동

Point ▸▸▸▸ 방화벽 정책설계적용 " 자동화 "

신청관리 | 결재관리 | 정책설계 | 정책적용 | 정책관리 | 최적화 | 보고서

- One Key 기반의 편리한 정책 신청 및 적용
- 객체 / 정책의 **업무 표준화 기반**

방화벽 정책 설계 적용의 자동화

신청
- 고객 보안포탈 연동
- ITSM 시스템 연동
- 자산관리 시스템 연동
- FOCS신청시스템 사용

설계
- 출발지/목적지 맵 제공
- 방화벽 정책정보 제공
- 운영 객체/정책명으로 설계

적용
- 즉시 적용
- 예약 적용

- 신청정보 조회 / 등록
- 중복정책 확인
- 규정위반 확인
- 정책 오류 확인

- 정책 논리 설계
- 정책 병합/분리 설계
- 정책 최적화
- 정책 적용 확정

- 방화벽 API연동
- 여러대의 방화벽 동시 적용
- 적용 결과 알림

Point ▸▸▸▸ 신청/결재 Process를 통한
" 방화벽 정책 관리 업무 표준화 "

신청관리 결재관리 정책설계 정책적용 정책관리 최적화 보고서

- 자산내역 검색을 통한 신청서 작성기능 제공
- 신청서 작성 단계에서 " 중복 및 규정 감사"기능 제공

신청관리

1 신청티켓 생성

"자산내역" 검색을 통한신청

2 감사 및 운영

내부 규정 위반 검사
컴플라이언스 위반 검사
"실시간 알림" 기능
신청티켓번호를 통한 관리

3 전자결재

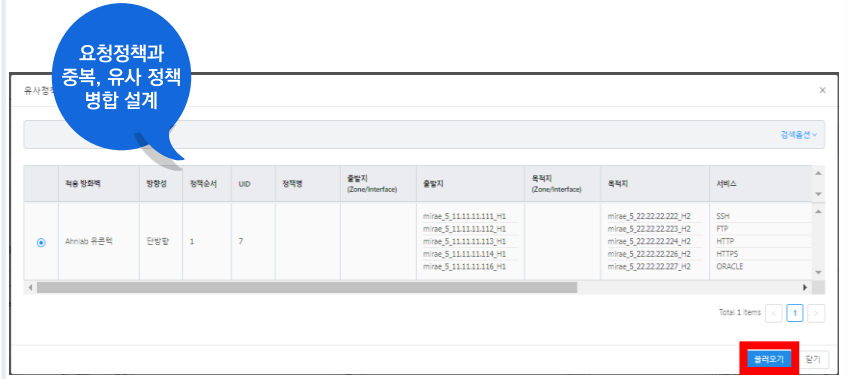
신청부서 신청자 / 팀장
보안부서 담당자 / 팀장

사용신청 부서 → 보안담당 부서 → 적용

정책논리설계

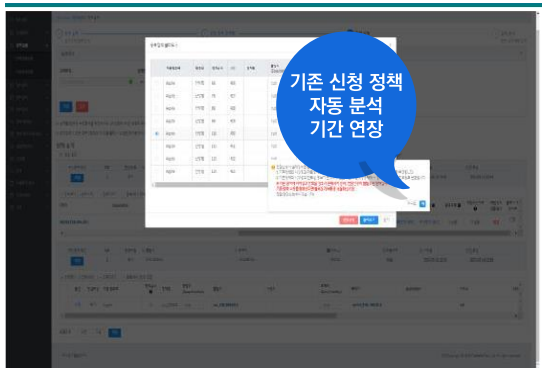
- 요청 정책의 클래스 별 분리 및 병합 논리 설계

정책병합설계



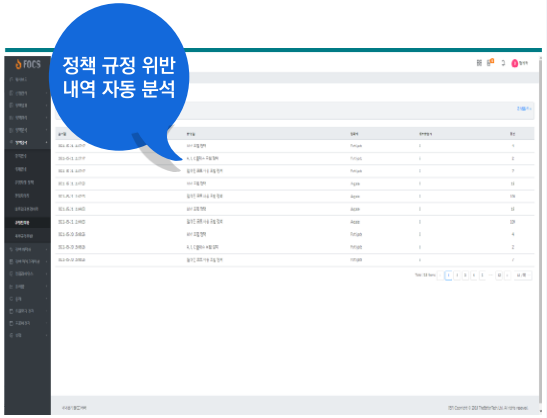
- 기존 유사정책과 병합 설계

정책 연장신청 설계



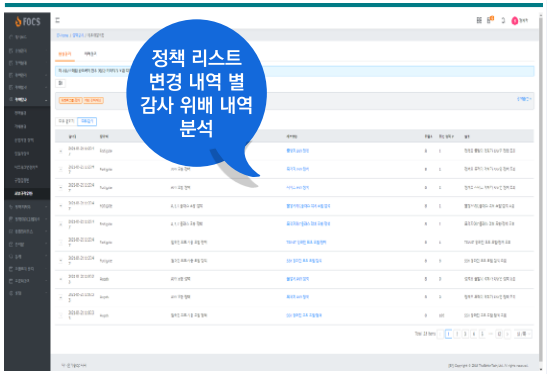
• 기존 정책의 기간 연장 설계 적용

규정집 위반 조회



• 규정집 위반 정책 조회

세부 규정 위반 정책 분석



• 설정한 세부규정 위반 정책

Point ▸▸▸▸ FOCS를 통한 "방화벽정책 최적화환경" 제공

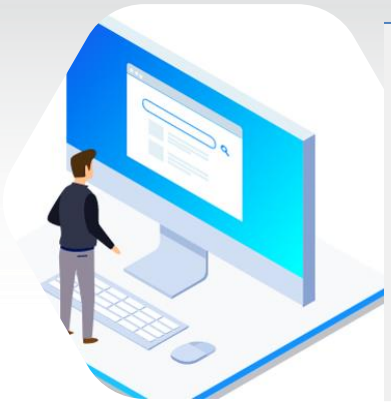
- ☑ 정책 정비 Process 제공
- ☑ 이력관리를 통한 근거자료 확보

STEP 01 **정책 분석**

STEP 02 **정비대상 선별**

STEP 03 **일괄 정비**

STEP 04 **이력 관리**



- 중복 정책
- 미사용 정책
- 과다 허용 정책
- 기간 만료 정책
- 규정위반 분석
- 완전 중복 객체
- 양방향 정책 분석
- 실사용률 정책 기반 통신 성공 정책
- 유사정책 분석
- 정책 삭제
- 정책 순서 변경
- 누가/언제/무엇을 작업 했는지에 대한 이력 관리

Point ▸▸▸▸ 정합성높은 "정책분석데이터" 제공

- 다양한 기준의 정책 분석 데이터 제공
- 이력관리를 통한 **근거 기록** 제공

중복 정책
- 완전 중복 객체 / 정책
- Redundant 객체 / 정책
- Shadowed 객체 / 정책

미사용 정책
- 방화벽 로그 기반 미사용 정책
- 실사용률 Hit Count Zero인 정책

과다허용 정책
- 실사용률 기반 모든 정책 분석
- 과다허용정책 TCP FLAG분석

기간만료 정책
- 기간 만료 정책

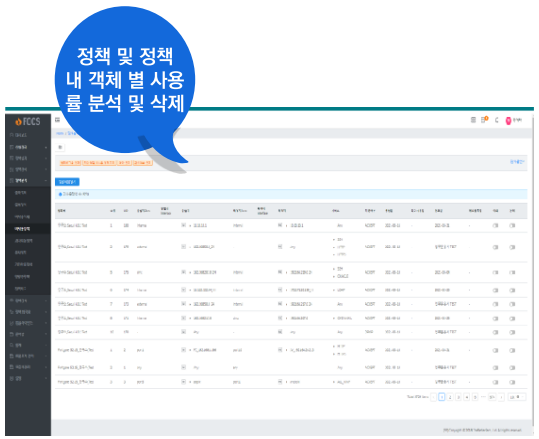
중복 정책 분석
Action ▫ 개별 / 일괄 정비 기능
Action ▫ 참조 / 미참조 여부 확인
Action ▫ 부분 / Any 포함 중복 정책 정보 제공

미사용 정책 분석
Action ▫ 미사용 정책이면서 미참조 객체 / 정책
Action ▫ 미사용 정책 Tag로 기본 정책 삭제 방지

과다허용 정책 분석
Action ▫ 실사용률 분석정보 활용
Action ▫ C / D Class 별 세분화 지원

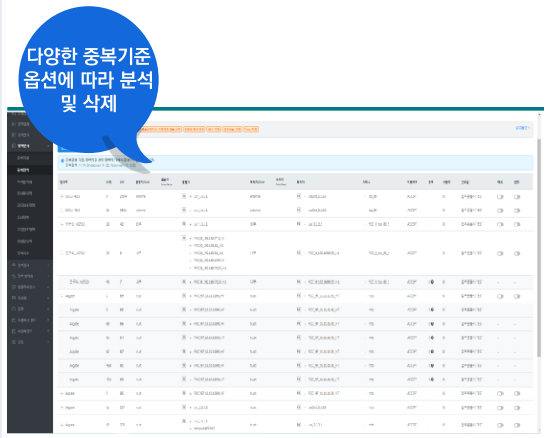
기간만료 정책 분석
Action ▫ 기존 만료 정책 일괄조회 및 삭제
Action ▫ 삭제된 정책 이력관리
Action ▫ 신청서 기반 만료정책 안내 (7/3/1일 전)

정책 사용률 분석



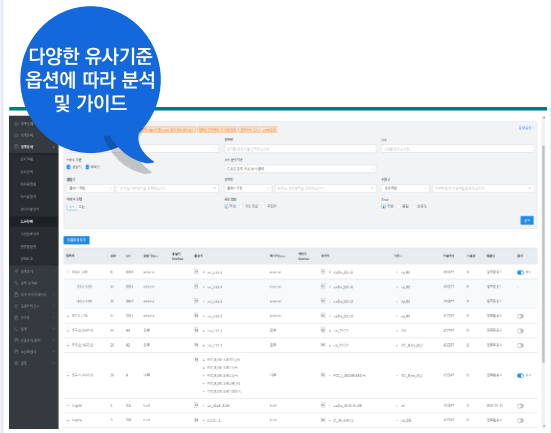
- 사용/미사용 정책 및 정책 내 객체 사용율 분석

중복 정책 분석



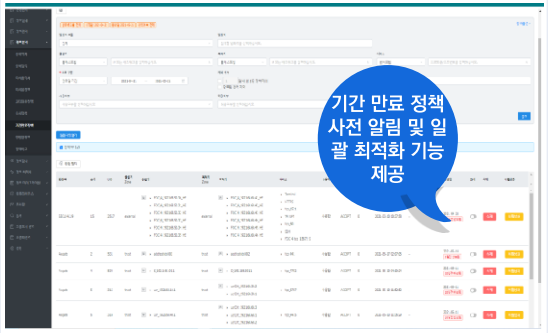
- 방화벽에 있는 중복된 정책 분석

유사 정책 분석



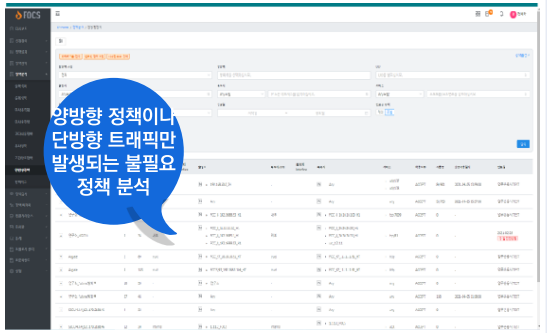
- 방화벽에 있는 클래스 대역 및 중복 유사 정책 분석

기간 만료 정책



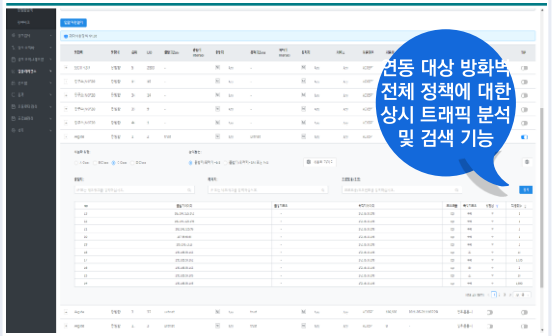
- 기간 만료된 정책 분석/삭제 및 비활성화

양방향 정책 분석



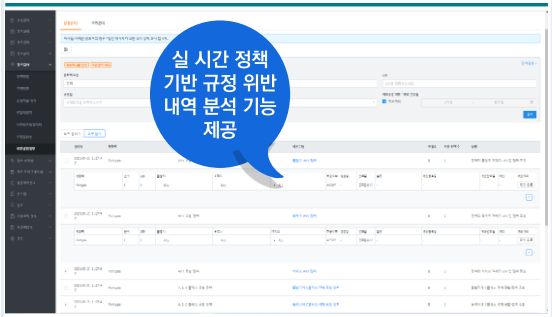
- 양방향 정책 분석 및 실제 사용되는 트래픽 조회

과다 허용 정책 분석



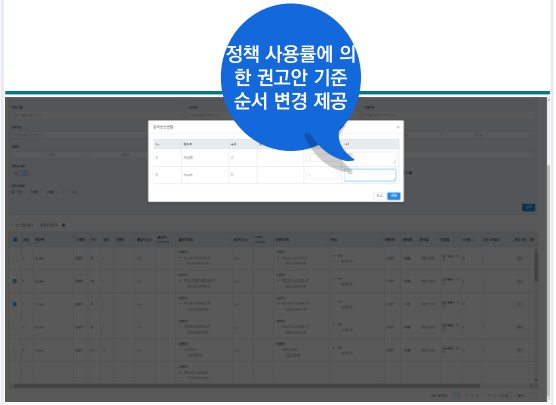
- 클래스 별 TCP Flag 출발지, 목적지 세분화 분석

규정 위반 정책 분석



- 컴플라이언스 규정 설정에 위배되는 정책분석

정책 순서 변경(1)

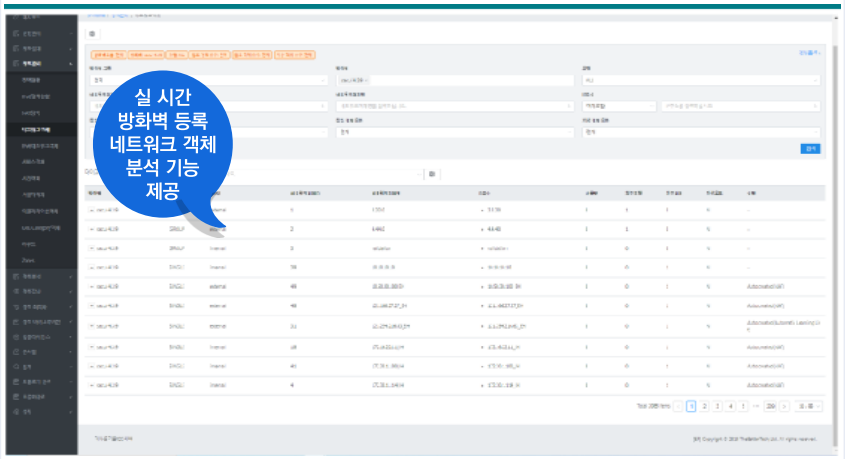


- 사용율이 높은 정책 순서 변경

정책 순서 변경(2)

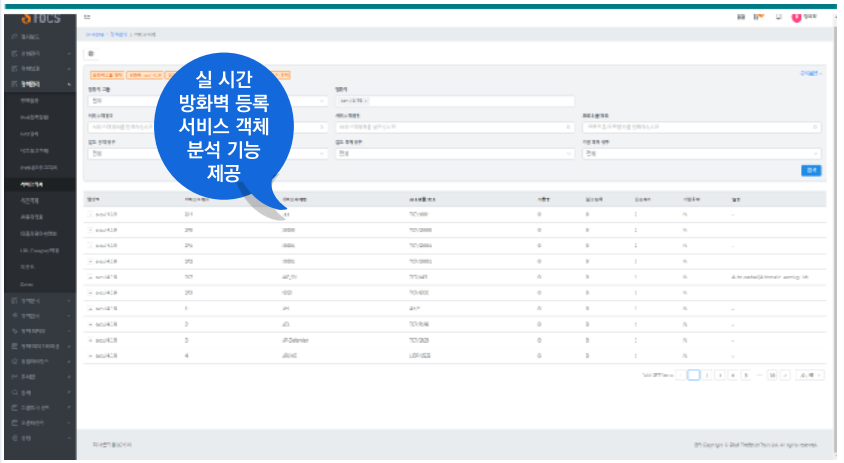
- 순서 변경 내역에 대한 이력 관리 기능

네트워크 객체 분석



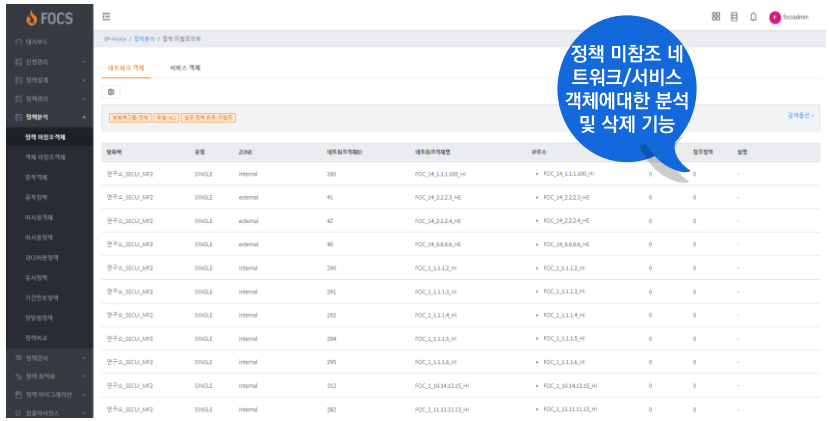
• 방화벽에 등록된 네트워크 객체 분석

서비스 객체 분석



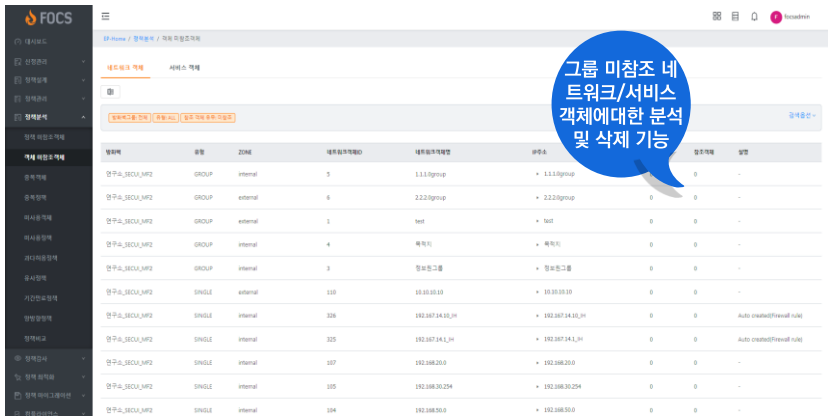
• 방화벽에 등록된 서비스 객체 분석

정책 미참조 네트워크/서비스 객체 분석



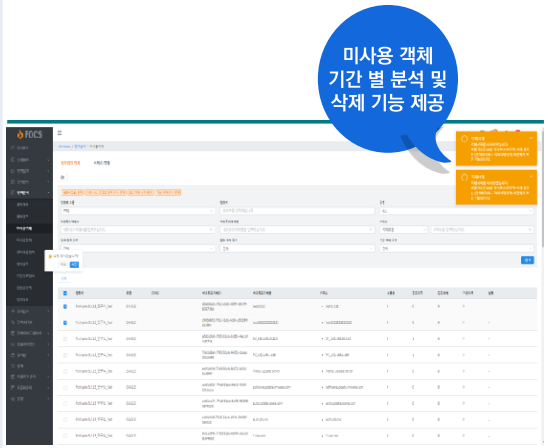
- 정책에 참여되지 않은 네트워크/서비스 객체 분석 및 삭제

그룹 미참조 네트워크/서비스 객체 분석



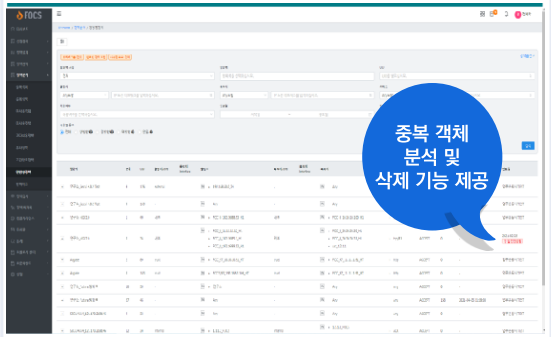
- 그룹에 참여되지 않은 네트워크/서비스 객체 분석 및 삭제

미사용 객체 삭제



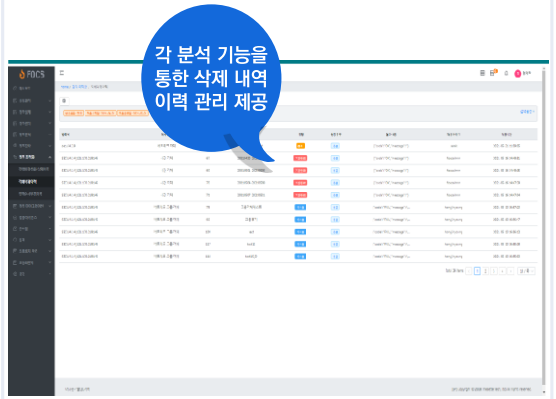
- 미사용 객체 분석 및 일괄 삭제

중복 객체 삭제



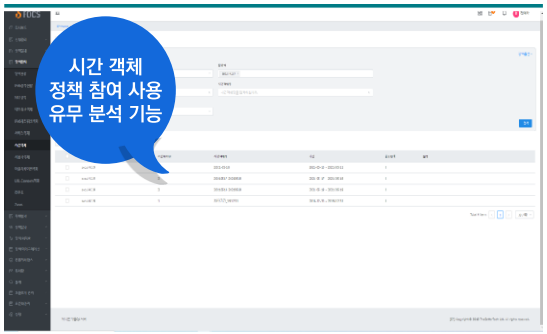
- 방화벽에 존재하는 동일한 불필요 객체 분석 및 일괄 삭제

객체 삭제 이력관리



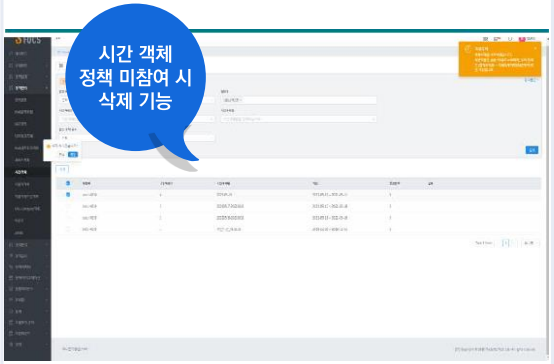
- 객체 삭제 이력 조회/관리

시간 객체 분석



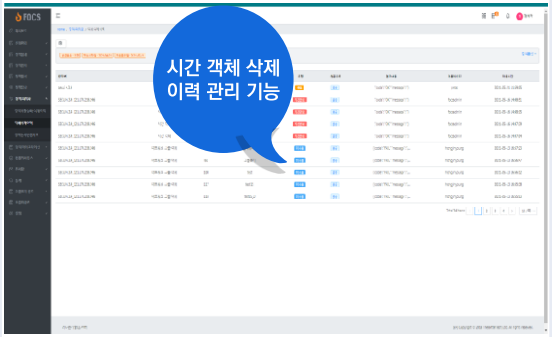
• 방화벽에 등록된 시간 객체 분석

시간 객체 삭제

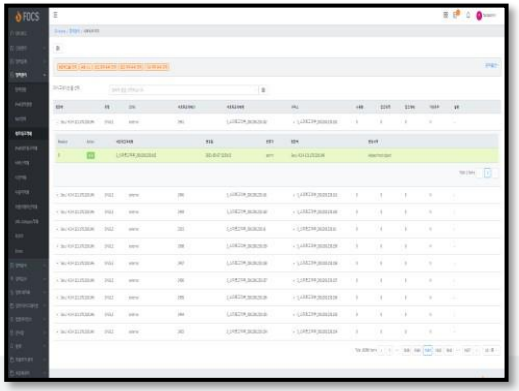


• 방화벽에 등록된 시간 객체 삭제

시간 객체 삭제 이력 조회

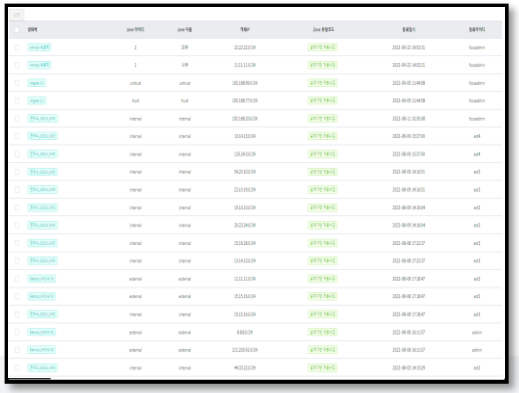


• 방화벽에 등록된 시간 객체 삭제 이력 조회



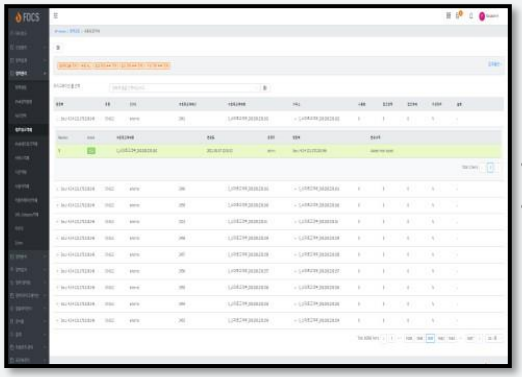
정책 현황을 통한 이력 관리

- 전체 방화벽 정책 이력 Viewer 제공
- 정책 신규 및 변경 이력 확인 가능
- 정책 룰 순서 확인 가능



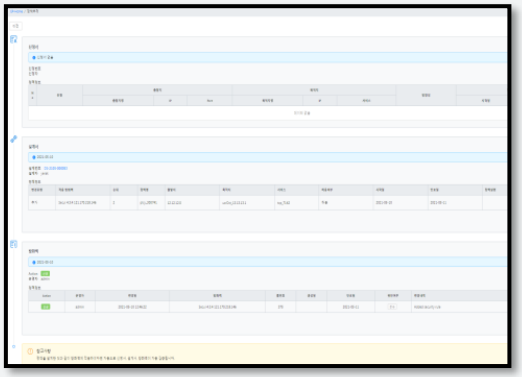
ZONE 정보 자동 매핑

- 딥러닝 기술을 통한 ZONE 정보 자동 매핑 관리



네트워크객체 현황 관리

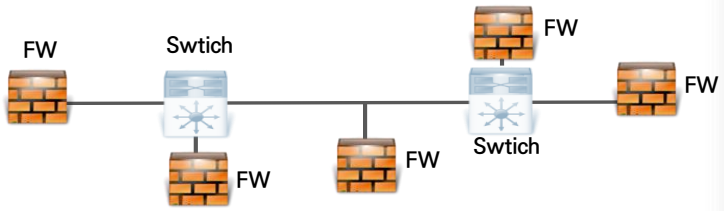
- 중복 객체를 방지하기 위한 현황 제공
- 다양한 조건 검색을 통한 이력 확인



정책 추적을 통한 이력 관리

- 정책 추적을 통한 규정 보안 위반 내역 및 변동 내역 확인 가능
- 정책 별 이력 및 근거 문서 자동 매핑

기존 토폴로지 맵 구성 기술



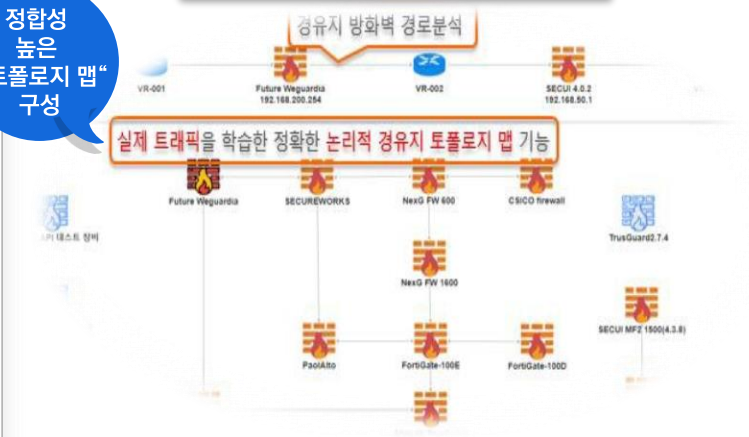
기존 토폴로지 맵 기술

- 방화벽 인터페이스(ZONE)/라우팅정보 기반 정보 활용 토폴로지 구성
- 토폴로지 맵에 기반한 추천 방화벽 정보가 맞지 않아 방화벽 설계 시 제공 데이터에 대한 신뢰도 이슈 발생
- 브릿지 모드 사용시 경유지 분석 정합성 낮음

Sophisticated

FOCS 토폴로지 맵 구성

정합성 높은 " 토폴로지 맵" 구성



FOCS 토폴로지 맵 적용기술

- 실트래픽 수집 및 학습을 통한 정확한 경유지 토폴로지 맵 제공
- 실 트래픽 기반기술과 방화벽 인터페이스(ZONE)/라우팅 정보 기반 정보를 더하여 정확한 방화벽 경유지 분석
- 정확한 방화벽 경유지 분석을 통한 신청정책 설계/적용으로 보안업무 효율성 증대

컴플라이언스

컴플라이언스 규정을 통한 보안 준수 및 보안 위반 여부 실시간 모니터링 제공

변경이력조회

- 신규,삭제,변경(정책,객체) 이력
- 네트워크 (라우팅,Zone)이력
- 일 단위 전일자 정책 변경 이력

운영자별 정책 이력조회

- 운영자별 정책, 객체 작업(신규,삭제, 변경)이력
- 통합 관리 페이지를 통한 정책 및 객체 현황 및 이력 추적

규정위반 정책조회

- 설정된 규정집 위반 정책 조회
- 설정한 세부규정에 위반되는 정책조회
- 감사 규정 위반 이력 조회 및 관리

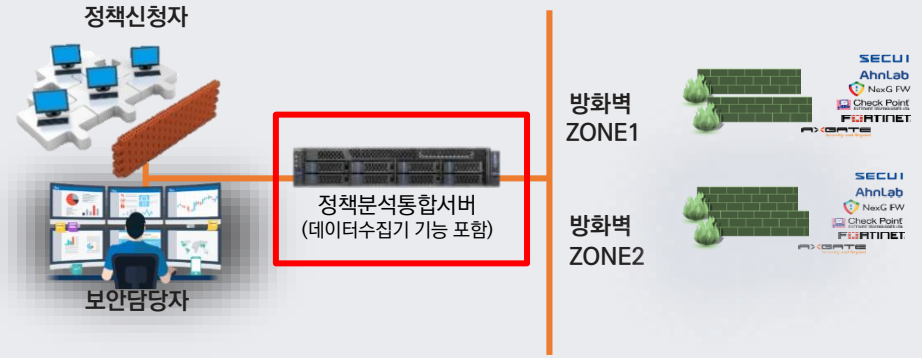
Point ▸▸▸▸ 방화벽 정책변경 현황을 포함한
"요약 및 근거자료 보고서" 제공

- ✔ 정책 변경 현황
- ✔ 90일 이상 미 사용정책 및 만료 정책
- ✔ 계정별 정책변경 이력 현황
- ✔ 계정 변경 현황
- ✔ 컴플라이언스 위반 TOP10

Action	변경일	장비명	운영자	정책 번호	허용 여부	출발지				도착지			
						Zone	그룹	객체	상세IP 주소	Zone	그룹	객체	상세IP 주소
신규	2018-11-14	secui4.3.3	admin@192.168.10.12	274	허용			4IH 김신 청 PC2	192.168.10.251/32			4DH 신청서버2	192.168.20.12/32
신규	2018-11-14	secui4.3.3	admin@192.168.10.12	273	허용			4IH 김신 청 PC	192.168.10.250/32			4DH 신청서버	192.168.20.11/32

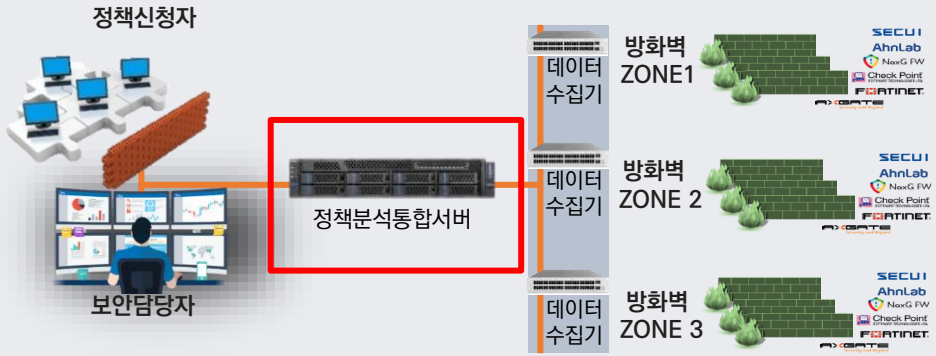
각 세부 상세 정보 제공

방화벽 20대 이내



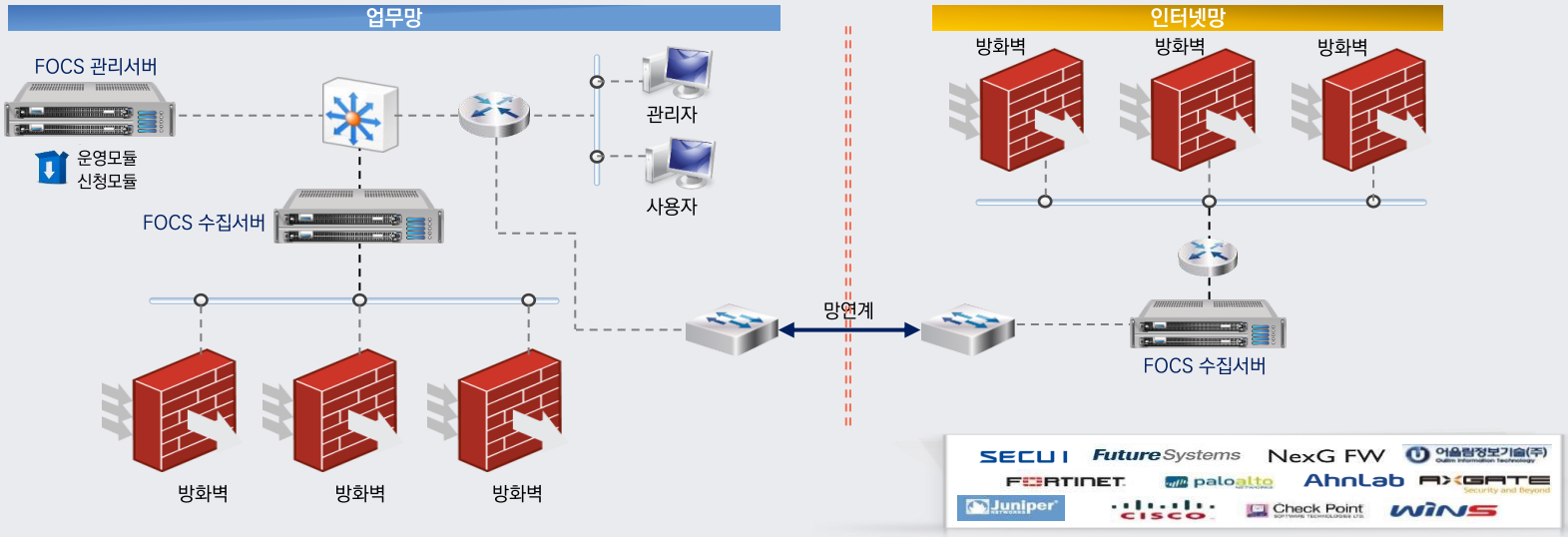
품목	필요수량
운영모듈	1
신청모듈	1
방화벽 연동 for 운영	방화벽 수량
방화벽 연동 for 설계 /적용	
권장 H/W사양 : 16Core CPU/ 64G RAM / 1Tera HDD*2EA	

방화벽 20대 이상 (데이터 수집기 분산 배치)



품목	필요수량
운영모듈	1
신청모듈	1
방화벽 연동 for 운영	방화벽 수량
방화벽 연동 for 설계 /적용	
데이터 수집 모듈	방화벽 20대당 1대
운영모듈 권장 H/W사양: 16Core CPU/ 64G RAM /SSD 960G / 2Tera HDD* 각 2EA (수집 모듈 HW는 운영모듈 HW와 동일_ HDD 2EA 만 제외)	

망분리 환경 (데이터 수집기 망연계 솔루션 앞 배치)



품목	필요수량
운영모듈	1
신청모듈	1
방화벽 연동 for 운영	방화벽 수량
방화벽 연동 for 설계 /적용	
데이터 수집 모듈	방화벽 20대 당 1대
운영모듈 권장 H/W사양: 16Core CPU/ 64G RAM /SSD 960G / 2Tera HDD* 각 2EA (수집 모듈 HW는 운영모듈 HW와 동일_ 2Tera HDD 2EA 만 제외)	

제품특징

- 신청/설계/적용/분석/감사 전 과정 연계 관리
- 통합 관리 대시보드를 통한 정책관리업무 현황 실시간 모니터링
- 실시간 규정준수 위반 정책 모니터링을 통한 상시 감사실행
- 실무적 결재라인 업무를 지원하는 유연한 정책 신청/설계/적용 프로세스
- 그룹별 (운영자,방화벽,날짜)방화벽 정책 변경 관리

구분	관리서버(H/W)	수집서버(H/W)
CPU	Intel 32Core	Intel 32Core
메모리	DDR4 64GB	DDR4 64GB
저장장치	SSD 2TB *2EA (RAID)	SSD 2TB *2EA (RAID)
NIC	1G Dual Port NIC	1G Dual Port NIC
전원	Dual Power Supply	Dual Power Supply

7. 주요 레퍼런스

구분	고객사	구축내용	사업년도	보안시스템
금융	하나카드	신청/운영/설계/적용	2021.01	체크포인트 / 시큐아이 /포티넷
	하나캐피탈	신청/운영/설계/적용	2020.12	시큐아이 / 엑스게이트
	하나손해보험	신청/운영/설계/적용	2023.03	시큐아이
	Sh 수협은행	신청/운영/설계/적용	2021.01	시큐아이 / 안랩
	애큐온저축은행	신청/운영/설계/적용	2021.01	포티넷 / 팔로알토 /시큐아이
	한화투자증권	신청	2020.01	포티넷/ 시큐아이 / 엑스게이트
	meritz 메리츠증권	신청	2020.02	포티넷 / 시큐아이
	IBK기업은행	신청/운영/설계/적용	2021.09	시큐아이 / 안랩 / 넥스지
	KB 저축은행	신청/운영/설계/적용	2021.11	시큐아이 / 안랩
	신한EZ손해보험	신청/운영/설계/적용	2023.08	팔로알토/포티넷/NHN클라우드 SG
	수산업협동조합중앙회	신청/운영/설계/적용	2023.11	안랩 / 퓨처
공공 / 기업	우정사업본부	신청/ 설계	2018.07	시큐아이
	KORAIL	신청/운영/설계/적용	2020.01	시큐아이 / 안랩
	국토교통부	신청/운영/설계/적용	2020.11	시큐아이 / 안랩
	한국동서발전㈜	신청/운영/설계/적용	2020.11	포티넷 / 팔로알토 /시큐아이 / 휴네시온
	aT 한국농수산식품유통공사	신청/운영/설계/적용	2020.11	시큐아이
	한국재정정보원	신청/운영/설계/적용	2021.09	시큐아이 / 소포스
	한전KDN	신청/운영/설계/적용	2021.12	시큐아이
	COCON	신청/운영/설계/적용	2022.03	시큐아이 / 안랩
	한국서부발전㈜	신청/운영/설계/적용	2022.07	시큐아이
	통영시	운영/설계/적용	2023.02	시큐아이
	ESTsoft	신청/운영/설계/적용	2022.02	시큐아이 / 안랩
	한국남부발전㈜	신청/운영/설계/적용	2023.11	시큐아이 / 팔로알토
	경기신용보증재단	운영/설계/적용	2023.12	엑스게이트
	진주시	운영/설계/적용	2024.02	안랩
	산청군	운영/설계/적용	2024.03	안랩 / 엑스게이트 / 시큐아이

방화벽(국산/외산 방화벽)들의 신속한 연동을 지원 (신규 버전일 경우 2~3주 연동지원)

Vendor	Device		비고
SECUI		SECUI MF2 / BlueMAX	모든 버전 지원
FORTINET		FortiGate	모든 버전 지원
FutureSystems		FUTURE XTM	모든 버전 지원
NexG FW		NexG	모든 버전 지원
paloalto		Paloalto	모든 버전 지원
AhnLab		Ahnlab TrusGuard	모든 버전 지원
어울림정보기술(주) Outim Information Technology		SECUREWORKS IPSWall	모든 버전 지원
AXGATE Security and Beyond		AXGATE	모든 버전 지원
JUNIPER NETWORKS		SSG	모든 버전 지원
CISCO		Cisco ASA	모든 버전 지원
CHECK POINT		CheckPoint	모든 버전 지원
WINS		스나이퍼NGFW	모든 버전 지원
XN systems		Neo Box	모든 버전 지원

자동화된 정책관리를 통해 업무 표준화 완성!!

Process

- 특허받은 방화벽 정책 대용량 Syslog 처리
- 신청 / 분석 / 적용까지 정확한 정책관리 운영지원
- 방화벽 정책 통합관리 솔루션이 제공하는 신뢰도 있는 분석 데이터 제공
- 사용률 분석을 통한 과다허용 세분화 정책 지원

Technology

- 방화벽 정책의 신청, 설계, 적용 및 감사에 대한 체계적인 운영 절차 및 서비스 제공
- 정책의 신청, 설계 적용 및 결재가 단일 솔루션을 통해 기능을 제공하여 업무 자동화 제공

Operation

- 365일 방화벽 정책관리 서비스 운영환경 지원
- 방화벽이나 네트워크의 변경 발생시에도 안정적인 보안운영 환경 제공

효율화

- 보안담당자의 효율적 업무 관리
- 이기종 보안설비 활용/관리 편의성 제공
- 보안정책 운영상태 및 현황 실시간 공유
- 보안감사 및 컴플라이언스 대응

최적화

- 정책 신청자와 보안 담당자간 협업체계 지원
- 보안서비스 요구사항 적기제공으로 고객만족도 향상
- 방화벽 정책의 중복정책 / 불필요 서비스 제거를 통하여 보안설비 성능 향상 제공

안정화

- 자동화 및 실시간 모니터링으로 인적 실수 요인 차단
- 보안정책 신청/점검/최적화/적용 Process 자동화
- 보안정책 유효성 검사 및 Lifecycle 관리 자동화


감사합니다.
㈜싸이버텍홀딩스