

Network DLP (Data Loss Prevention)

Venus/CS 3.0

개인/내부정보 유출방지 시스템

Contents



01 제안 개요

02 제안시스템 소개

01

제안 개요

- 제안 배경
- 도입 필요성

제안 배경

연도별 개인정보 유출 신고 현황

연도별 개인정보 유출신고 현황

단위: 건

관련법	신고기준	신고접수 현황								
		2011	2012	2013	2014	2015	2016	2017	2018	
개인정보보호법	1건건*이상/5일내	1	12	6	40	8	-	14	28	
정보통신망법	1건 이상/24시간 내	-	19	7	100	17	40	50	205	
합 계		1	31	13	140	25	40	64	233	

개인정보보호법 강화, 징벌적 배상 법령 발효!

개인정보 관련 법률

소관부서	규제대상 사업자	개인정보의 종류	법률	구분
행정자치부	공공기관 오프라인사업자 CCTV설치자 기타 개인정보처리자	공공기관 개인정보 민간영역 개인정보 개인영상정보	개인정보보호법	일반법
방송통신위원회	정보통신서비스 제공자 위치정보 사업자	온라인 정보 (개인)위치정보	정보통신망법 위치정보법	특별법
금융위원회	신용정보회사 등 금융회사	신용정보 금융거래정보	신용정보법 전자금융거래법	
보건복지부	의료기관	의료정보	의료법	
교육부	교육기관	교육정보	교육기본법	

개인정보보호법

제24조(고유식별정보의 처리 제한)

- ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.
- ④ 행정안전부장관은 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다.

제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24.>

제31조(개인정보 보호책임자의 지정)

- 2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
- 6. 개인정보파일의 보호 및 관리·감독

제34조(개인정보 유출 통지 등)

① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

- 1. 유출된 개인정보의 항목
- 2. 유출된 시점과 그 경위
- 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보



도입 필요성

모니터링 데이터양의 증가



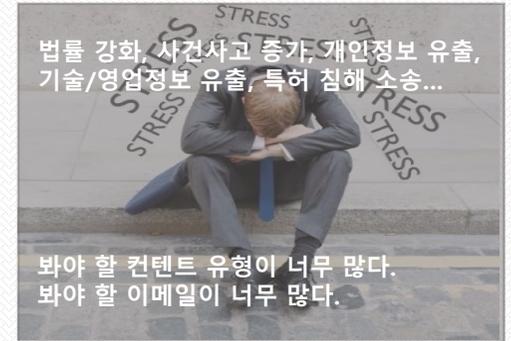
데이터의 지속적인 증가

모니터링 대상의 다양화



유출 수단 및 패턴의 다양화

보안 관리자 업무량의 한계



보안 및 유지관리 인력의 비용 증가

보안사고를 방지하기 위한 신속, 효율, 정확한 개인/내부정보 유출방지 시스템 도입 필요

02

제안시스템 소개

- Venus/CS 3.0 개요
- Venus/CS 3.0 주요기능
- Venus/CS 3.0 시스템 구성

Venus/CS 3.0 개요

업무용 정보통신수단(메일, 메신저 등)으로 발송된 개인정보 및 내부정보를 사전에 정의된 룰에 의해 실시간 차단과 모니터링이 가능한

개인/내부정보 필터링에 특화된 보안시스템

사용자 중심의
직관적인 UI

- 01 Web 기반의 통합 대시보드
- 02 관리자 중심의 대시보드 관리 지원
- 03 다양한 브라우저 환경을 지원

강력한
내부정보 필터링

- 01 개인/내부정보 차단 및 모니터링
- 02 비업무사이트 접속 차단 및 모니터링
- 03 암호화 트래픽 (HTTPS) 분석 지원

대용량 데이터
고속 분석

- 01 대용량 로그 데이터의 빠른 검색 환경
- 02 개인정보 유출 경로 상세 분석
- 03 특정 사용자 별 정보 유출 이력 관리

Venus/CS 3.0 주요 기능

메인화면 | 대시보드

The dashboard displays the following data cards:

- 패턴(개인정보)메시지: 2,424 / 2,424
- 패턴(위협행위)메시지: 147,188 / 147,188
- 커워드(메약어): 0 / 0
- 외부 발신 데이터: 38,833 / 38,833
- 금일 수집 데이터: 375,204
- 1MB 이상 파일 전송: 2,030
- 비업무시간 데이터: 88,767 / 88,767
- 그룹웨어 데이터: 1 / 1

Below the cards are two charts:

- 서비스별 데이터 수집건수**: A bar chart showing data collection counts for various services. The total is 374,022. Services include: 메일 (21), 웹메일 (674), 커뮤니티 (98), 소셜 (72), 영상 스트리밍 (11), 메신저 (95), 파일전송 (136), 노트 (74), 기타 서비스 (374,022), 웹서비스(이분류), and 그룹웨어 (1).
- 외부 메일 발신 서비스 비율**: A pie chart showing the distribution of external email sending services across categories like 그룹웨어, 메일, 커뮤니티, 소셜, 영상 스트리밍, 메신저, and 웹메일.

On the left side, there is a **LOG IN** section for **VENUS/CS V3.0 MEMBERSHIP** with fields for ID and PASSWORD, and a **로그인** button.

데이터 수집현황, 패턴메시지(개인정보/위험행위 등), 발신 서비스별 이용 현황 등을 한눈에 볼 수 있는 직관적인 UI

Venus/CS 3.0 주요 기능

정책

내부정보 유출 차단

사용자 화면



정책 설정



관리자 알림메일



차단 로그



키워드(예약어) 기반의 내부정보 차단 및 로깅

Venus/CS 3.0 주요 기능

정책

비업무사이트 접속 차단

사용자 화면

http://www.itembay.com/intro



지금 접속하려고 하는 사이트에서 **비업무 내용**이 제공되고 있어 이에 대한 접속이 **차단**되었습니다.

차단 동명	비업무사이트 차단 정책
접속 일시	2019-09-06 14:10:23
접속 IP	218.234.36.36
차단 여부	차단
URL	www.itembay.com/

정책 설정

VENUS/CS V3.0

정책 설정

필터링 정책

네트워크를 통해 전송되는 개인정보의 차단, 비업무 사이트의 접속 제한을 할 수 있습니다. SMTP, POP3, HTTP, FTP 등 다양한 유출 경로에 대해 차단, 허용, 승인 정책을 관리 합니다.

IP 필터링 정책 비업무 서비스 필터링 정책 세션 정책 **비업무 사이트 차단 정책** 콘텐츠 정책

순서	적용	정책명	출발지	카테고리	동작	로그남김	동작스케줄	동작만료일
1	ON	비업무사이트 차단 정책	* 새	유해정보>유해사이트,게임>온라인게임,게임>PC게임.....(152)	차단	ON	일~토 00:00-23:59	기간제한없음

차단 로그

VENUS/CS V3.0

차단 로그

비업무 사이트 차단 정책

비업무 사이트 차단 정책 로그 정보를 조회합니다.

No	날짜	차단상태	정책이름	URL	출발지 이름	출발지 적금	출발지 부서	출발지 IP
1	2019-09-06 14:53:56	차단	비업무사이트 차단 정책	www.itembay.com/	이주형	과장	ESS팀	218.
2	2019-09-06 14:11:40	차단	비업무사이트 차단 정책	www.itembay.com/	이주형	과장	ESS팀	218.
3	2019-09-06 14:10:23	차단	비업무사이트 차단 정책	www.itembay.com/	이주형	과장	ESS팀	218.

유해사이트 DB를 활용한 비업무 사이트 차단 및 로깅

Venus/CS 3.0 주요 기능

분석

데이터 관계 분석

LIST

No	메일ID	*수집수	전체패킷량
8	navou@xcurenet.com	16	1.2MB
10	diclever@dsum.net	16	82.9KB
9	cleverdi	14	919.5KB
14	shinmk1009	11	1.8KB
2	stardom1290@hanmail.net	9	45.5MB
6	cleverdi@dreamwiz.com	6	3.9MB
1	dltpqud1129	4	304.6MB
11	cleverdi@hata.com	4	42.0KB
12	maplebook	3	4.1KB
3	cho.sil20@gmail.com	2	43.5MB
4	sejnyim@hanmail.net	2	27.7MB
5	dltpqud1129@gmail.com	2	6.2MB
7	wind-3lein	2	2.7MB
13	sejnyim@hata.com	2	2.8KB

조회완료: 16

← 관계도

본메일

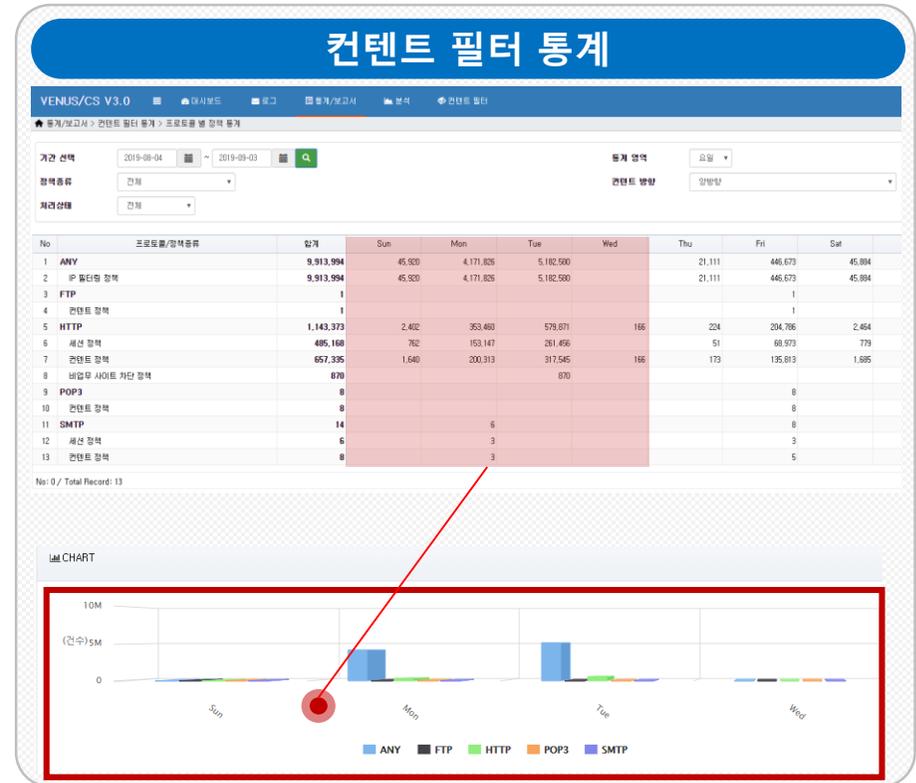
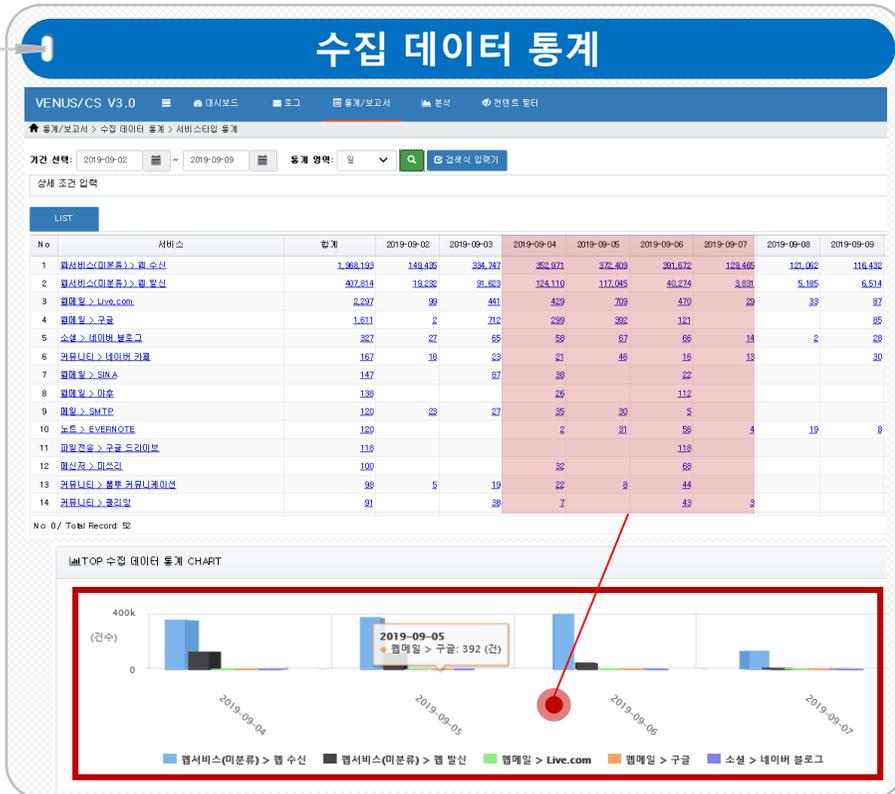
No	관심	알림	제일	내/외부	수/발신	서비스	제목	전체 크기	사용자	부서	직급	발신자	수신자
1	★	📧	1	외부	발신	휴대일 > 구글	w 개인정보 리포트 첨부 ☞	16.2 KB	나윤율(nyovu)	사업부	팀장	나윤율(nyovu@xcu-)	hacker@qq.com
2	★	📧	1	외부	발신	휴대일 > 구글	w 희기울 이사님 ☞	1.1 MB	나윤율(nyovu)	사업부	팀장	나윤율(nyovu@xcu-)	ts.choi@tvoli.com
3	★	📧	1	외부	발신	휴대일 > 구글	w 나윤율 이력서 송부 드립니다. ☞	73.6 KB	나윤율(nyovu)	사업부	팀장	나윤율(nyovu@xcu-)	insa.kang@tvoli.com
4	★	📧	1	외부	발신	휴대일 > 구글	w 무장님, 감사합니다. ☞	975 Byte	나윤율(nyovu)	사업부	팀장	나윤율(nyovu@xcu-)	ts.choi@tvoli.com
5	★	📧	1	외부	발신	휴대일 > 구글	w 나윤율입니다. ☞	91.8 KB	나윤율(nyovu)	사업부	팀장	나윤율(nyovu@xcu-)	ts.choi@tvoli.com
6	★	📧	1	외부	발신	휴대일 > 구글	w 나윤율 이력서 ☞	136 Byte	나윤율(nyovu)	사업부	팀장	나윤율(nyovu@xcu-)	shpark@samsung.com

데이터 관계 분석을 통한 정보 유출 추적

Venus/CS 3.0 주요 기능

통계

수집 및 차단 통계



관리자 편의의 다양한 형식의 통계데이터 분석 및 사용자 용도에 따른 리포트 제공

Venus/CS 3.0 주요 기능

보고서

리포트

The screenshot displays the Venus/CS 3.0 reporting interface. On the left, a sidebar titled '통계 항목 선택' (Select Statistics Item) contains several options with checkboxes. The '서비스 TOP10' (Service TOP10) option is selected, indicated by a red box and a red circle. The main area shows a 'Report' window titled 'VENUS/CS V3.0 Report' with a date of '2019년 9월 2일' and a period of '기준일: 2019-09-26 ~ 2019-09-02'. Below this is a table for '서비스 TOP10' with columns for '순위' (Rank), '서비스' (Service), and '건수' (Count). A red box highlights the table, and a red circle marks the '서비스' column header. At the bottom, a dialog box asks '10. 의 export_excel_20190909_161510.xlsx(를) 열거나 저장하시겠습니까?' (Do you want to open or save export_excel_20190909_161510.xlsx?).

순위	서비스	건수
1	웹서비스(미분류) > 웹 수신	1,270,335
2	웹서비스(미분류) > 웹 발송	109,658
3	웹메일 > 구글	447
4	커뮤니티 > 네이버 카페	360
5	소셜 > 네이버 블로그	285
6	커뮤니티 > 롤리앙	107
7	커뮤니티 > 뽀뿌 커뮤니티케이션	106
8	웹메일 > Live.com	87
9	파일전송 > OneDrive	57
10	웹메일 > 네이버	43

사용자 용도에 따른 통계 보고서 및 추출(내보내기) 제공

Venus/CS 3.0 주요 기능

감사로그 | 관리자 감사 로그

VENUS/CS V3.0

VENUS/CS V3.0 > 감사로그 > 운영자 감사 로그

운영자 감사 로그

운영자 감사 로그 위함은 운영자들의 작업 내역을 조회 합니다.
운영자 감사 로그는 삭제되지 않습니다.

2019-09-09 ~ 2019-09-09 검색어를 입력하세요.

시스템관리자 (sysadmin) - 상위메뉴 선택 - - 작업메뉴 선택 -

No	작업시간	운영자 ID	운영자 명	운영자 IP	상위 메뉴	작업메뉴	작업행위	정보
1	2019-09-09 11:39:56	sysadmin	시스템관리자	218.	운영 관리	장비 이벤트 로그	조회	[조회] 기간: 20190909 - 20190909
2	2019-09-09 11:37:56	sysadmin	시스템관리자	218.		장비 트래픽 통계	조회	[조회] 기간: 20190904 - 20190904
3	2019-09-09 11:37:47	sysadmin	시스템관리자	218.		장비 트래픽 통계	조회	[조회] 기간: 20190909 - 20190909
4	2019-09-09 11:37:46	sysadmin	시스템관리자	218.	현업트 필터	필터링 정책	조회	[IP 필터링 정책 조회] 프로토콜: 전체
5	2019-09-09 11:37:45	sysadmin	시스템관리자	218.	현업트 필터	필터링 정책	조회	[IP 필터링 정책 조회] 프로토콜: 전체
6	2019-09-09 11:37:45	sysadmin	시스템관리자	218.		장비 트래픽 통계	조회	[조회] 기간: 20190909 - 20190909
7	2019-09-09 11:37:42	sysadmin	시스템관리자	218.		장비 트래픽 통계	조회	[조회] 기간: 20190909 - 20190909
8	2019-09-09 11:37:40	sysadmin	시스템관리자	218.	현업트 필터	필터링 정책	조회	[IP 필터링 정책 조회] 프로토콜: 전체
9	2019-09-09 11:37:30	sysadmin	시스템관리자	218.	시스템	접속정보	로그인	로그인 성공
10	2019-09-09 11:36:34	sysadmin	시스템관리자	218.	시스템	접속정보	로그인	로그인 성공

오남용 통제를 위해 관리자 정책 이력 세부 감사 로깅

Venus/CS 3.0 주요 기능

기타

인사 연동 및 알림 설정

인사 연동

인사 연동 설정

인사 정보 관리 방법

직접연동 자동연동

자동 연동 설정

- 파일 위치

- 컬럼 구분자

- 요일 설정

전체 일 화 수 목 금 토

- 시간 설정

메시 경각

- 실행

- 컬럼 순서

1. 아이디
2. 이름
3. E-mail(중복가능)
4. IP(중복가능)
5. 회사 코드
6. 외사명
7. 시업장명
8. 부서명
9. 직급명
10. 재직명
11. skip this column(중복가능)

인사DB 정보와 연동하여 부서별 사용자 객체 정렬 및 자동갱신 기능 제공
(자동연동 시 인사 DB에서 컬럼(변경 가능)을 통한 스케줄 연동)

알림 설정

예약 설정 - 추가 및 수정

예약 알림 설정

1단계

*예약 알림 이름

키워드 Notice

사용여부 사용 미사용

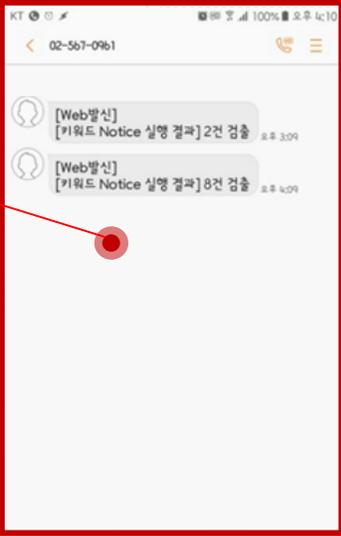
*알림 유형 메일 SMS 화면알림

실행 주기 매주 매일 매시간

실행 시간 0시 절각

* 표시된 항목은 필수

이전



간편한 인사DB 연동 및 다양한 알림 유형을 통해 알림 설정 제공

Venus/CS 3.0 시스템 구성

특장점

설치의 편의성

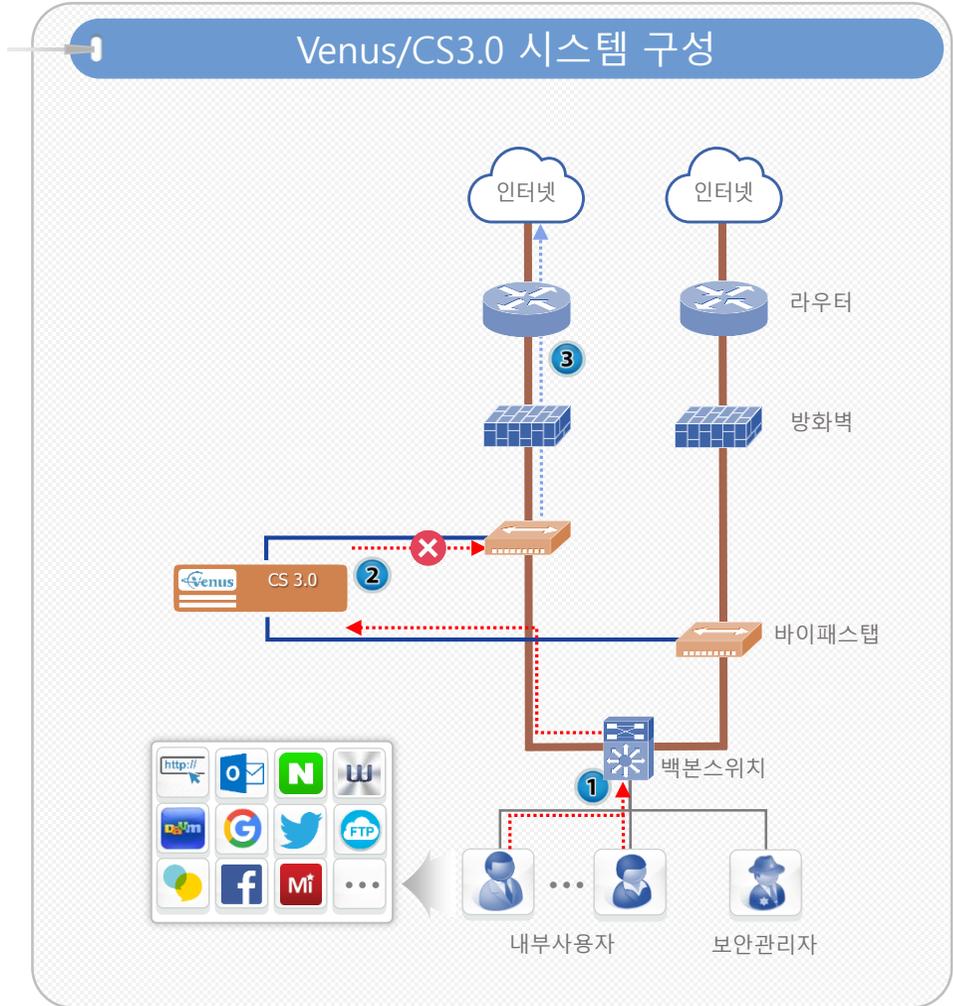
- S/W, H/W 일체형의 Appliance 타입
- Plug & Use 방식의 간편한 설치
- 기존 네트워크 환경 변화 없이 설치

부하 분산 구성

- 네트워크 트래픽 양과 사용자 동시 세션 수에 따른 분산 구조
- 효과적인 분산 처리로 부하 경감

네트워크 통신 가용성

- 하드웨어 및 소프트웨어 엔진 장애 시 네트워크 통신 가용성 보장 (By-Pass TAP 활용)



감사합니다.

영업 및 기술 문의

영 업	본 사	122-826 서울시 은평구 가좌로 276(신사동, J타워 빌딩)
	연 락 처	Tel : 02-567-0961 / Fax : 02-567-0963
기 술	고 객 전 용	helpdesk@xcurenet.com