nurit

네트워크 장비의 보안강화를 위하여 다계층 인증을 위한

BaroPAM 솔루션 소개서

2026. 1.

Ⅰ. 배경 및 변화

1. 기본 보안부터 철저히 해야

"기본 보안부터 철저히 해야"

겉보기에 그럴듯한 보안 조치들이 그동안 우리 사회를 안심시켜 왔을 뿐입니다.

현재의 보안체계로는 정보자산을 충분히 지킬 수 없다는 거, 보안 전문가라면 다 알고 있습니다.

주요 인프라 공격의 85%가 "**패치, 2차 인증(추가 인증), 최소 권한 원칙**" 등 기본적인 수준의 보안을 지키지 않아서 발생한 것으로 나타납니다. (2024년 IBM 보고서)

MS의 조사에 따르면 "**다중 인증(MFA)을 구현하면 계정 공격의 99.9%을 차단**" 할 수 있다고 합니다.

랜섬웨어를 포함한 **침해 사고의 80~90%가 원격 접속과 관련된 문제**입니다. (KISA, 데이터 백업 8대 보안수칙에서 백업 저장소는 백업 전담 인력을 제외하고는 접근을 차단하고, 가능할 경우 OTP 등 다단계 인증을 적용)

보안 솔루션 중 도입해야 할 1순위가 계정도용, 권한상승, **우회/원격접속을 차단할 수 있는 2차 인증 솔루션**입니다.

기본 보안 정책만 지켜도 대부분의 공격은 막을 수 있습니다.

"**망분리 했다고 해커들의 침투를 100% 막을 수 없다**"는 걸 인정하고, "**해커들은 이미 망 내부에 들어와 활동하고 있다**"는 가정으로 보안 전략을 수립해야 합니다.

외부의 해커 또는 내부 사용자가 불법적으로 정보자산에 접근하는 상황을 제한하고, 보안의 위험을 분산함으로써 피해를 최소화해야 합니다.

최근 들어, 중앙 집중식 관리 서버의 운영체제(OS) 및 관리자 계정이 해킹되어, 관리 서버를 장악하고 정보를 유출하여 도용 및 악용하거나, 악성코드 삽입, 정보를 삭제한 후 관리 서버를 무력화시켜 서비스를 불능 상태로 만드는 "**단일 지점 공격**"의 침해사고가 발생하여 기업에 많은 피해를 주고 있습니다.

2. 네트워크 장비 해킹 시 발생 가능한 주요 피해

관리 규정 미비로 관리의 사각지대에 있는 네트워크 장비에 해킹되었을 때 발생할 수 있는 일들은 개인과 조직 모두에게 심각하고 광범위한 피해를 초래할 수 있습니다. 해커는 장비를 통해 시스템에 무단으로 침입하여 다양한 악의적인 활동을 수행할 수 있습니다.

시스템 및 서비스 마비	데이터 유출 및 손상	사이버 공격에 악용	추가적인 침입/통제	금전적/평판적 피해
제일 무서운 것은 네트워크 장비에 물려 있는 장비에 대해 악성 코드를 유포하여 감염되어 상상할 수 없는 재앙이 발생하여 시스템 및 서비스가 마비 되어 상상할 수 없는 재앙이 발생할 수 있음.	민감 데이터 탈취: 고객 정보, 영업 비밀, 금융 정보, 개인 신상 정보 등 중요하고 민감한 데이터를 해커가 훔쳐 갈 수 있음. 데이터 파괴 또는 변조: 시스템의 데이터를 삭제하거나 악의적으로 변조하여 업무 시스템 마비나 혼란을 야기할 수 있음.	해킹된 네트워크 장비가 봇넷(Botnet)의 일부가 되어 다른 목표 시스템에 대한 분산 서비스 거부(DDoS) 공격을 수행하는 데 악용될 수 있음. 장비 자체의 설정이 변경되거나 악성 소프트웨어에 감염되어 네트워크 기능이 제대로 작동하지 않게 되어 전반적인 시스템 다운타임이 발생할 수 있음.	해킹된 장비를 교두보 삼아 내부 네트워크의 다른 서버나 장치로 추가 침투를 시도하여 피해 범위를 넓힐 수 있음. 해커가 장비에 원격 접근 권한을 얻어 장비의 설정을 변경하거나, 악성 스크립트를 실행하는 등 장비를 마음대로 통제할 수 있음.	시스템 복구 비용, 법적 처벌에 따른 벌금, 수익 감소, 고객 이탈 등으로 인해 막대한 금전적 손실을 입을 수 있음. 데이터 유출이나 서비스 마비로 인해 기업이나 조직의 평판과 고객 신뢰도에 치명적인 손상을 입을 수 있음.

3. 네트워크 장비에 대한 보안이 얼마나 중요한지를 일깨워 준 침해사고

2025년 9월경에 발생한 일본 아사히 그룹에 대한 사이버 침해 사고는 단순히 데이터를 암호화하는 것을 넘어, 대규모 개인정보 유출과 함께 생산 및 유통망 전반을 마비시켜 기업 운영에 막대한 피해를 준 대표적인 랜섬웨어 공격 사례로 관리 규정 미비로 관리의 사각지대에 있는 네트워크 장비에 대한 보안이 얼마나 중요한지를 일깨워 준 침해사고.

침해 경로 (공격 과정)

초기 침투 (9월 19일경)는 외부 공격자가 아사히 그룹 내 네트워크 장비를 경유하여 그룹 네트워크에 침입한 후 패스워드 등을 훔쳐 내부 시스템에 접근할 수 있는 권한을 확보함.

공격자는 데이터센터 네트워크에 무단 접근하여 활성 서버와 네트워크에 연결된 일부 PC 장치의 데이터를 동시에 랜섬웨어를 배포하여 암호화함.

이 과정에서 데이터센터 서버에 보관 중이던 개인정보가 외부로 유출되었을 가능성이 확인됨.

대규모 개인정보 유출 우려

피해 규모: 총 약 191만 4천 건의 고객 및 직원의 개인정보가 유출되었을 가능성이 제기됨.

고객센터 문의 이력이 있는 고객의 성명, 주소, 전화번호, 이메일 주소, 성별 등.

직원 및 그 가족 (약 27만 5천 명): 현직 및 퇴직 직원, 그 가족의 성명, 생년월일, 성별, 주소, 전화번호 등.

기타 외부 연락처 (약 11만 4천 명): 경조사 전보 수신자 등의 성명, 주소, 전화번호 등.

시스템 마비 및 경영 활동 차질

시스템 장애: 랜섬웨어 공격으로 인해 그룹의 서버와 컴퓨터 시스템 일부가 마비되고 데이터 접근이 어려워 짐.

운영 중단: 일본 내 생산 라인 다수 가동이 중단되었으며, 온라인 시스템을 통한 수주, 출하, 물류 등 핵심 경영 활동 전반에 심각한 차질이 발생.

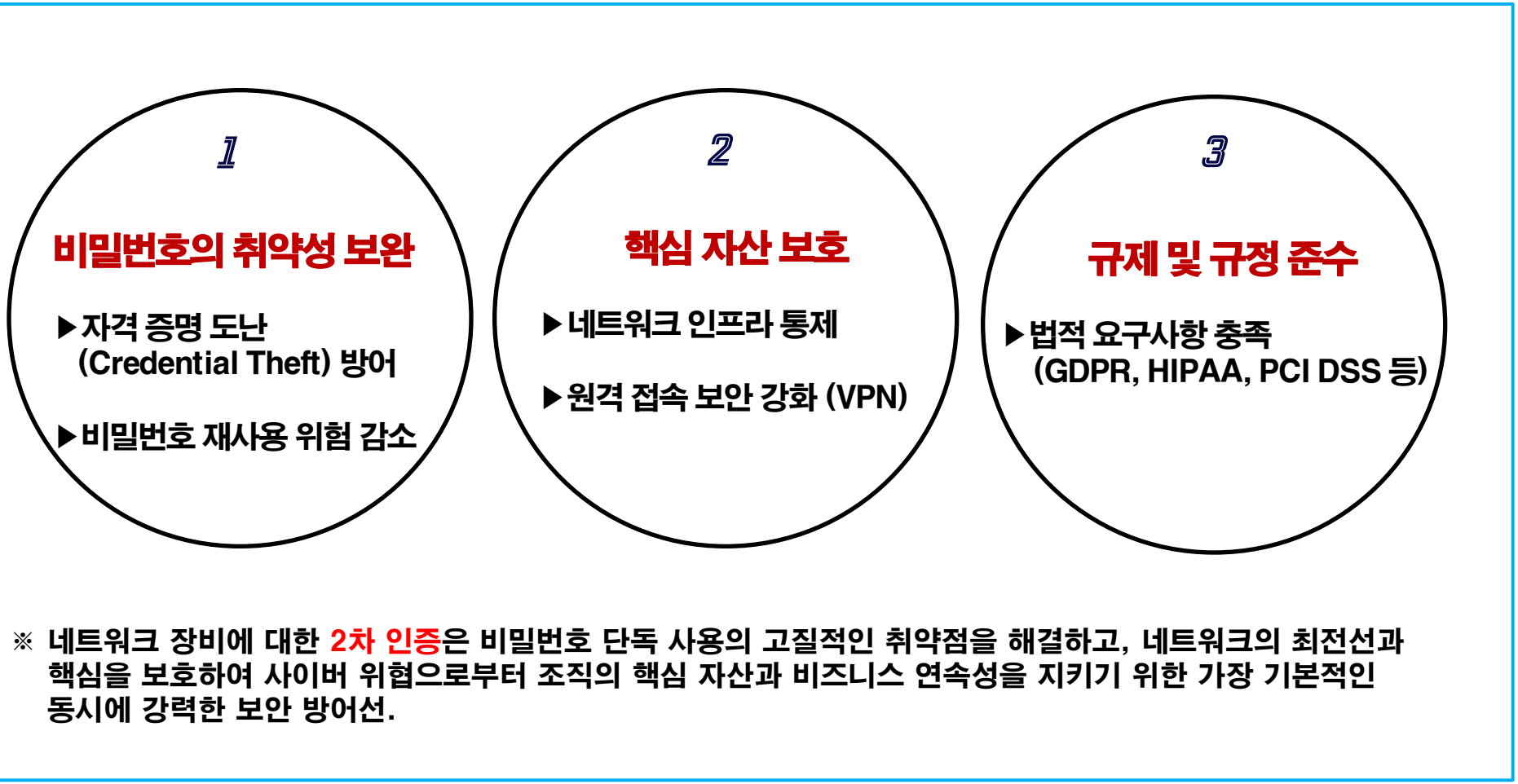
물류 대란: 맥주, 음료 등 제품의 공급이 원활하지 않아 일본 내 레스토랑, 술집, 상점에서 품절 사태가 발생.

매출 감소: 사고 발생 다음 달, 맥주 부문 매출은 전년 동기 대비 90% 수준을 유지했으나, 음료 부문은 60% 수준으로 크게 하락.

복구 지연: 물류 인프라의 완전한 정상화까지는 사고 발생 후 수개월이 소요될 것으로 예상됨.

4. 2차 인증이 필요한 주요 이유

방화벽(Firewall), VPN(Virtual Private Network), L2/L3 스위치 등 네트워크 장비들은 네트워크의 핵심적인 기능을 수행하고 민감한 데이터와 시스템을 보호하는 중요한 역할을 하므로, 만약 하나의 인증 요소(예: 비밀번호)만으로 접근이 허용되면 심각한 위험이 발생할 수 있습니다.



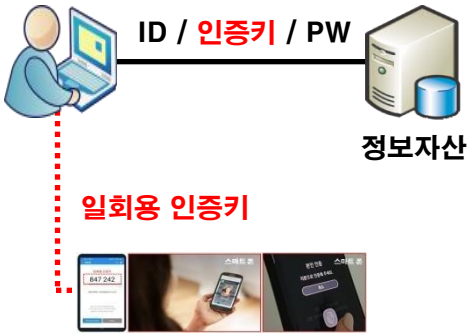
※ 네트워크 장비에 대한 2차 인증은 비밀번호 단독 사용의 고질적인 취약점을 해결하고, 네트워크의 최전선과 핵심을 보호하여 사이버 위협으로부터 조직의 핵심 자산과 비즈니스 연속성을 지키기 위한 가장 기본적인 동시에 강력한 보안 방어선.

2. BaroPAM

1. BaroPAM 이란?

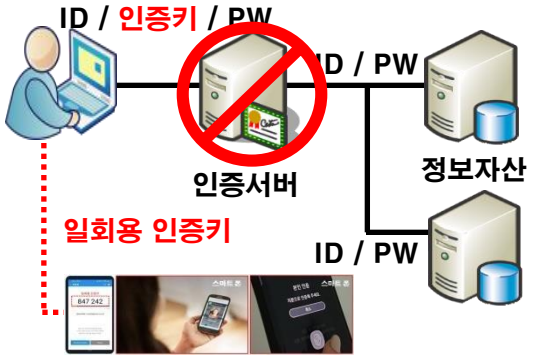
BaroPAM 솔루션은 제로 트러스트 보안 모델로 정보자산의 보안 강화를 위하여 2차 인증(추가 인증)이 필요한 다양한 운영체제와 애플리케이션에 누구나 손쉽게 곧바로 적용할 수 있는 플러그인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식을 기반으로 하는 보안에 최적화된 다계층 인증 체계를 지원하는 솔루션입니다.

정보자산 접근 보안강화



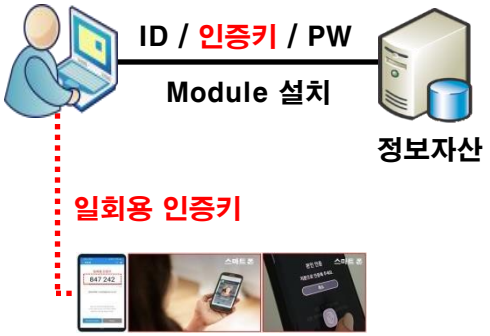
- 외부의 해커 또는 내부 사용자가 불법적으로 정보자산에 접근하는 상황을 제한하여 정보자산의 보안 강화
- 2-Factor 인증으로 기존의 "지식기반 인증"인 ID / PW 인증에 다른 요소인 소유기반/속성기반 인증요소를 추가한 인증기법

서비스의 용이성



- 2차 인증을 별도 인증키 토큰/카드 필요 없이 BaroPAM 앱을 이용하여 인증이 용이함
- 별도 인증서버나 Windows/서버 접근 제어를 관리하는 서버가 필요 없는 구조로 관리/운영비용 절감

손쉬운 적용

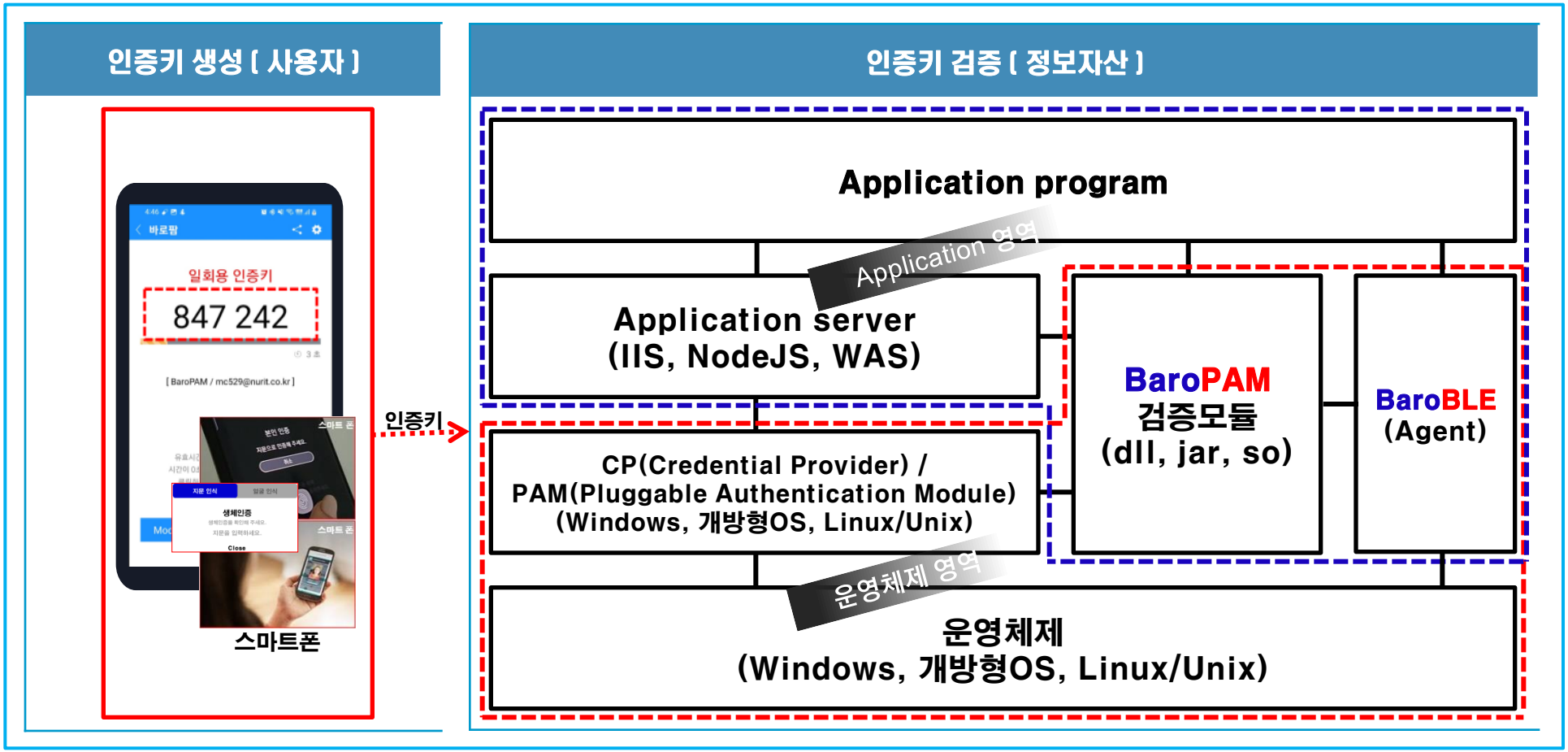


- 각 Windows 또는 서버에 모듈을 설치하는 구조로 간단히 적용 가능
- Windows 또는 서버를 재기동하지 않기 때문에 운영 중에도 적용 가능
- 기존 네트워크 장비의 설정변경 불필요

nurit

2. BaroPAM 아키텍처

BaroPAM 솔루션은 사용자가 일회용 인증키를 생성하는 장치, 일회용 인증키를 적용하는 정보자산, 일회용 인증키를 검증하는 모듈, BaroPAM 앱과 데스크탑의 블루투스/애플리케이션간 통신하는 BaroBLE로 구성되어 있습니다.



2. BaroPAM

3. 솔루션 특장점

BaroPAM 솔루션은 별도의 인증서버가 필요 없는 모듈인증 방식으로 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증을 지원하며, 보안성이 강하고, 단순하고, 관리도 필요 없고, 장애도 없고, 누구나 손쉽게 곧바로 적용하여 사용할 수 있고, 솔루션을 도입할 때 별도의 서버나 DB 같은 추가 도입이 필요 없는 저비용 고효율의 솔루션입니다.

- ▶별도의 인증서버가 필요 없는 모듈인증 방식의 다계층 인증 지원
- ▶빠른 인증속도로 서비스 보장 (평균 인증시간 0.01초 이내)
- ▶BaroPAM 앱 소스 난독화 및 화면 캡쳐 방지 기능 제공
- ▶BaroPAM 앱 실행 시 생체인증(지문인식,얼굴인식) 기능 제공
- ▶전세계적으로 인정된 512Bit 표준 Hash 함수 사용 (HMac-SHA512 / 인터넷 보안표준 IETF RFC 6238)
- ▶금감원에서 권장하는 Time-Sync, 동적 Secret key 방식 지원
- ▶환경 설정 정보를 파일 이외에 MariaDB와 연동 기능 제공
- ▶인증의 제한 횟수 및 제한 시간(예: 30초에 3회) 설정 기능 제공
- ▶중간자(man-in-the-middle) 공격을 예방하는 기능 제공
- ▶빈번하게 발생하는 통신 장애 또는 보안 지역에서도 인증 가능
- ▶매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안 지원
- ▶인증절차 시 인증정보가 위변조 되더라도 우회인증 불가능
- ▶인증 우회(우회기술, 피로공격 등) 불가능
- ▶이상 인증 탐지 및 차단할 수 있는 기능 제공
- ▶간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 가능
- ▶iOS는 자체적으로 본인인증 할 수 있는 기능 제공
- ▶자동 로그인 기능을 악용한 계정 정보 탈취해도 로그인 불가능
- ▶스마트 폰 이용 불가 시 응급 일회용 인증키 제공
- ▶다양한 정보자산 등 2차 인증이 필요한 모든 분야에서 적용가능 (정보자산의 RADIUS 인증 중 PAM/SQL/HTTP 인증도 지원)
- ▶2차 인증에서 허용 / 제외할 수 있는 계정에 대한 ACL 기능 제공
- ▶자유로운 Customizing 및 다양한 응용 프로그램과의 연동 개발 제공 (Java, C, C++ 등의 API 연동)

※ **HMac (Hash-based Message Authentication Code) : 해쉬 기반 메시지 인증 코드**
HMac는 Key를 조합하여 Hash 함수를 구하는 방식으로, 송신자와 수신자만이 공유하고 있는 Key와 메시지를 혼합하여 Hash 값을 만드는 방식이다. 또한 채널을 통해 보낸 메시지가 훼손되었는지 여부를 확인하는데 사용할 수 있으며, Mac 특성상 역산이 불가능하므로, 수신된 메시지 와 Hash 값을 다시 계산하여, 계산된 HMac과 전송된 HMac이 일치하는지를 확인하는 방식이다.

nurit

4. 지원 환경

BaroPAM 솔루션은 누구나 손쉽게 적용할 수 있는 2차 인증(추가 인증)이 필요한 OS, Language, Application, Database, Network 장비, 저장장치, ARM system 등의 다양한 개발 및 운영환경을 지원합니다.

No	구분		내용	비고
1	OS	Windows 계열	Windows 8.1 이상 Windows server 2012 R2 이상	
		Linux 계열	Radhat, CentOS, AlmaLinux, RockyLinux, NAVIX, Oracle linux, Debian, Fedora, Mint, Ubuntu, openSUSE, KaliLinux, 개방형 OS(하모니카OS, 구름OS) 등 Open Linux 지원	
		Unix 계열	AIX, HP-UX, Solaris, FreeBSD, MacOS 등	
2	Language		C, C++, C#, Java, ASP, PHP, PowerBuilder, Delphi, Visual Basic 등	
3	Application	ARM system	Shard object 제공(인증, 암복호화)	
		IIS	dll 제공(인증, 암복호화)	
		NodeJS	jar 제공(인증)	
		WAS	jar 제공(인증, 암복호화)	
4	Database	암복호화	Oracle, Tibero, Cubrid, MySQL, MariaDB, PostgreSQL, SQL Server 등	
		인증	Oracle, MySQL, MariaDB, PostgreSQL 등 RADIUS 인증을 지원하는 데이터베이스	
5	Network 장비		Open Linux 및 RADIUS 인증을 지원하는 장비, OpenVPN은 PAM/RADIUS 인증 지원	
6	저장장치		상용OS를 지원하는 장치.	

3. RADIUS란?

RADIUS(Remote Authentication Dial In User Service, 원격 인증 전화 사용자 서비스 위치)는 네트워킹 프로토콜로 사용자가 네트워크에 연결하고 네트워크 서비스를 받기 위한 중앙 집중화된 인증, 인가, 회계 (AAA, 회계 Accounting은 인증, 인가 후 각종 사후 처리를 맡는다.) 관리를 제공한다. RADIUS는 1991년 서버 접근 인증, 회계 프로토콜로써 Livingston Enterprises, Inc. 에서 개발했다. 그리고 후에 IETF표준으로 등재되었다.

지원 범위가 넓고 유비쿼터스 환경에서도 사용이 가능하기에 ISP와 기업들이 인터넷이나 인트라넷 접근을 관리하거나 무선 네트워크 인증, 통합 메일 서비스 등에 자주 쓰인다. 모뎀, 무선 액세스 포인트, 디지털 가입자 회선, 가상 사설망, TCP 및 UDP 포트, 웹 서버 등에 사용된다.

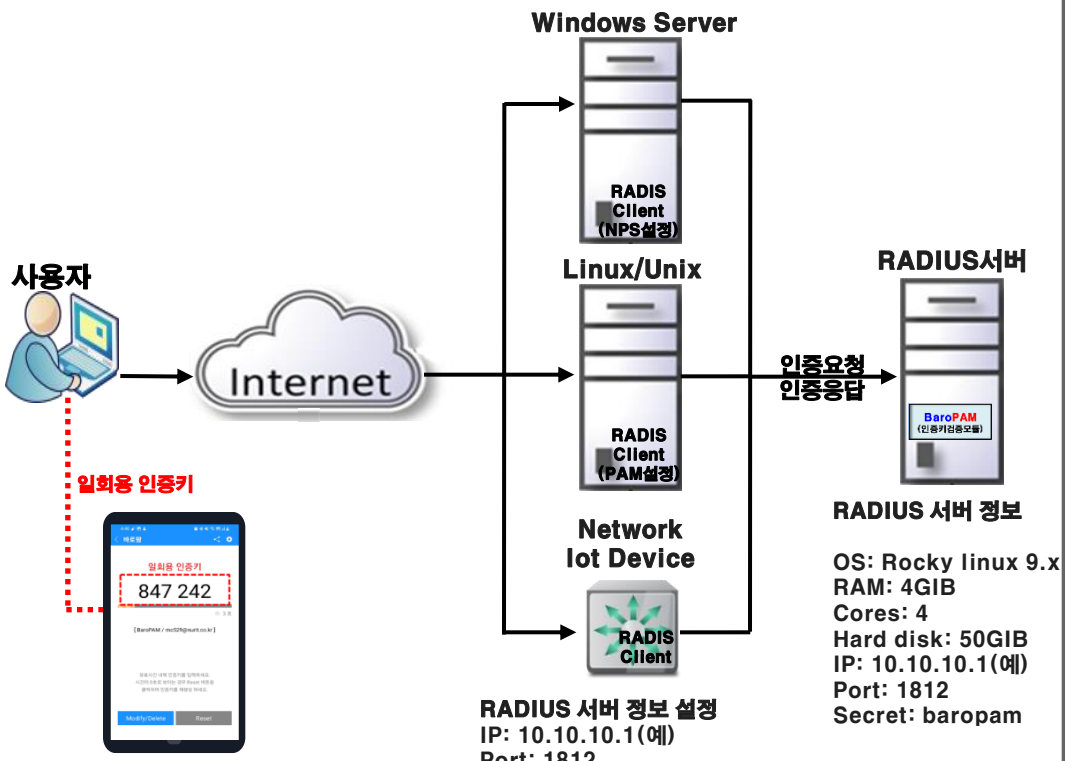
RADIUS는 응용 계층에서 작동하는 클라이언트 및 서버 프로토콜이며 사용자 데이터그램 프로토콜을 통해서 전송된다. 원격 접속 서버, 가상 사설망, 네트워크 스위치의 포트 인증, 네트워크 엑세스 서버(NAS) 이들 모두는 RADIUS서버와 통신하는 컴포넌트를 가진다. RADIUS는 종종 IEEE 802.1X 인증의 기반이 되기도 한다.

RADIUS 서버는 리눅스/유닉스 시스템이나 윈도우 서버에서 자주 백그라운드 프로세스로 실행된다.

RADIUS 인증 과정인 프로세스 흐름은 비교적 간단하지만 이해하는 것이 중요하다.

1. 어플리케이션 클라이언트는 어플리케이션 서버에 연결을 시도하고 일회용 인증키와 함께 자격 증명(로그인-ID와 비밀번호)을 제공한다.
2. 어플리케이션 서버가 이 정보를 수신하고 로컬 카탈로그에서 사용자를 찾고 인증 유형이 PAM인지 확인한다.
3. 그런 다음 외부 사용자를 인증할 위치를 결정한다.
4. RADIUS 연결 정보를 사용하여 어플리케이션 서버는 자격 증명 세부 정보를 RADIUS 서버로 전달한다.
5. RADIUS 서버는 먼저 PAM, HTTP, SQL, Active Directory, LDAP 서비스 등이 될 수 있는 PAM를 사용하여 로그인-ID / 비밀번호로 "기본 인증(Primary Authentication)"을 한다.
6. 유효성이 확인되면 RADIUS 서버는 2차 인증 서비스인 BaroPAM 모듈로 일회용 인증키로 "2차 인증(Secondary Authentication)"을 한다.
7. 유효성이 확인된 경우 RADIUS 서버는 "Access-Accept" 응답을 어플리케이션 서버로 다시 전달한 다음 연결을 수락하고 완료한다.

4. RADIUS 서버 구성(I)

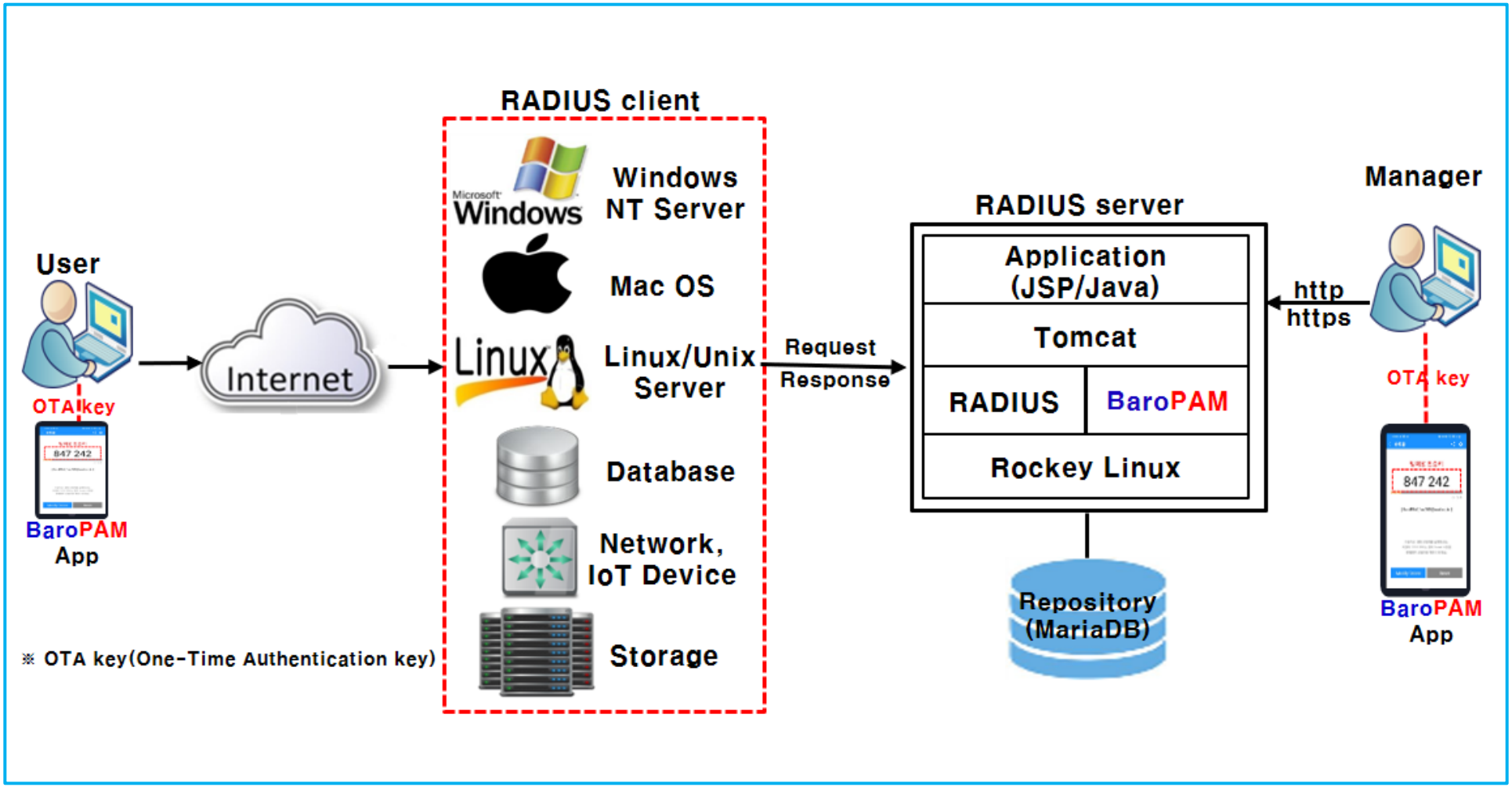


특장점

- ▶정보자산의 계정(아이디/비밀번호) 통합 관리 및 통합 인증
- ▶정보자산의 계정(아이디/비밀번호)은 OS 계정 사용
- ▶전세계적으로 인정된 512Bit 표준 Hash 함수 사용 (HMac-SHA512 / 인터넷 보안표준 IETF RFC 6238)
- ▶금융감독원에서 권장하는 시간 동기화(Time-Sync) , 동적 Secure key 방식
- ▶매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안
- ▶빠른 인증속도로 서비스 보장 (평균 인증시간 0.01초 이내)
- ▶인증절차 시 인증정보가 위변조 되더라도 우회인증 불가능
- ▶정보자산별 / 계정별 일회용 인증키 및 생성주기 개별부여
- ▶인증 우회(우회기술, 피로공격 등) 및 MFA 피로 공격 (fatigue attacks) 불가능
- ▶자동 로그인 기능을 악용한 계정 정보 탈취해도 로그인 불가능
- ▶인증의 제한 횟수 및 제한 시간(예: 30초에 3회) 설정 기능 제공
- ▶중간자(man-in-the-middle) 공격을 예방하는 기능 제공
- ▶2차 인증에서 허용 / 제외할 수 있는 계정에 대한 ACL 기능 제공
- ▶이상 접속 탐지 및 차단할 수 있는 기능 제공

4. RADIUS 서버 구성(II)

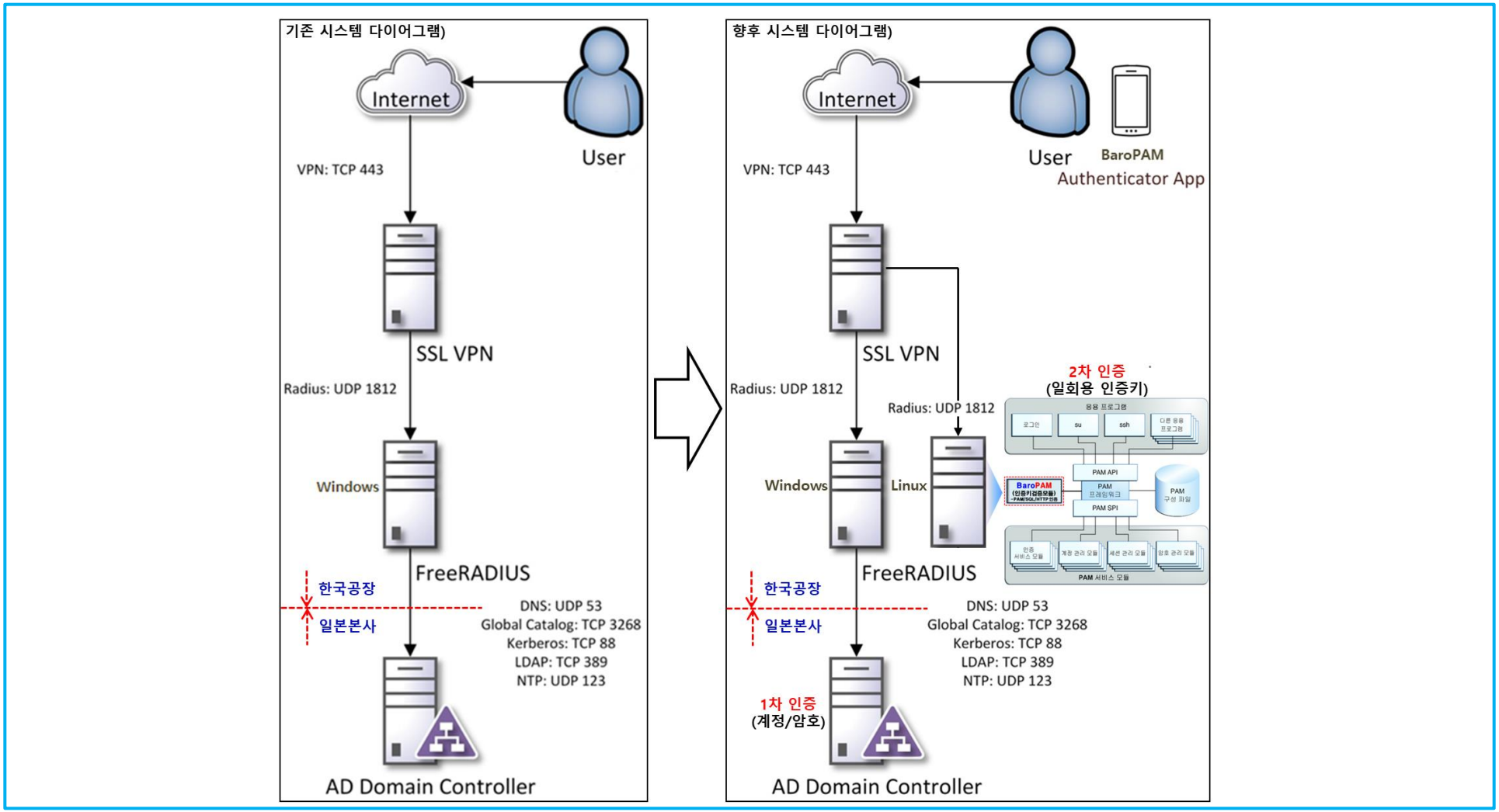
RADIUS(Remote Authentication Dial In User Service)는 네트워킹 프로토콜로 사용자가 네트워크에 연결하고 네트워크 서비스를 받기 위한 중앙 집중화된 인증으로 보안 강화를 위한 **통합 계정관리 및 통합인증**을 위하여 **BaroPAM**을 적용하여 보안을 강화 합니다.



5. RADIUS 서버 구성(적용 예)

예) 반도체 회사

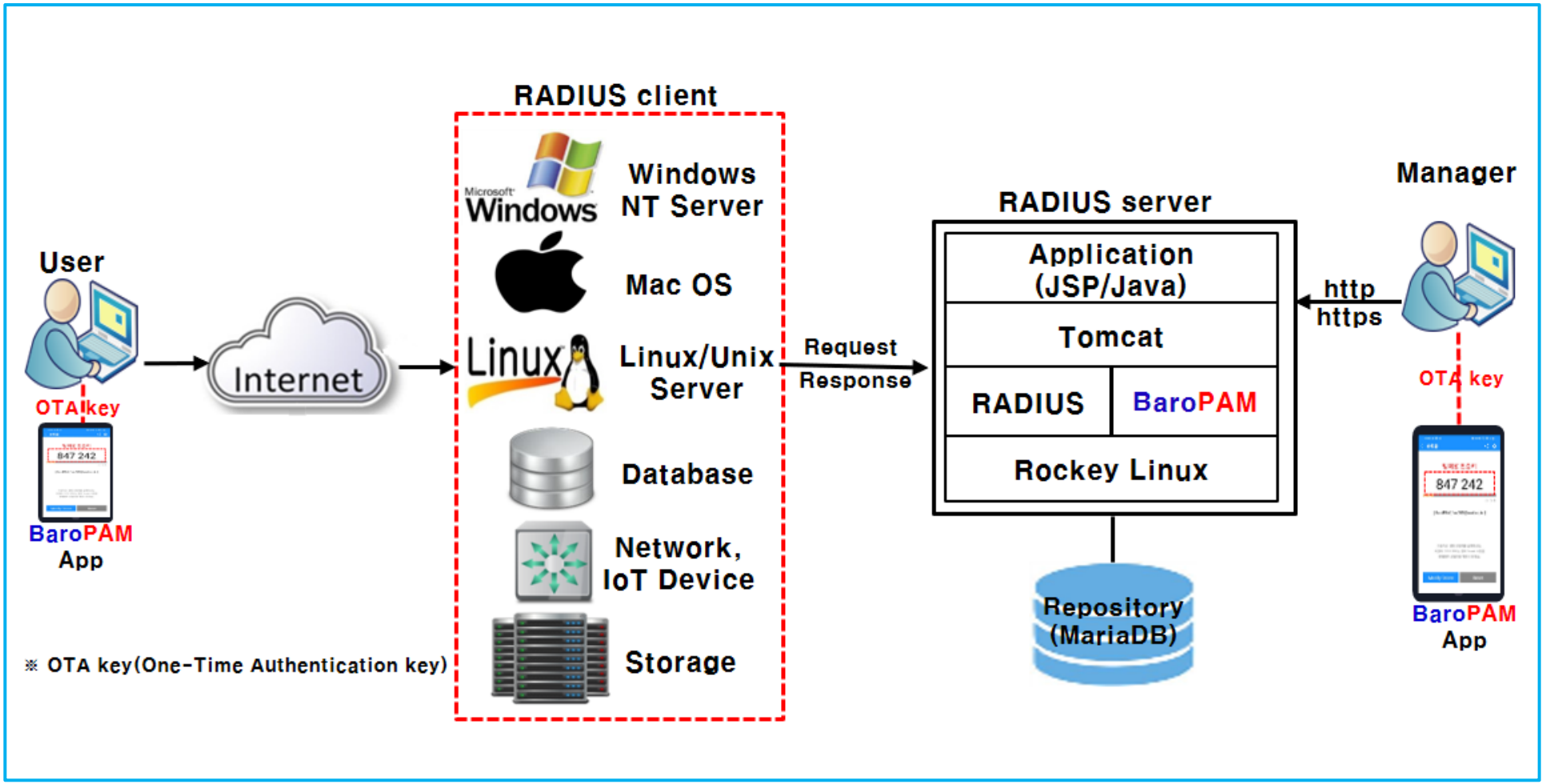
CISCO SSLVPN: 1차 인증(계정/암호)은 Active Directory, 2차 인증(일회용 인증키)는 BaroPAM으로 처리함.



5. RADIUS 서버 구성(적용 예)

예) 통신사

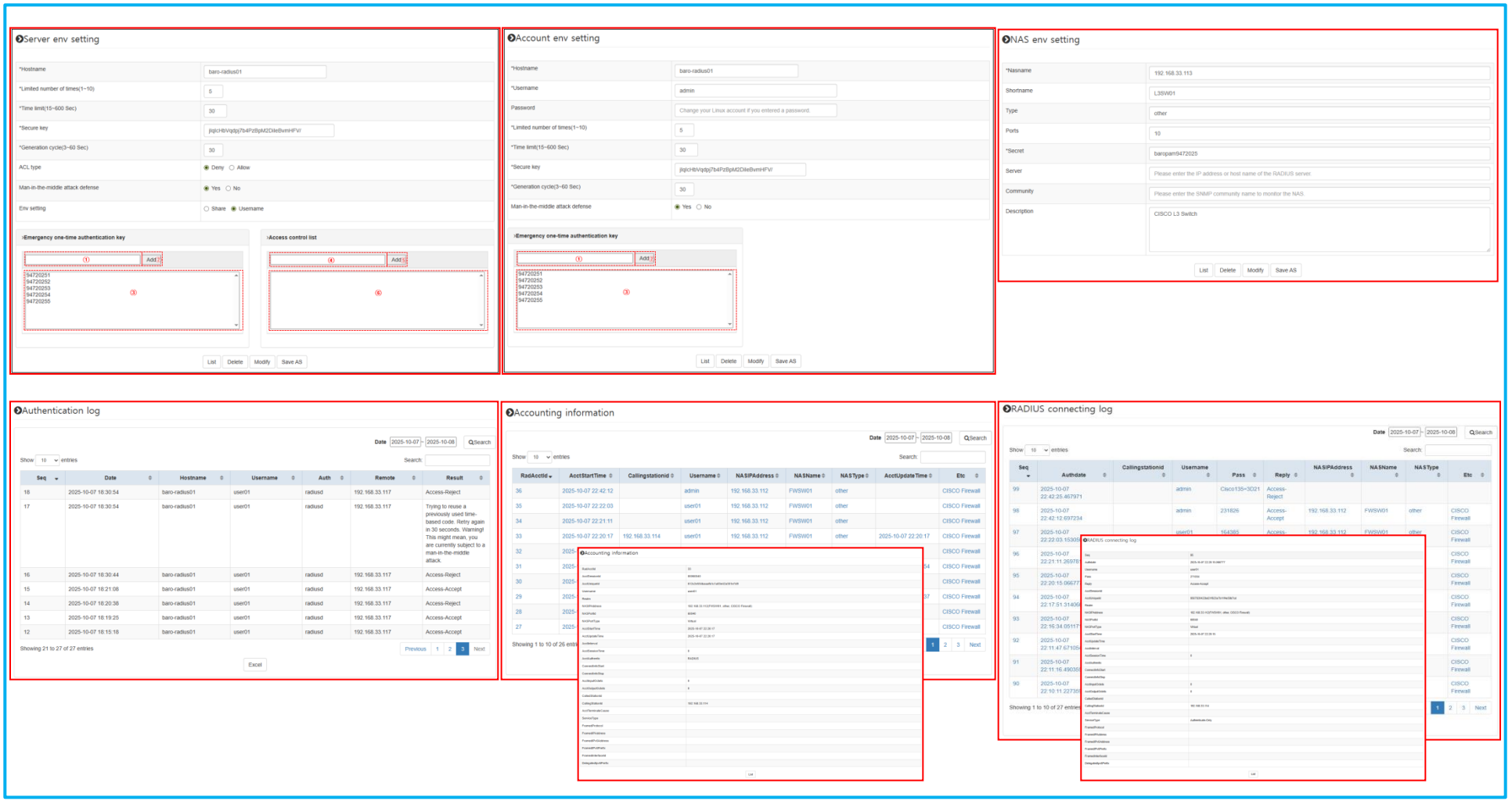
Ahnlab의 방화벽, Axgete의 SSLVPN, CISCO L2/L3의 보안 강화를 위하여 통합 계정관리 및 통합인증을으로 BaroPAM을 적용함.



5. RADIUS 서버 구성(관리 콘솔)

예) 주요 화면

관리 콘솔은 J2EE 환경에 MariaDB를 연동하여 웹 환경에서 (서버, 계정, NAS)환경 설정 및 인증 로그를 관리함.



6. 맺는 말

"망분리" 했다고 해커들을 침투를 100% 막을 수 없다는 걸 인정하고, 해커들이 이미 망 내에 들어와 있는 걸 상정하고 보안 전략을 마련해야 합니다.

아직도 보안에 취약한 이런 방식이 사용되고 있다는 현실
▶2차 인증 중 해커들의 가장 좋아하는 적용 방식: Gateway(+Proxy) 방식
▶2차 인증 중 가장 취약한 인증 방식: SMS, 이메일 등 문자기반의 인증
▶2차 인증 중 해커들이 가장 애용하는 우회 기술과 피로공격에 취약한 인증 방식: 2 채널 인증
▶피싱 공격에 잘 속는 링크 방식: QR 코드 방식

정보자산의 보안 강화를 위해서는 가장 중요한 기본 사항
▶계정정보(ID/PW)가 유출되어도 대안이 있는지?
▶보안 관점에서 위험을 얼마나 분산 시킬 것인지?
▶인증 절차 시 데이터 위변조를 어떻게 방어할 것인지?
▶계정 정보 도용 및 악용은 어떻게 차단할 것인지?
▶관리자 권한상승은 어떻게 차단할 것인지?
▶브라우저 자동 로그인은 어떻게 방어할 것인지?
▶단일 지점 공격을 어떻게 방어할 것인지?
▶우회/원격접속을 어떻게 차단할 것인지?
▶중간자 공격을 어떻게 방어할 것인지?
▶다중 인증(MFA)의 우회기술/피로공격을 어떻게 방어할 것인지?

무엇보다도 인증키는 본인이 소유하고 있는 인증키 생성매체를 사용해서 본인이 직접 인증키를 생성하여 본인이 접근하고자 하는 정보자산에 직접 입력 및 검증해야 그나마 정보보안 사고를 예방할 수 있는 최선책.

결론은 "2차 인증을 도입했다"는 것이 아니라 기술 및 보안성 등 "어떤 2차 인증을 도입했느냐"가 관건.

nurit

기억할 필요가 없는 비밀번호!
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 02-2665-0119