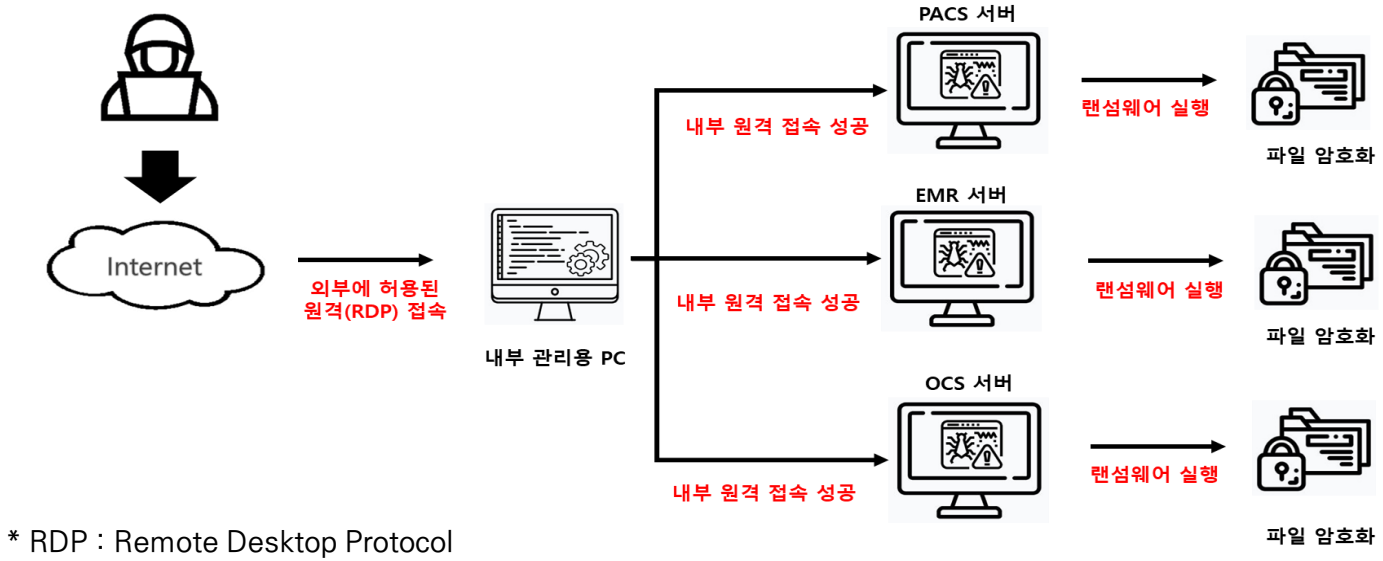
HISC 의료정보보호센터

의료기관 원격접속 보안조치 가이드

원격 접속(RDP) 서비스를 이용한 내부 정보시스템 침투

1. 원격접속 보안조치 미흡으로 인한 해킹 사고 사례

▶ 외부 오픈된 원격접속(RDP)를 통해 침투 후 내부 서버(원격허용) 추가 접속하여 랜섬웨어 감염



* RDP : Remote Desktop Protocol

운영체제, 보안장비, 시스템 등 보안조치를 통한 안전한 서비스 이용 필요

2. 원격접속 보안 조치 사항

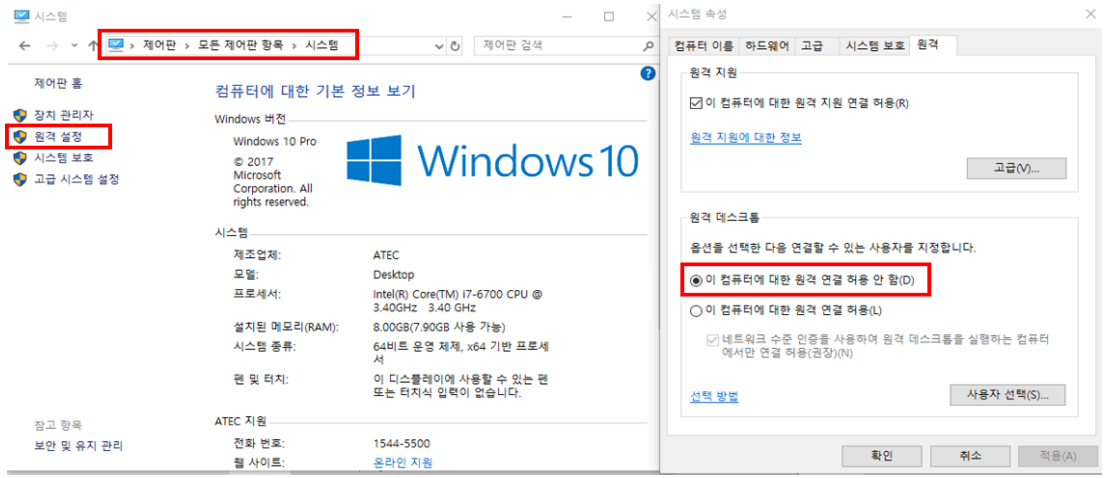
운영체제(OS)	RDP 서비스 비활성화	사용하지 않는 원격 데스크톱 프로토콜(RDP) 비활성화
	RDP 기본 포트 변경	원격 데스크톱이 필요한 시스템은 기본 포트 변경하여 사용
	Windows 방화벽 RDP 접근 설정	Windows 방화벽 설정을 통해 인가된 IP만 원격 접속 허용
보안장비	방화벽 보안정책 설정	방화벽 보안 정책 적용을 통해 인가된 IP만 원격 접속 허용
시스템	원격근무시스템 구성	원격근무시스템 구성하여 원격 근무자 보안관리 방안 마련

사용하지 않는 원격 데스크톱 프로토콜(RDP) 비활성화

2-1. (OS) RDP 서비스 비활성화

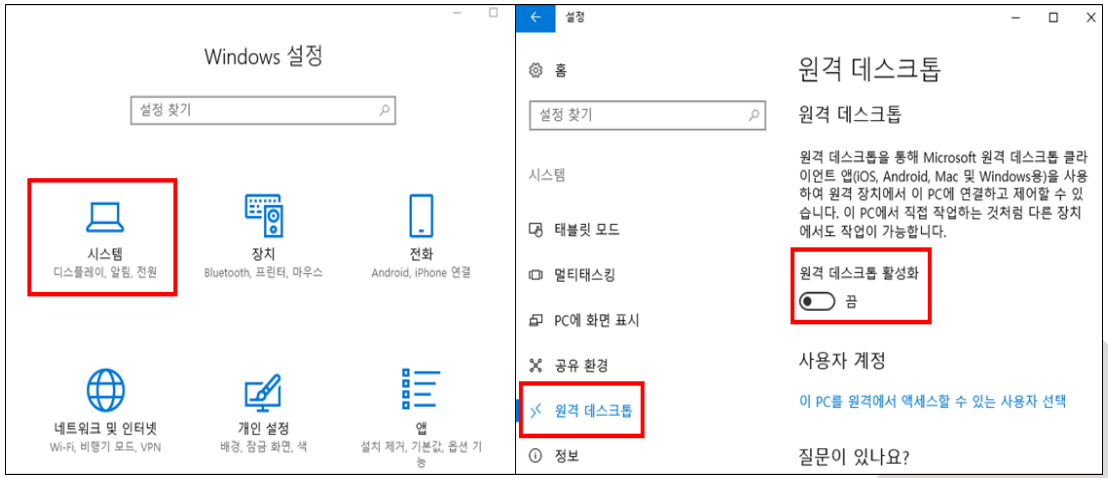
(방법1)

▶ 제어판 → 시스템 → 원격 설정 → 시스템 속성 → 원격 탭 → 원격 연결 허용 안 함 선택



(방법2)

▶ 시작 → 설정 → 시스템 → 원격 데스크톱 → 원격 데스크톱 활성화 끔

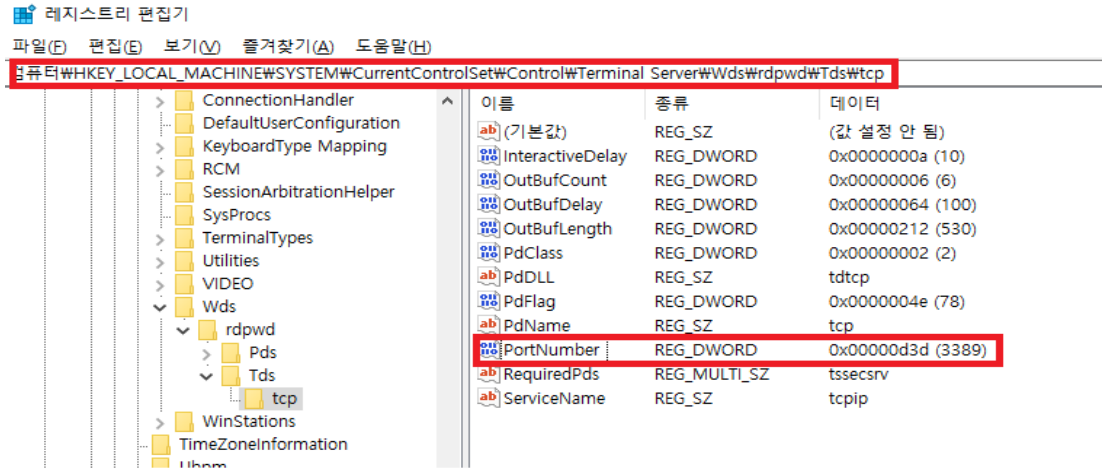


원격 데스크톱이 필요한 시스템은 기본 포트 변경하여 사용

2-2. (OS) RDP 기본 포트 변경

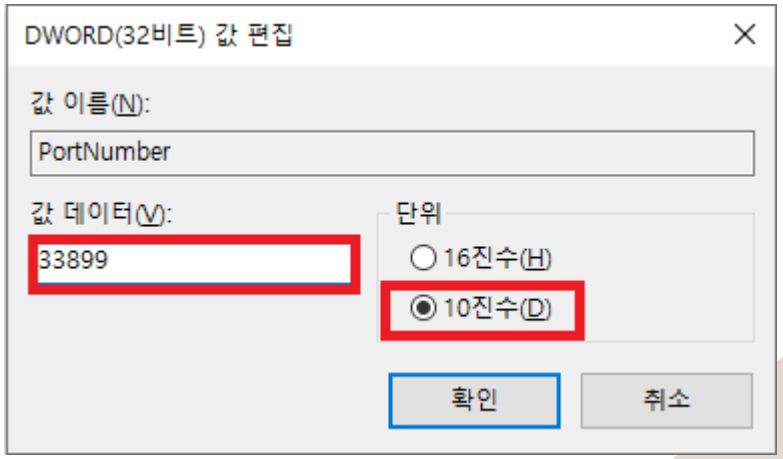
(순서1)

▶ 윈도우 키( ) ⊞R → 실행 창에서 “regedit” 입력 → “HKEY_LOCAL_MACHINE₩SYSTEM₩ CurrentControlSet₩Co17.ntrol₩TerminalServer₩Wds₩rdpwd₩Tds₩tcp” 경로 확인



(순서2)

▶ [PortNumber] 수정 → (단위) 10진수 선택 → 기본 값 “3389” 에서 임의의 숫자로 변경 후 확인



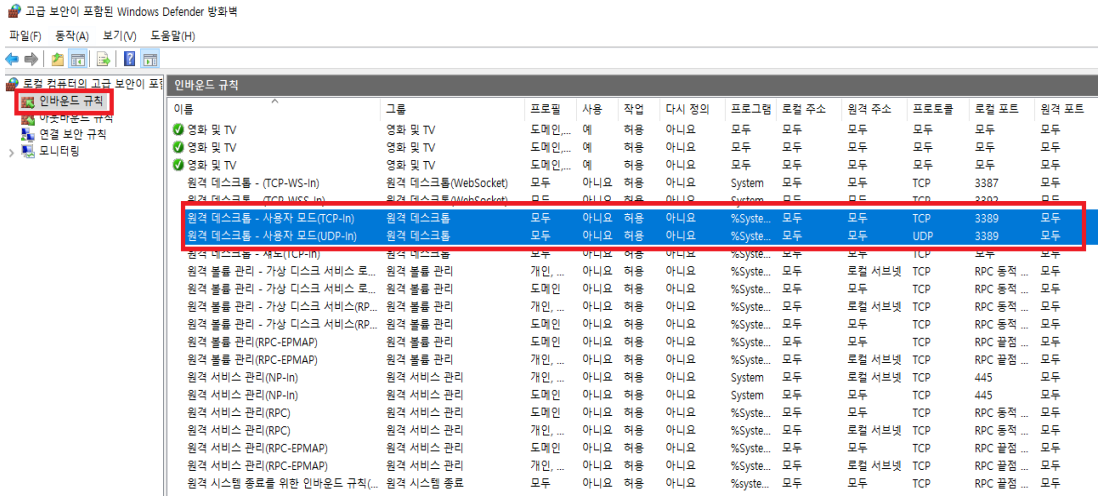
Windows 방화벽 설정을 통해 인가된 IP만 원격 접속 허용

2-3. (OS) Windows 방화벽 RDP 접근 설정

(순서1)

▶ 윈도우 키(⊞) + R → 실행 창에서 “wf.msc” 입력 →“인바운드 규칙” 내 “원격 데스크톱 – 사용자 모드” 정책 확인

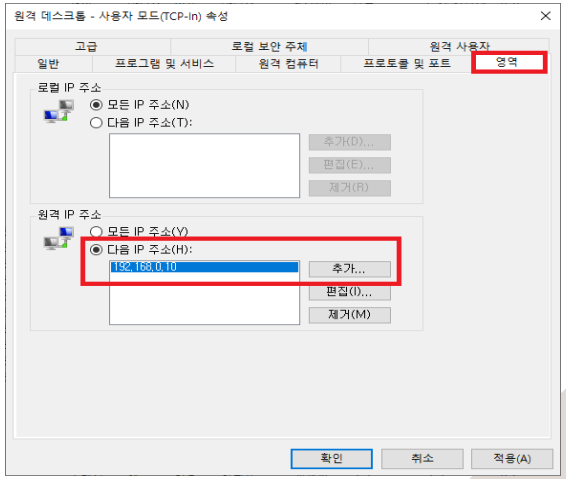
※ RDP 디폴트 포트 변경하여 사용 시 새 규칙을 통해 변경된 포트로 프로토콜 TCP, UDP 용 2개 규칙 생성 필요



(순서2)

▶ [원격 데스크톱–사용자 모드] 확인 → 영역 탭 → 원격 IP 주소 선택 → 허용된 원격접속 사용자 IP 추가 후 적용(TCP-in, UDP-in 모두 적용)

※ 원격 접속 비활성화 시스템 추가 방화벽 설정 – 일반 탭 → 작업 → “연결 차단” 선택 후 적용



방화벽(FW) 보안 정책 적용을 통해 인가된 IP만 원격 접속 허용

2-4. (보안장비) 방화벽(FW) 보안 정책 설정

(설명)

▶ 방화벽 정책은 우선순위가 존재, 'Top-Down' 방식으로 정책 리스트에서 위쪽에 있을수록 정책의 우선순위 적용

※ 방화벽 마지막 정책에는 모든 접근을 차단하는(Any → Any, Deny) 정책 적용 필요

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	홈페이지서버	TCP_80(HTTP)	Allow
외부	Any	홈페이지서버	TCP_443(HTTPS)	Allow
---	---	---	---	---
---	---	---	---	---
Any	Any	Any	Any	Deny

<방화벽 기본 정책 예시>

(원격접속 정책 적용)

▶ 외부에서 내부 시스템 원격 접속 차단 권고

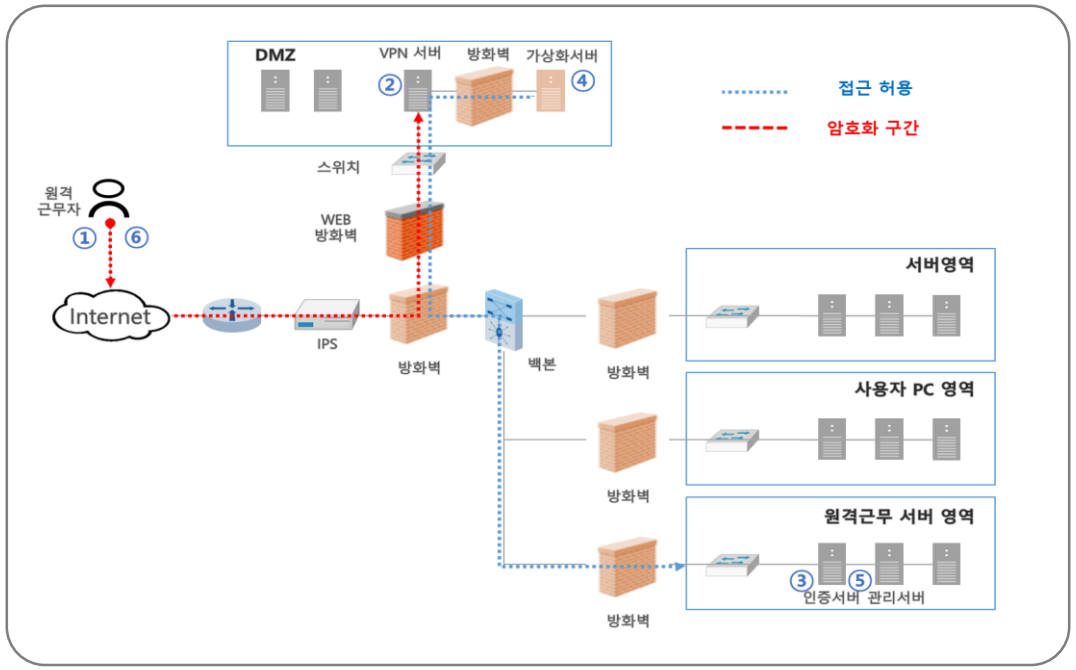
▶ 외부에서 원격 접속이 필요한 경우, "방화벽 원격접속 정책 적용 예시"와 같이 허용된 IP만 원격 접속 가능하도록 설정

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	홈페이지서버	TCP_80(HTTP)	Allow
외부	Any	홈페이지서버	TCP_443(HTTPS)	Allow
허용 IP	Any	원격 허용 시스템 IP	TCP_33899	Allow
Any	Any	Any	Any	Deny

<방화벽 원격접속 정책 적용 예시>

원격근무시스템을 구성하여 원격 근무자 보안관리 방안 마련

2-5. (시스템) 원격근무시스템 구성



〈구성도〉

구성요소	기 능
가상화 서버(VDI)	원격근무를 위한 가상데스크톱 생성
인증서버	원격 근무를 위한 접속 사용자 인증 수행
관리서버	원격근무PC 와 가상 데스크톱 매치 및 관련 보안정책 적용
원격근무 PC (VDI 단말)	가상데스크톱 접속

〈구성요소〉

2-5. (시스템) 원격근무시스템 구성

① 원격근무자는 원격근무PC에 설치된 VPN Client이용, VPN 서버에 접속

② VPN 서버에서 원격 근무를 위한 VPN 사용자 인증

③ 가상화 서버는 인가된 근무자인지 인증 요청(인증 서버)

④ 근무자는 가상화 서버에서 관리 서버 가상데스크톱 요청

⑤ 관리 서버는 인증된 근무자에게 가상데스크톱 할당

⑥ 할당 받은 가상데스크톱 이용하여 원격근무 수행

<원격근무 절차>

▶ 원격근무시스템 구축 전, 원격근무 가능 업무 범위 선별

▶ 원격 근무 보안 준수 사항이 포함된 업무 수칙 등 '원격근무 보안관리지침' 수립·운영

▶ 원격 근무자 변경 시, 시스템에 접근권한 즉시 반영 절차 마련·운영

▶ 원격 근무자 이중 인증(OTP 등)을 활용하여 적절한 접근권한 통제

▶ 업무 자료 유출 방지를 위한 자료 암호화 대책 적용

▶ 원격근무 PC 보안관리(백신, 화면 캡쳐 방지 등)

<보안대책>

랜섬웨어 대비 백업도 잊지 마세요!

랜섬웨어 피해 신고 병원 대다수가 **데이터 백업 체계가 없어** 어려움을 겪었습니다.

- [x] 정기적인 백업 주기 정하기
- [x] 네트워크 분리하여 소산 백업하기
- [x] 외장디스크, TAPE, NAS, 클라우드, 자체 백업 시스템 등 이용하기
- [x] 2차 백업 체계 확보하기

HISC 의료정보보호센터

HISC 의료정보보호센터

감사합니다.

문의사항: 의료정보보호센터 보안관제실

Tel.02-6360-6280
Fax.02-6360-6284
https://www.hisc.or.kr)