

Sikkerhet og Windows 2000

Dette er femte og siste artikkel i en serie som startet i Mellvik-Rapporten nr. 86.

Vi konstaterte avslutningsvis i forrige artikkel at RRAS, Routing and Remote Access Services, er et omfattende og komplisert stykke programvare, og at dens mangfoldige sikkerhetsmekanismer kan være et tveegget sverd: Her har vi muligheten til å etablere tett sikkerhet og god kontroll – dersom vi har den nødvendige innsikt, bakgrunn og kunnskap. I motsatt fall kan mengden, variantene og kompleksiteten bli en trussel i seg selv.

Når vi skal foreta første gangs konfigurering av RRAS, får vi for eksempel opp et bilde som gir en samling standardkonfigurasjoner å velge fra. Disse skal hjelpe oss å komme raskt i gang, og gjøre det mulig for personer uten ekspertise å sette opp et system som er godt sikret.

Ett av valgene som tilbys er VPN-tjener (*Virtual Private Network (VPN) Server*), tilsynelatende et rimelig valg i mange sammenhenger. Konfigurasjonen har imidlertid en rekke bivirkninger som gjør at den aldri bør velges, med mindre vi besitter dyptgående ekspertise på sikkerhetssystemene i Windows 2000: Den aktiviserer blant annet pakkefiltere for PPTP og L2TP protokollene, hvilket vil resultere i en rekke kinkige kommunikasjons-problemer – med mindre vi er klar over forholdet og vet hvordan filtertabellene skal manipuleres.⁵ Det sikre førstevalget blant de tilgjengelige standardkonfigurasjonene er 'manuell konfigurering', som gir eksplisitt kontroll over alle alternativer, og foreslår rimelige standardverdier.

Et lerret å bleke

Bøker kan skrives – og er blitt skrevet – om RRAS, konfigurering og sikkerhet.⁶ Grundige studier av både Microsofts egen dokumentasjon og bøker på markedet er en forutsetning for å kunne utnytte de mulighetene som er bygget inn i systemet.

Er W2k riktig verktøy?

Første punkt på programmet er knyttet mer til arkitektur enn til sikkerhet: Å avgjøre om RRAS er en komponent vi ønsker å gjøre bruk av, eller om det er optimalt å ivareta funksjonene andre steder (i annet utstyr). Windows 2000 er et generelt operativsystem, laget for et spekter av oppgaver – en kamelon som kan en del av det meste, men få oppgaver virkelig godt. Dette er optimalt for små og mellomstore organisasjoner med beskjedne og lett definerbare behov.

Som vi konstaterte i forbindelse med gjennomgangen av IPSec, er skalerbarheten for et W2k-system beskjeden. Det er for eksempel neppe hensiktsmessig å bruke en W2k-tjener til å betjene mer enn ca. et dusin samtidige VPN-brukere. Selv om antallet er høyere – og avhengig

⁵ Artikkelen Q243374 i Microsoft Knowledge Base forklarer dette forholdet.

⁶ Vi nevnte én av dem i forrige artikkel: "Windows Routing and Remote Access" av K. Charles.

av den underliggende hardware – for direktekoblede fjernbrukere via RRAS, er betraktningen den samme: Dette er løsninger for små forhold.

Dermed dukker det interessante paradoks opp, at mulighetene som finnes i W2k er optimale for beskjedne omgivelser, mens de krever ekspertise som sjelden er å finne i slike omgivelser. Det er riktignok ikke spesielt krevende å komme i gang med en fjernaksess-løsning, men å gjøre den sikker og å vedlikeholde sikkerheten, er en oppgave for eksperter.

Med den store vekt som sikkerhet har fått, går trenden klart i retning av å bruke spesialisert utstyr til fjernaksess og ruting av eksternt trafikk. Videre er det sjelden hensiktsmessig, selv for store organisasjoner, å etablere egne kontaktpunkter for fjernbrukere. Internettet er en billig og effektiv aksesskanal som gir kvalitet på nivå med egne linjer, både med hensyn til effektivitet og sikkerhet. En VPN-løsning med kryptering og autentisering av godt merke ivaretar sikkerheten, og kan i sin tur enten termineres mot et Windows 2000 system, eller i dedikerte bokser (se Mellvik-Rapporten nr. 88 side 24).

RRAS i praksis

Etter å ha gjennomført slike evalueringer, og kommet til at RRAS er den foretrukne løsning, er neste trinn å sette i gang med planleggingen: En rekke forhold er innlysende – hvem skal ha tilgang til hva og når, hvilke regler som skal gjelde og så videre, men det er ikke desto mindre viktig å sette dem på papiret, som dokumentasjon og bakgrunn for policy-valg i systemkonfigurasjonene.

Punktene nedenfor gir en kort oversikt over forhold som erfaringsmessig er kritiske for å etablere varig god sikkerhet i tilknytning til RRAS-baserte løsninger:

- ✓ Installér og ta i bruk Microsofts *High Encryption Pack*, som følger med W2k på en diskett. Sørg også for å holde systemene oppdaterte med siste *Service Pack* fra Microsoft, samt *patches* knyttet til sikkerhetsmessige svakheter.
- ✓ Fjern historie fra nettverket i den grad det er mulig. Et blandet NT/W2k-miljø er sikkerhetsmessig sterkt handikappet i forhold til et rent Windows 2000 miljø, som kan utnytte RRAS' policy-mekanismer og andre egenskaper – for eksempel filtrering av innringere basert på hvilket nummer de ringer fra.
- ✓ I et rent W2k-miljø⁷ er det viktig at alle brukere enten er blokkert fra fjernaksess (*Deny Access*) eller har definert tilgangsrettigheter via RRAS-policy (*Control Access Through Remote Access Policy*).
- ✓ Bruk RRAS-policy og profiler til å kontrollere hvilke brukere som har tilgang på hvilke tidspunkter. Opprett globale grupper

⁷ Vi snakker her om tjenermiljøet, klienten påvirkes ikke av dette kravet. Likeledes påvirkes ikke forholdet av tjenere som kjører andre operativsystemer enn Windows.

MPPE – Microsoft Point-to-Point Encryption
DES – Digital Encryption Standard
3DES – Triple-DES
RC4 – Metode for utveksling av krypto-nøkler utviklet av selskapet RSA Security.
EAP – Extensible Authentication Protocol
TLS – Transport Level Security
NAT – Network Address Translation
CHAP – Challenge Handshake Authentication Protocol

med fjernaksess via policy, og bruk profiler til å filtrere trafikken per bruker, i henhold til gruppedlemskap. Benytt den samme informasjonen til å begrense trafikken til den eller de tjenerressursene brukerne trenger aksess til når de kommer inn utenfra.

- ✓ Dersom trafikk fra fjernbrukere ikke skal rutes videre til Internettet, kan dette defineres i filtre knyttet til nettverksgrensesnitt. Slik filtrering er spesielt aktuell dersom en RRAS-tjener også fungerer som NAT-ruter mot Internettet.
- ✓ Benytt autentisering basert på MS-CHAPv2 eller EAP-TLS (se forrige artikkel, Mellvik-Rapporten nr. 89 side 22).
- ✓ *High Encryption Pack* (se ovenfor) er inkludert fordi den er nødvendig for god sikring, og bør brukes. Det betyr 128-bits RC4-kryptering i MPPE og 168-bits 3DES-kryptering i IPSec (se Mellvik-Rapporten nr. 88 side 20/21).
- ✓ Aktiviser logging av mest mulig informasjon (men ikke hver enkelt PPP-pakke som utveksles). Dette forutsetter at maksimalstørrelse for systemets loggfiler økes, og at rutiner for hyppig tømning og sikkerhetskopiering av loggene etableres.
- ✓ Aktiviser automatisk stenging av RRAS-konti (*lockout*). En rimelig grense for stenging er 5 mislykkede innlogginger i løpet av en time. Dette gir god balanse mellom hva som er administrativt mulig og effektiv reduksjon av muligheter for passord-angrep.
- ✓ Når flere tjenere settes opp til å betjene en større mengde samtidige brukere, er det en god idé for såvel sikkerhet som administrasjon å sentralisere autentisering og logging til en RADIUS-tjener, for eksempel IAS (Microsofts Internet Authentication Server, en RADIUS-implementasjon som er en del av RRAS-pakken).

VPN og W2k

Tidligere i denne serien (Mellvik-Rapporten nr. 87 og 88) gjennomgikk vi IPSec-implementasjonen i Windows 2000, og konstaterte blant annet at dette er et respektabelt stykke programvare med stor nytteverdi i flere sammenhenger. Den mest nærliggende for de fleste er VPN, Virtuelle Private Nettverk: Koblingen mellom VPN og IPSec er så tett at mange tror IPSec er en VPN-implementasjon. Dette er imidlertid feil, som vi også konstaterte under gjennomgangen av IPSec. Her ligger også årsaken til at de fleste andre sidene av IPSec ikke er kjent, og gjerne kommer som en overraskelse, selv for erfarne driftspersoner.

Vi diskuterte VPN-teknologi og anvendelser i en egen artikkelserie i Mellvik-Rapporten nr. 58-62. Gjennomgangen nedenfor tar utgangspunkt i at grunnleggende prinsipper og mekanismer er kjent, og belyser bruksmessige forhold som er spesielt relevante i forhold til Windows 2000.

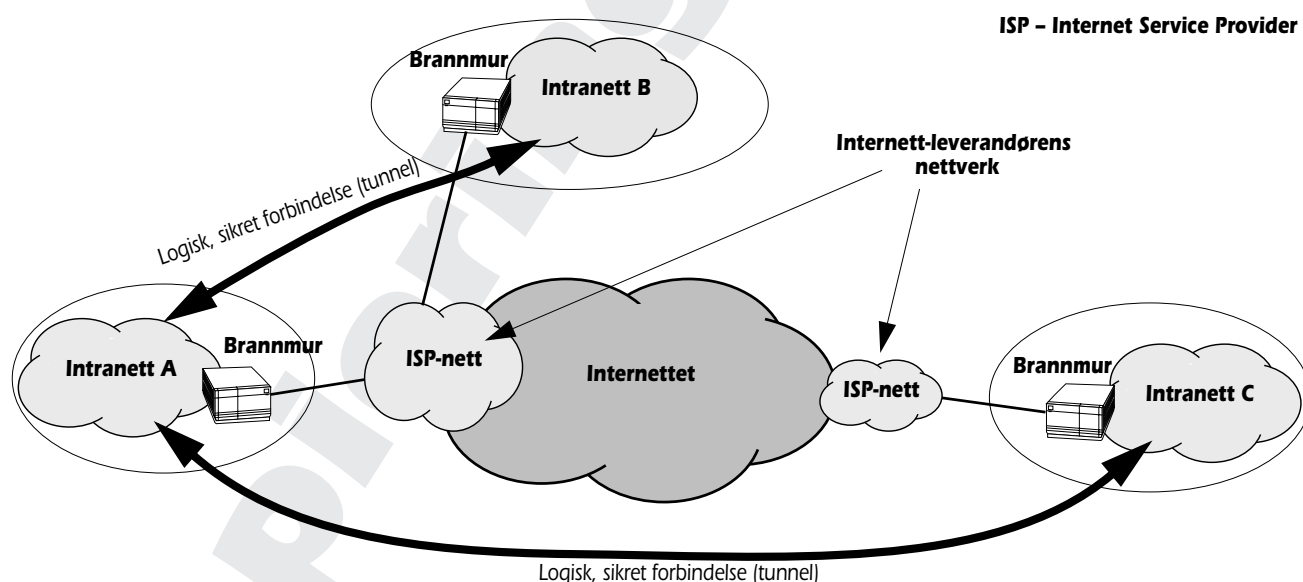
Tunnel, innhold og sikring

Det er en utbredt misforståelse at VPN automatisk impliserer god sikring: Begrepet er misbrukt lenge nok til at det for svært mange har skiftet betydning: Opprinnelig betyr uttrykket et 'logisk nettverk over-

lagt et fysisk nettverk', et abstraksjonsnivå der standardiserte mekanismer utnytter en underliggende fysisk infrastruktur til å implementere logiske nettverk eller punkt-til-punkt forbindelser (se figur 3). Det ligger ingen implisitt sikkerhet her – trafikken i et VPN trenger ikke å være sikret. At den ofte er det, og at VPN er grunnlaget for effektiv transportsikring i moderne nettverk, er årsaken til begrepsforvirringen: Sammen med VPN etableres i de fleste tilfeller også krypterings- og autentiseringsmekanismer som sørger for god sikkerhet – for eksempel IPSec.

Forbindelsesvarianter

VPN-forbindelser etableres vanligvis på én av to måter: Mellom to rutere, som typisk befinner seg i hvert sitt lokalnett, og sørger for en sikret forbindelse dem imellom, eller mellom en maskin og en ruter. I sistnevnte tilfelle etableres den sikrede forbindelse mellom den involverte maskinen og nettverket bak ruterens. Denne varianten er typisk for eksterne brukere – på reise, fra hjemmekontor eller kanskje på oppdrag ute hos klienter. Etter at brukeren har identifisert seg (autentisering) overfor VPN-tjeneren – via smartkort, passord eller på andre måter, opprettes en logisk punkt-til-punkt forbindelse, og trafikken krypteres i henhold til retningslinjer definert på tjenersiden og egenskaper hos klienten. Det er ingen ting i veien for at en klient kan ha flere slike forbindelser aktive på samme tid. Videre kan forbindelsene være permanente i den forstand at de holdes i live hele tiden, eller de kan kobles opp og ned etter behov.



Figur 3 – I Virtuelle Private Nett legges logiske forbindelser over en fysisk infrastruktur og gis de egenskaper behovene tilsier – innenfor rammene det underliggende nettverket tillater. Figuren er hentet fra Mellvik-Rapporten nr. 52.

Forbindelsene er usynlige for applikasjoner og tjenester som bruker nettverket – en viktig kvalifikasjon: Klienten kan opptre som en lokal maskin overfor tjenere og tjenester på det interne nettverket – med de restriksjoner som er lagt inn i ruterens som formidler trafikken.

L2TP – Layer 2 Tunneling Protocol
PPTP – Point-to-Point Tunneling Protocol

I Windows 2000 er L2TP den foretrukne mekanisme for etablering av VPN-forbindelser, mens sikring og autentisering fortrinnsvis ivaretas av IPSec. Kombinasjonen gir høy effektivitet og god sikkerhet, men begrenset kompatibilitet: Utover W2k og Windows XP er det få klienter som støtter L2TP. Alternativet er PPTP, som er mer utbredt og standardisert, men ikke like sikker. Dessuten: Slik implementasjonen er i W2k, kan IPSec ikke brukes sammen med PPTP, og vi er henvist til å bruke Microsofts egen krypteringsmekanisme i stedet, MPPE. Denne gir isolert sett god sikkerhet, men langt fra like god og fleksibel som IPSec. IPSec er på sin side inkompatibel med NAT, og kan ikke brukes gjennom rutere som oversetter adresser.

Valgets kvaler

Det finnes med andre ord ikke noe universelt valg for enhver situasjon: Begge varianter har fordeler og ulemper, og hvilket valg som er riktig eller mulig, kommer an på omstendighetene.

L2TP/IPSec gir best sikkerhet der den kan brukes, og det vil i en del tilfeller være mulig å tilpasse arkitekturen slik at NAT-relaterte problemer kan unngås – for eksempel gjennom å plassere endepunktet og NAT-funksjonen i samme boks. Samtidig er det ingen grunn til å frykte PPTP/MPPE – med mindre kravene er spesielt strenge. Sist, men ikke minst finnes det andre kombinasjoner som implementeres via en blanding av innebygget programvare og tredjeparts produkter.

Like viktig som å sørge for sikkerheten i en VPN-løsning, er det å sørge for at usikret trafikk ikke slipper inn i tunellen. En hjemmebruker med en infisert maskin er like smittefarlig uansett hvor god eller dårlig VPN-løsningen er. Derfor er personlige brannmurer ikke bare 'kjekt å ha',⁸ men et krav for eksterne brukere. Det finnes utallige eksempler på 'hackede' hjemme-PCer som i lang tid har fungert som åpne rutere mellom Internettet og interne nettverk – via VPN. Slikt skal ikke forekomme, men gjør det like fullt, og demonstrerer hvor viktig det er med forsvar på flere nivåer.

Oppsummering

God sikkerhet er et resultat av helheten, ikke enkelttiltakene. At Windows 2000 har gode mekanismer for sikring, gir ikke bedre sikkerhet på egen hånd, men yter et viktig bidrag i positiv retning der forgjengerne har gjort det motsatte.

Windows 2000 er et komplekst system, med utallige muligheter – ikke minst for feilkonfigurasjoner og hull. Å holde oversikten i denne jungelen er praktisk talt umulig. Vi trenger verktøy som kan foreta jevnlig kontroll – mer eller mindre automatisk. Dette er utgangspunktet for en artikkel som i løpet av første kvartal 2002 følger opp denne serien.

■

⁸ Se Mellvik-Rapporten nr. 75.