

# Sikkerhet og Windows 2000

Dette er andre artikkel i en serie som startet i Mellvik-Rapporten nr. 86.

*I forrige utgave introduserte vi Windows 2000 fra en sikkerhetsmessig synsvinkel, og konstaterte blant annet at Microsoft virkelig har lagt seg i selen for å rette opp viktige problemområder som hemmet Windows NT. Nykommeren, som allerede har over et års fartstid bak seg, har fått en lang rekke sikkerhetsrelaterte tjenester og forbedringer, hvorav de fleste er nyttige i en eller annen sammenheng.*

Videre påpekte vi at avstanden kan være lang fra arkitektur til byggverk, og at gode ideer og ambisjoner slett ikke betyr at implementasjonene blir av tilsvarende kvalitet. Fra tid til annen forekommer det sågar at implementasjoner av gode ideer ikke er praktisk anvendbare i det hele tatt. De fleste store programvareleverandører – inklusive Microsoft – har et betydelig synderegister i så henseende.

## Integrasjonens svøpe

Det faktum at vi hører om og opplever en nærmest kontinuerlig strøm av hull og svakheter i Windows 2000, er med andre ord ikke det samme som at arkitekturen er dårlig eller at sikkerhetsmekanismene mangler. Det som avsløres er i de fleste tilfeller svakheter i implementasjon – i operativsystemet, i applikasjoner eller i enkelttjenester. I særdeleshet har Web-tjeneren IIS (*Internet Information Service*) og nettleseren IE (*Internet Explorer*) vært gjengangere i så henseende.

I og med at Microsoft har valgt å integrere tjenestene tett i operativsystemet, og derigjennom fjernet det tradisjonelle skillet mellom operativsystem, brukerprogrammer og tjenester, er det vanskelig å skille det ene fra det andre – både for oss som er brukere eller administratorer, og for utviklerne. Dermed blir feilene tilskrevet Windows 2000 som produkt uansett hvor de måtte være. Dette kan kalles integrasjonens svøpe, og har en annen og vel så alvorlig side: Den tette integrasjonen fører til at det blir vanskelig å etablere barrierer mellom operativsystem og tjenester. Et innbrudd i en tjeneste har dermed lett for å gi inntrengerer kontroll over hele systemet.

Disse og mange andre konsekvenser av Microsofts integrasjonsfilosofi, skaper voksende utfordringer for såvel videreutviklingen av systemene som for brukermiljøene. For eksempel var Microsofts egen meldingstjeneste på MSN (*Microsoft Network*), ute av funksjon i dagevis i juli i år, av årsaker selskapet naturlig nok ikke har frigitt detaljer om. Driftsavbruddets varighet gir imidlertid grunnlag for å tro at problemene hadde systemteknisk opprinnelse. Stadig oftere dukker det opp feil og vanskeligheter som ikke lar seg spore, fordi systemene er blitt for komplekse, integrerte og uoversiktlige. Veien ut av uføret går gjennom forenkling, som igjen ikke kan bety noe annet enn å separere tjenestene fra operativsystemet. Frem og tilbake er like langt.

## Praktisk sikkerhet: IPSec

### IPSec fra Cisco

IPSec-implementasjonen i Windows 2000 er laget av Cisco Systems, og får gode karakterer av amerikanske sikkerhets-eksperter. Den er solid, pålitelig og effektiv, og støttes av verktøy som er det samme. Verdt å merke er det at kommentarene gjelder de medfølgende kommandolinje-verktøy, også utviklet av Cisco. De Windows-baserte verktøyene er Microsofts egne, og er langt enklere i bruk, og gir mindre direkte kontroll med funksjonene. Samtidig er de mindre pålitelige og beheftet med en rekke sideeffekter som langt fra alltid er opplagte.

**DES** – Digital Encryption Standard  
**CBC** – Cipher Block Chaining  
**PFS** – Perfect Forward Security  
**MD5** – Message Digest 5, standard-algoritme for generering av kontrolltall som representerer 'signaturen' til en gitt datamengde.  
**SHA-1** – Secure Hash Algorithm 1

### IPSec standarder:

**RFC 2401** – Security Architecture for the Internet Protocol  
**RFC 2402** – IP Authentication Header (AH)  
**RFC 2406** – IP Encapsulating Security Payload (ESP)  
**RFC 2409** – The Internet Key Exchange (IKE)

Verken integrasjonen eller problemer innen sikkerhet og på andre områder, har imidlertid forhindret W2000 eller andre Microsoft-produkter fra å bli gigantiske suksesser i markedet. Mangt kan være kritikkverdig fra faglige og tekniske synsvinkler, men i det daglige er det pragmatismen som gjelder, og som foreskriver at vi benytter de verktøy som finnes – der de av én eller flere årsaker passer best. Svakheter og problemer som følger med på kjøpet, må i den samme pragmatismens ånd håndteres, elimineres eller reduseres.

### IPSec – en sikker vinner

Et av de nyttigste og mest velutviklede tilleggene i W2000 er støtten for IPSec – en etterhvert veletablert standard for sikring av trafikk i IP-baserte nettverk. Vi har introdusert IPSec-standarden tidligere her i Mellvik-Rapporten,<sup>4</sup> og kan konstatere at den har svart til forventningene: Oppslutningen fra leverandører og marked har vært øredøvende, og utbredelsen er blitt deretter.

Standardiseringen har ført til at VPN som teknologi og løsning har flyttet seg fra 'lovene' til 'etablert' på rekordtid, med viktige positive konsekvenser for sikkerheten. Ikke desto mindre befinner vi oss fortsatt i startgropen for en total sikring av datakommunikasjon, og Microsofts innebygde støtte for IPSec i W2000 og etterfølgere er viktig for den videre progresjonen – alminneliggjøringen.

Hvorvidt IPSec spesielt og VPN generelt hører hjemme i et system (som W2000) eller i en boks i nettverket (ruter, brannmur eller lignende), er en annen diskusjon – som vi i noen grad skal komme inn på nedenfor. Faktum er i alle fall at Microsofts IPSec-implementasjon har fått god mottagelse i markedet også fra eksperter. Den er laget av Cisco Systems, som burde ha de beste forutsetninger for oppgaven. Kompatibiliteten med standarden er god, slik at samspillet med andre implementasjoner og produkter går greit, om ikke problemfritt.

Fordelene knyttet til IPSec og dermed til å benytte Windows' IPSec-implementasjon til å heve den generelle nettverkssikkerheten, er tallrike. Her er noen av dem:

- ✓ **Autentisering:** IPSec kan kontrollere identiteten til avsenderen av datapakker (ikke person, men en maskin eller en ruter). Brukt sammen med X.509-sertifikater, som også støttes av W2k, blir denne autentiseringen 'sterk', dvs. meget pålitelig.
- ✓ **Kryptering:** Enten innholdet i pakken eller hele pakken (tunnel) kan krypteres. For eksperter: W2k støtter 168-bit DES-kryptering i såkalt CBC-modus med PFS (også kjent som 3DES). I tillegg støttes den tradisjonelle 56 bits DES-standard, som representerer minimal belastning i forhold til 3DES, mens den fortsatt gir rimelig god sikkerhet.<sup>5</sup>

<sup>4</sup> Artikkelen "IPSec: Sikkerhet på overtid for TCP/IP" i Mellvik-Rapporten nr. 66 (oktober 1999) gir en innføring i bakgrunn og teknologi for IPSec-standarden.

**IPSec i nettverkskortet**

IPSec befinner seg på nettverksnivå, og kan dermed flyttes ut til nettverkskortet (NIC) uten komplikasjoner for vertsmaskin eller operativsystem. Med slik dedikert hardware øker effektiviteten samtidig med at belastningen på vertsmaskinen reduseres kraftig. Våre tester viser at overføring av en 80 MB binær fil via 10 Mbps Ethernet konsumerer 62% CPU uten slik hardware, og 6% med (W2000 Advanced Server). Tallene vil variere fra én maskin til en annen, men demonstrerer klart nytteeffekten av en slik akselerator. **Konklusjonen blir at nettverkskort uten IPSec-støtte ikke lenger burde finnes på våre innkjøps-lister.**

Eksempler på kort som har slik støtte er 3Coms EtherLink 3XP og Intels PRO/100S.

**L2TP** – Layer 2 Tunneling Protocol  
**IETF** – Internet Engineering Task Force

**Kompatibilitet**

I og med at IPSec er en etablert IETF-standard, og ikke minst takket være opprinnelsen til den implementasjonen W2k leverer, er kompatibiliteten med andre produkter relativt god. Følgende produkter og teknologier er verifisert compatible, og den virkelige listen er betydelig lenger:

- PGP Desktop Security 7.0.3 ([www.pgp.com](http://www.pgp.com))
- De fleste Cisco-produkter
- FreeS/WAN IPSec client for Linux ([www.freeswan.org](http://www.freeswan.org))
- OpenBSD isakmpd ([www.openbsd.org](http://www.openbsd.org))

**IPSec og IPv6**

IPSec er utviklet med tanke på neste IP-generasjon, IPv6, og implementasjonen i Windows 2000 er klargjort for å håndtere nykommeren. Detaljer er å finne på referansesiden til denne utgaven av Mellvik-Rapporten, se side 35.

✓ **Integritet:** IPSec kan integritetskontrollere datapakkene som forsikring mot at de er blitt skadet eller forandret underveis. I henhold til standarden støttes MD5- og SHA-1-algoritmene for integritetskontroll.

✓ **Pakke-filtrering:** IPSec er mest kjent for VPN, autentisering og kryptering, men kan også benyttes til statisk pakkefiltrering. Egenskapen har så langt fått liten oppmerksomhet og er tilsvarende lite benyttet. Den er imidlertid både nyttig og viktig, og burde markedsføres bedre av Microsoft. For eksempel kan den benyttes som personlig brannmur – på bærbare og stasjonære maskiner, tjenere og klienter. Behovet er akutt, et forhold vi har diskutert ved flere anledninger tidligere.<sup>6</sup>

✓ **Usynlig for applikasjoner og tjenester:** IPSec er implementert på nettverksnivå, og er derfor usynlig for applikasjoner og tjenester – og brukere. Det betyr at nytteverdien er umiddelbar, ingen programmer – nye eller gamle – må forandres eller oppdateres for å benytte sikringsmekanismene. Videre fordres det ingen opplæring eller bevissthet fra brukernes side. Denne usynligheten er en grunnleggende kvalifikasjon: Sikkerhet generelt og IPSec spesielt er altfor komplisert til å håndteres av brukere.

✓ **Automatisk styring:** Regler og filtre som skal implementeres av IPSec, kan defineres sentralt og distribueres automatisk til maskiner og rutere. W2k benytter en såkalt Group Policy mekanisme for å både automatisere og homogenisere sikkerhetsmekanismene for brukergrupper og deres utstyr.

✓ **Intelligent hardware:** Hardware-støtte for IPSec blir i disse dager bygget inn i stadig flere nettverkskort, og blir dermed i voksende grad en implisitt del av nettverkskommunikasjonen. Dessuten avlastes maskinene kraftig ved bruk av slik hardware (se margrammen).

✓ **VPN-støtte:** Den mest kjente og dermed oftest benyttede egenskapen i IPSec. VPN betyr å etablere logiske punkt-til-punkt kanaler i nettverket (ofte kalt tunneller). Slike kanaler impliserer ingen sikkerhet i seg selv. Det er kryptering av trafikken i tunnelen som gir sikkerhet – ved siden av autentisering av endepunktene og integritetskontroll av datastrømmen. IPSec har alle fasiliteter som trengs for å etablere pålitelige og sikre tunneller i et hvilket som helst IP-nettverk (se også kommentar under ulemper nedenfor). Selve tunnelen etableres fortrinnsvis av underliggende transportprotokoller, i W2k typisk L2TP.

✓ **Beskyttelse mot 'replay-attack':** IPSec inneholder mekanismer som eliminerer muligheten for slike angrep, som

5 56-bits kryptering er ikke vanskelig å knekke for eksperter og andre med skikkelige verktøy, men representerer like fullt vesentlig sikring i forhold til ingenting: Det skal betydelig interesse til for å gi seg i kast med dekrypteringsjobben.

6 Se "Gratis sikkerhet" i Mellvik-Rapporten nr. 86 og "Skal det være en personlig brannmur" i nr. 75.

fremkommer når datapakker blir kopiert av en angriper mens de er underveis, modifisert og deretter sendt på nytt.

At IPSec kan gi god sikkerhet og at implementasjonen i W2k er god, betyr ikke at den er blottet for ulemper og svakheter. Enkelte av disse er det spesielt viktig å være oppmerksom på:

- ✓ **Ytelse og effektivitet:** Kombinasjonen W2k/IPSec/VPN vil ikke ha den samme effektive hastigheten som en hardware-løsning, der en egen boks tar seg av hele oppgaven. Dette gjelder selv om grensesnitt med akseleratorer benyttes. Løsningen egner seg for klientmaskiner og for miljøer med et beskjedent antall brukere der W2k allerede er i bruk på tjenersiden. Ved mange samtidige brukere er en egen hardware-løsning å anbefale.
- ✓ **Svake tunneller:** IPSec-implementasjonen i W2k dekker akkurat nok av protokollens tunnel-modus til å være innenfor standarden, men ingen av utvidelsene som mange andre leverandører har tatt med. Dette er en bevisst utelatelse fra Microsofts side som det kan føres sikkerhetsmessige argumenter for, men som ikke desto mindre kompliserer etableringen av VPN-forbindelser mot utstyr fra andre leverandører. L2TP er den foretrukne tunnel-protokoll.
- ✓ **INTRUSION DETECTION:** Det er viktig å være klar over at bruk av IPSec generelt eliminerer muligheten til å benytte nettverksbasert innbruddsdeteksjon (produkter som kontinuerlig skanner nettverket for å finne uregelmessigheter). Dette har ingen ting med W2k å gjøre, men er en konsekvens av kombinasjonen tunnel og kryptering (VPN).

## IPSec i bruk

I forrige avsnitt 'markedsførte' vi IPSec som et allsidig og effektivt sikkerhetsverktøy. Her skal vi ta frem en samling praktiske anvendelser som på den ene siden er teknisk overkommelige å få i drift, og på den andre siden kan bidra betydelig til bedre sikkerhet.

Forenklet bilde av bestanddelene i IPSec:

<b>Kryptering</b>
<b>Autentisering</b>
<b>Filtrering</b>

- ✓ **Pakkefiltrering** (enkel brannmur-funksjonalitet): Som vi allerede har nevnt, kalles denne egenskapen ofte 'den glemte'. IPSec inneholder et ideelt pakkefilter som kan bidra vesentlig til å heve sikkerhetsnivået. Filtrering kan også gjøres på et høyere nivå, i en funksjonsmodul som kalles RRAS, *Routing and Remote Access Services*, men er både enklere å administrere og mindre ressurskrevende i IPSec.
- ✓ **Web-applikasjoner:** Mange Web-tjenester betjenes av en samling *front end* tjenere som støttes av databasetjenere i intranettet. Sikring av trafikken mellom disse er ekstremt viktig. Her kan IPSec yte et viktig bidrag gjennom autentisering av tjenerne på begge sider av brannmuren, integrasjonskontroll av trafikken og filtrering av all annen trafikk. Kryptering er normalt overflødig i et slikt scenario, men er tilgjengelig for miljøer med spesielle behov.

- ✓ **Viktige interne tjenere:** Dybdesikkerhet betyr å sørge for flere lag (skanser) innover i nettverket. I mange, kanskje de fleste, nettverk representerer brannmuren den eneste forsvarslinjen. Når en inntrenger har forsert brannmuren, er alt annet åpent. En slik blind tillit til én enkelt boks eller produktgruppe skaper unødig avhengighet av ett eneste ledd – *single point of failure*. IPSec kan bidra til å heve nivået gjennom ekstra sikring av kritiske tjenere og arbeidsstasjoner. For eksempel: Domene-kontrollere kan replisere sine data via IPSec, databaser kan synkronisere følsomme data via IPSec, de sikkerhets-ansvarliges arbeidsstasjoner behandler nærmest kontinuerlig følsomme data, og bør sikres spesielt – og så videre.
- ✓ **Intern sikring:** Det er et kjent faktum at 70% eller mer av all datasnoking og andre sikkerhetsbrudd har sin opprinnelse internt. Et bedre argument for å sikre følsom intern trafikk kan vanskelig finnes, og IPSec legger forholdene godt til rette. Slik sikring kan implementeres mellom utvalgte maskiner, eller ved å forbinde avdelinger eller grupper via IPSec-rutere eller VPN-tuneller.
- ✓ **Partner-nett (ekstranett):** Sikring av kommunikasjon med partnere – for epost, ehandel, innsyn i avtaler, ordrestatus etc., er hyperaktuelt. Windows 2000 IPSec legger forholdene godt til rette for slik sikring, også om partneren ikke benytter samme plattform. Tjener-til-ruter-forbindelser, autentisering (med digitale sertifikater) og kryptering er ikke begrenset til W2k-miljøer.
- ✓ **Brukere på farten:** Eksterne brukere som trenger sikker tilgang til det interne nettverket, kan benytte IPSec sammen med L2TP for å etablere autentiserte og krypterte VPN-tuneller fra klient til en intern ruter. Med en slik tunnel blir klienten logisk en del av det interne nettverket.<sup>7</sup>
- ✓ **Fjernstyring:** Ikke minst for system- og sikkerhetsansvarlige er muligheten for å benytte VPN-mekanismene fra hjemmekontor eller på reise essensielle. Den type oppgaver som gjøres – og informasjonen som formidles – er sjelden av en kategori som bør sendes åpent.
- ✓ **Nett-til-nett VPN:** Helt uavhengig av W2k er IPSec en god og etterhvert meget populær løsning for sikring av nett-til-nett (ruter-til-ruter forbindelser). Som vi nevnte innledningsvis, foregår all sikring på nettverksnivå, ute av syne for brukere og applikasjoner, hvilket gir den grad av transparens som må til for at sikkerheten ikke skal komme i veien for effektivitet og produktivitet.

<sup>7</sup> Vi har ved tidligere anledninger – også i denne utgaven, se “VPN og smittefare” på side 27 – diskutert risikomomenter og krav til ‘god hygiene’ ved bruk av slike forbindelser.

**ICSAIabs** (en divisjon i selskapet TruSecure, Inc.) tester kompatibilitet mellom blant annet IPSec-implemterasjoner og produkter. Resultatene er å finne på [www.icsalabs.com/html/communities/ipsec](http://www.icsalabs.com/html/communities/ipsec).

## Oppsummering

IPSec er kort og godt blitt en nøkkel og en fundamental brikke i all tranportsikring av data – helt i tråd med ambisjonene fra utviklingen i standarden. Med solid støtte i W2k, bidrar Microsoft til å styrke denne utviklingen. IPSec-implemterasjonen er for det første et nyttig og forbausende allsidig hjelpemiddel for styrking av sikkerhet generelt. Dessuten sørger koblingene mot Active Directory (se forrige utgave) for en naturlig integrasjon med andre sikringstiltak.

## Neste utgave

I neste artikkel avslutter vi gjennomgangen av IPSec med en oppsummering av valgmulighetene som finnes, hvilke valg som anbefales og hvorfor.

Deretter tar vi fatt på RRAS, *Routing and Remote Access Services*, et annet element som er kritisk for sikkerheten i mange W2k-systemer. ■