Reference Guide

WinRoute Pro 4.1 SE

För version 4.1 Build 22 och sinare

Tiny Software Inc.

Innehållsförteckning

LÄS MIG FÖRST

Kära Kund,

Tack för att du köper/utvärderar WinRoute Pro. Tiny Software, ledaren inom brandväggsteknologi för små/medelstora nätverk, har lagt ner stor möda och mycket forskning på att ge dig en kraftfull men ändå lättanvänd router/brandvägg för Windows operativsystem.

WinRoute Pro är en nätverksapplikation som tillsammans med en dator väl ersätter en betydligt dyrare hårdvara baserad på routers och barndväggar. Som sådan kräver den att nätverket har ställts in riktigt och konfigurerats. En viss erfarenhet av nätverksomgivning krävs därför.

Läggg märke till att (grundat på vår statistik) omkring 90% av de problem kunder har att ansluta sitt nätverk till Internet orsalas av olämplig nätverkskonfiguration. This manual innehåller flera exempel på nätverkskonfiguration även om varje uppsättbing kan vara annorlunda med flera specialiteter.

Vi rekommenderar starkt att du mycket noggrannt läser igenom denna dokumentation. Den har utformats under antagandet att dess användare redan har grundläggande nätverkskunskap såväl som förmåga och kunskap att installera ett lokat nätverk (Local Area Network, LAN).

Om ytterligare tips, kontrollistor och heta uppdateringar behövs så ber Tiny Software sina kunder att först kontrollera på supportavdelningen online innan de ringer till Technical Support.

Vi vill återigen passa på att tacka dig för att du köper/utvärderar WinRoute.

Tack så mycket,

TINY SOFTWARE, INC.

KAPITEL 1

BESKRIVNING AV WINROUTE

I detta kapitel

WinRoute sammanfattning

WinRoute Pro är den ultimata mjukvaran för **routers/brandväggar på Internet** och gör det så gott som lönlöst att försöka manipulera alla datorer i ditt nätverk för att dela en enda Internet-anslutning! Anslut via telefonlinje, DSL, kabel, ISDN, LAN, T1, radio, DirecPC. Så lätt är det!

Fjärradministration

WinRoute Administrator ger konfiguration och inställningar för WinRoute Engine. WinRoute Administrator är en separat applikation (wradmin.exe) som kan köras från vilken dator som helst som har anslutning till datorn med WinRoute-motorn. Tillgången till motorn är säkrad genom stark kryptering och ett lösenord.

Loggning

WinRoute Pro ger dig en administratör med definitiv kontroll över den värddator den körs på. Administratören kan dra nytta av att analysera flödet av TCP, UDP, ICMP, ARP-paket, DNS-förfrågningar, drivkretsinformation och annat. Alla operationer har tidsmärkning.

NAT IP-router

WinRoute inbegriper de (bästa) implementeringarna av den teknologi för Network Address Translation (NAT) som finns tillgängliga idag. Den är utformad för att förse användare med det ultimata av routing-kapacitet och nätverksskydd. Drivrutinen för NAT som skrivits exklusivt för WinRoute erbjuder till väsentligt lägre kostnad en säkerhetslösning som är jämförbar med dyrare produkter .

Advancerad NAT-routing

Avancerad NAT ger möjlighet att ändra källans IP-adress för utgående paket baserat på flera olika kriterier. Detta säkerställer enkel integration LAN bakom WinRoute in i den totala WAN-omgivningen med olika segment, demilitariserade zoner, verkliga privata nätverk etc.

Värdservrar bakom WinRoute

I grundläget stänger WinRoute alla portar för maximal säkerhet. Därför avslås alla icke initierade förfrågningar såvida inte en mappning har skapats. Port Mapping technology allows users to decide how they want to divert IP packets passing through any interface operated by WinRoute. With WinRoute, users can set packets coming to a specific port to be passed to a specific internal computer. This allows them to run a web server, mail server, FTP server, VPN server or virtually any other type of server securely behind the firewall.

Brandväggssäkerhet

WinRoute ger användarna en nivå av brandväggskapacitet som är jämförbar med de som hittas i betydligt dyrare lösningar. Detta kan åstadkommas på grund av dess NAT-struktur och förmåga att fungera på låg nivå. Detta i sin tur tillåter WinRoute att fånga upp både inkommande och utgående paket, vilket gör det omöjligt att bryta igenom. Antispoofing är ett tillägg till WinRoutes paketfiltrering, för ytterligare skydd av LAN mot attacker där inkräktaren förfalskar ursprungliga IP-adresser.

Enkel nätverkskonfiguration

DHCP-servern och DNS-befordraren som kommer med WinRoute Pro förenklar administrationen av nätverkskonfiguration. Båda komponenterna är teknologiskt avancerade. WinRoutes DHCP-server kan lätt ersätta DHCP-servern som finns i Windows NT.

E-postserver

WinRoutes e-postserver, komplett med SMTP/POP3-kompatibilitet, praktisk taget obegränsade möjligheter att skapa alias och automatisk e-postsortering är extremt mångsidig. Användare kan ha en eller flera e-postadresser och kan effektivt arbeta i grupper (dvs. försäljning, support etc.) och varje grupp kan tilldelas flera användare. Alla dessa egenskaper finns tillgängliga oavsett typen Internet-anslutning som används.

HTTP-cache

WinRoutes struktur inbegriper en innovativ cache-motor. Till skillnad från proxyservrar med cache-funktionalitet, lagrar WinRoutes cacheminne passerande data i en fil av fördefinierad längd i stället för att använda en enda fil för varje objekt. Detta sparar signifikant diskutrymme speciellt i FAT16-omgivningar (det mesta av Windows95).

Omfattande protokollsupport

WinRoute stöder alla standardprotokoll för Internet inklusive:

IPSEC, H.323, NetMeeting Net2Phone WebPhone UnixTalk RealAudio RealVideo ICA Winframe IRC FTP HTTP Telnet PPTP Traceroute Ping Year 2000 Aol, chargen, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssl, ssh, systat, tacacs, uucpover IP, whois, xtacacs

NAT-router

I denna avdelning

Introduktion i NAT

NAT - Network Address Translation

Översättning av nätverksadresser, eller NAT,är en av WinRoutes mest kraftfulla säkerhetsegenskaper. NAT är ett koncept för Internet standardprotokoll med syfte att "gömma" privata nätverksadresser bakom en enda adress eller flera adresser. En version av NAT kallad "IP Masquerading" har i många år varit populär inom Linux-gemenskapen och WinRoute är en av få produkter för Windows-plattformen som faktiskt ger inträdesbiljett till NAT-funktionalitet.

NAT kan implementeras på många sätt men huvudsakligen skapar det ett nästan obegränsat utrymme för privatadresser i internationella nätverk som "översätts" av WinRoute så att meddelanden kan passera till och från allmänna nätverk utan att avslöja information om känsliga internsystem. Utan kunskap om det privata adressutrymmet på det internationella gränssnittet i en WinRoute-brandvägg är det praktiskt taget omöjligt att direkt attackera ett system på det NAT-skyddade interna nätverket.

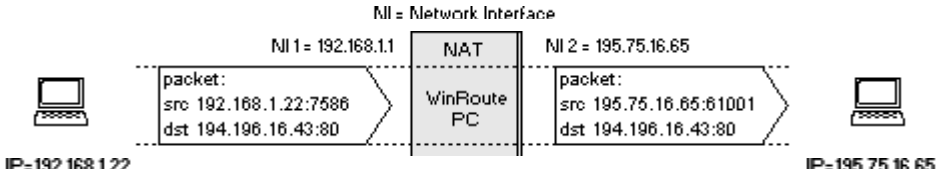
Hur NAT fungerar

Översättning av nätverksadresser (NAT) är en process som förändrar paket som skicktats från/till det lokala områdesnätet till/från Internet eller andra IP-baserade nätverk.

På vägen ut

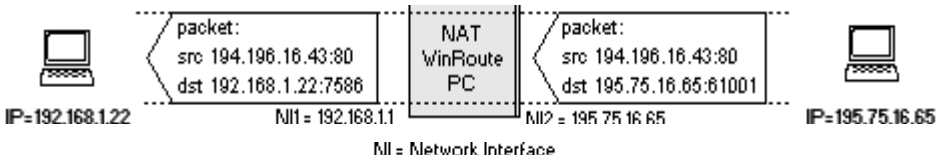
Paket som passerar via adressöversättningsmaskinen på väg från **från** LAN ändras eller översätts för att se ut som om de kom från den dator som styr NAT (denna dator är direktansluten till Internet). Vad som faktiskt händer är att "källans" IP-adress ändras i huvudet och ersätts av den (allmänna) IP-adressen för "NAT"-datorn.

NAT-maskinen skapar också en registreringstabell med information för varje paket som paserat genom till Internet.



På vägen tillbaka
Paket som passerar via NAT på vägen **TILL** LAN genomsöks och jämförs gentemot de register som NAT-maskinen har behållit. Där ändras "destinationens" IP-adress (baserat på registren i databasen) tillbaka till den specifika interna IP-adressen för att sedan nå datorn på LAN .

Kom ihåg att paketet ursprungligen kom med den allmänna IP-adressen för NAT-datorn som "destination". NAT-maskinen måste ändra denna information för att kunna leverera paketet till rätt mottagare inom det lokala nätverket.



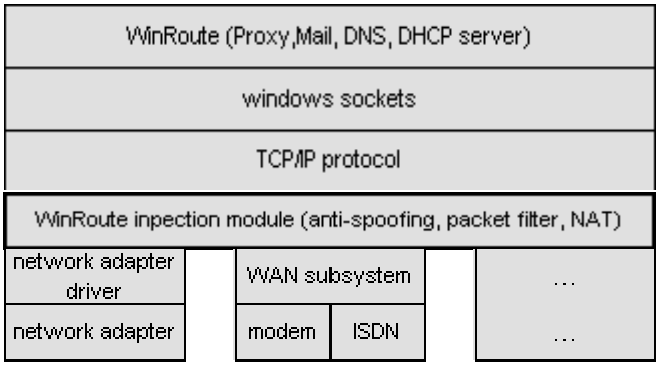
WinRoutes struktur

WinRoutes uppbyggnad

För avancerat arbete på Internet är det av nytta att förtså hur WinRoute arbetar. Att döma av förklaring och exempel här nedan visar sig WinRoute var en utmärkt lösning för nästan vilken nätverkskonfiguration som helst.

1. **Fullständig säkerhet**
   WinRoute abetar nedanför **TCP-stacken** på IPSEC-nivån. Med andra ord - den fångar upp både **utgående** och **inkommande** paketer **INNAN** de har haft en chans att komma in i din dator.

Denna avancerade utformning gör WinRoute nästan **oförstörbar.**



2. **Fullständigt protokollstöd**
   WinRoute är en ROUTER i mjukvaran. Som sådan kan Win Route, till skillnad från proxyservrar som WinGate eller WinProxy, tillåta nästan vilket Internetprotokoll som helst att passera igenom. Samtidigt kontrollerar WinRoute varje paket med användning av de avancerade säkerhets- och brandväggsegenskaper som finns inbyggda i mjukvaruutformningen. På system som kör Windows 95 och 98 hanterar WinRoute routingen av paketer. På system som kör Windows NT, utför operativssytemet NT routingen och WinRoute styr NAT-funktionaliteten och andra data.

3. **Fullständig flexibilitet**
   WinRoute utför NAT (Network Address Translation) i det gränsnsitt du valt. WinRoute utför också vilka förinställda säkerhetsregler som helst på de specifika gränssnitten. Detta ger användaren stor frihet när han utformar och konfigurerar säkerhetsvalen.

Att ställa in NAT på båda gränssnitten

Du kanske önskar använda WinRoute endast som den **neutrala åtkomstroutern** för den trafik (paket) som kommer från **Internet** till ett **lokalt nätverk**. I det fall du redan har en lösning för delad Internet-tillgänglighet; om denna lösning inte tillåter dig att köra servrar och applikationer på ditt privata nätverk som måste vara tillgängliga från Internet kan WinRoute vara rätt lösning i denna specifika konfiguration.

Exempel på tjänster du kanske önskar vore tillgängliga från Internet är:

- telnetserver (dvs.AS400)
- WWW-server
- Mail Server
- PC Anywhere
- FTP server
- … och vilken annan server (tjänst) som helst som är tillgänglig på en särskild port.

WinRoute kommer att ge dina användare/kunder pålitlig och säker tillgång till sådana tjänster. Konfigurationen av WinRoute för dessa tjänster beskrivs i andra kapitel:

Egenskap	Normal rekommendation	Med detta scenario
Gränssnitt NAT på Internet	PÅ	PÅ
NAT på internt (LAN) gränssnitt	AV	PÅ
WinRoutes interna gränssnitt för IP-adress som standardgateway för de andra datorerna inom nätverket	JA (ett MÅSTE)	NEJ (ej nödvändigt)

Med andra ord - att använda WinRoute kommer att tillåta dig att göra vissa andra tjänster från Internet tillgängliga UTAN att du behöver ändra nätverkskonfigurationen.

- ***OBS! Genom att installera NAT på båda gränssnitten kommer du INTE att kunna använda WinRoute för gemensam Internet åtkomst!***

Standardinställningen för din gateway i detta exempel ger dig stor frihet. Du kan behålla alla existerande omgivningar oförändrade. För att behålla de routers och routes som redan har upprättats inom ditt nätverk genom arbetet, kan du genom att lägga till nya datorer som kör WinRoute, låta externa användare få tillgång till servrarna inom ditt lokala nätverk.

Detta är bra (till exempel) när du har en befintlig WAN och du vill tillåta externa användare att få tillgång till din AS400 (telnetserver) eller ditt interna nätverk genom PPTP.

För att göra det måste du följa följande steg:

1. Koppla in en dator med två gränsnitt till ditt nätverk. Ett gränssnitt (externt) kommer att länka till Internet medan ett annat (internt) kommer att länka till ditt existerande nätverk.
2. Tilldela det externa gränssnittet en IP-adress som kommer att användas för tillgång till de tjänster/servrar som du skulle vilja göra tillgängliga från Internet.
3. Tilldela den interna IP-adressen antingen manuellt eller via DHCP-server

4. Ställ in WinRoute att utföra NAT på båda gränssnitten
5. Ställ in portmappning för de tjänster du vill köra inom ditt nätverk

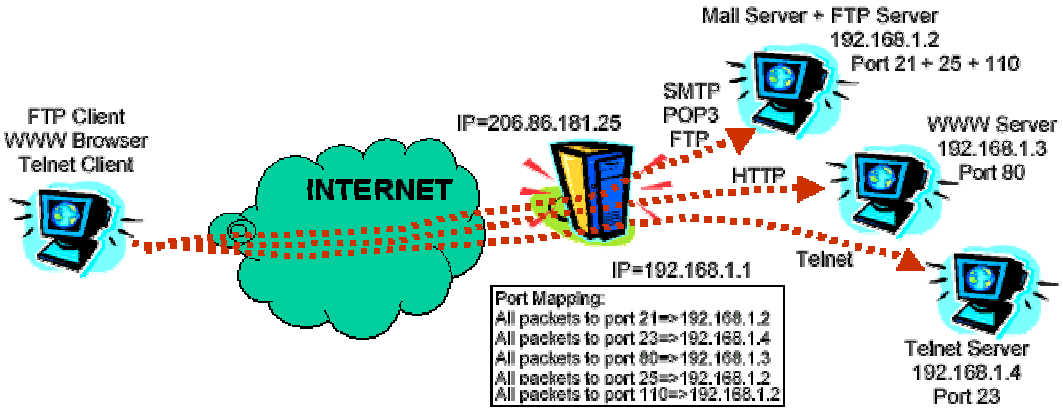
När du gjort dessa inställningar kommer de externa användarna att från Internet kunna få tillgång till dina interna tjänster som körs på specifika portar. Säkerheten vid sådan tillgång garanteras av WinRoutes brandvägg.

Portmappning - paketbefordran

WinRoute utför NAT, vilket gör det omöjligt att utifrån gå in i det skyddade nätet. Med användninga av allmänna portmappningstjänster (eller Port Address Translation - PAT) som en WWW-server eller en FTP-server och andra som körs på ditt privata nätverk kan de bli åtkomliga från Internet.

Hur portmappning fungerar

Varje paket som tas emot från nätet utanför (från Internet) kontrolleras för att se om deras attribut (dvs. protokollet, destinationsporten, och destinationens IP-adress) överensstämmer med en uppgift i portmappningstabellen (protokoll, avlyssningsport, avlyssnings-IP). Om det anländande paketet motsvarar önskade kriterier modifieras det och skickas till IP-adressen för det skyddade nätverket vilken definierats som "destinations-IP" i tabellens uppgift och till den port som definierats som "destinationsport".



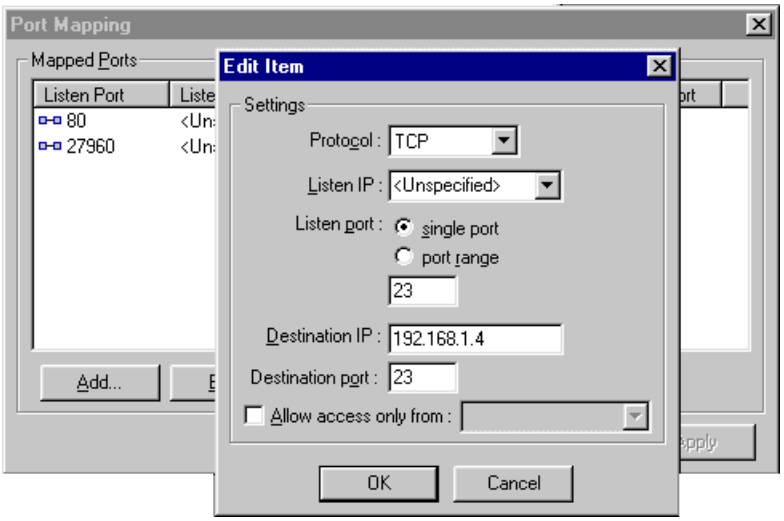
Om du till exempel kör en webbserver på en intern IP 192.168.1.3 och du önskar ge användare från Internet tillgång till den kommer förfrågningar från Internet att komma till din WinRoute-dator med extern IP-address som är lika med DNS-uppgiften för din webbserver www.yourdomain.com. Eftersom alla förfrågningar till webbservern kommer på port 80 kommer du att sätta upp en portmappning som säger att all TCP-kommunikation på port 80ska styras om till den interna IP-adressen 192.168.1.3.

Konfiguration av portmappning

Att ställa in portmappning

1 Gå till menyn *Inställningar->Avancerat->Portmappning*

2 Lägg till ny portmappning:



Protokoll

Välj det protokoll som används av applikationen/tjänsten. En del applikationer/tjänster använder TCP- och UDP-protokoll tillsammans. Så till exempel modulen WinRoute Administrator

Avlyssnings-IP

Den IP-adress som de inkommande paketen kommer till. Vanligtvis är IP-adressen förbunden med ditt Internetgränssnitt. Obs: du kan ha mer än en IP-adress förbunden med gränssnittet (om du t.ex. har flera webbservrar)

Avlyssningsport

Det portnummer som paketen kommer till.

Destinations-IP

Den IP-adress inom dtt lokala nätverk som kör servern (tjänsten) som besvarar inkommande paket (webbserver, FTP-server etc.)

Destinationsport

Den port på vilken destinationsapplikationen avlyssnar. I det typiska fallet samma nummer som avlyssningsporten.

Ge tillgång endast från

Du kan ange den IP-adress från vilken du önskar ge tillträde. Detta är mycket viktigt för en ökad säkerhet i fall du ställer in portmappning för fjärrstyrningsapplikationer som WinRoute administrator, PC Anywhere etc. Du kan ange grupp av IP-adresser. Du måste först skapa en sådan grupp i dialogrutan "Adressgrupper".

Portmappning för system med flera hem (flera IP-adresser)

Du kan ha flera IP-adresser tilldelade till Internetgränssnittet och inom ditt nätverk köra multipla tjänster som du vill göra tillgängliga från Internet.

Scenario 5xWWW-servrar

Låt oss som exempel anta att du vill köra 5 webbservrar där var och en av dem har en separat domän ansluten med olika IP-adresser.

I ett sådant scenario kommer du att tilldela 5 IP-adresser till ditt externa gränssnitt (länkade till Internet) och köra webbservrar på andra datorer inom ditt interna nätverk.

Varje webbserver kan köras på en separat dator eller du kan tilldela fler IP-adresser till en dator på ditt interna nätverk och köra alla webbservrar på en sådan dator.

Sedan kommer du att definiera 5 portmappningar i en portmappningsdialog. För varje webbserver (domän) kommer du att definiera:

- IP-adress för avlyssning (allmän IP-adress associerad med domänen)
- Avlyssningsport: 80 i vårt scenario
- IP-adress för destination: den IP-adress som kör webbservern
- Destinationsport: 80 (för www)

För fler exempel på Avancerad portmappning se kapitlet Mer avancerat (Inter)netarbete.

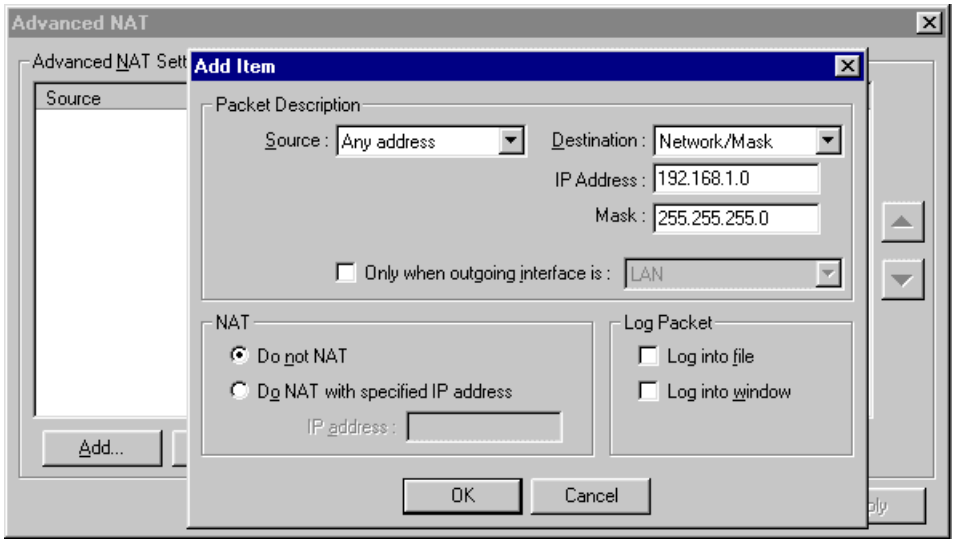
Multi-NAT

WinRoute tillåter enkel **NAT** (Network Address Translation) och även mer komplicerade inställningar. Baserat på paketets IP-adress för **källa** eller **destination** kan du ange att NAT ska förses med någon **annan IP-adress** (dvs. paketen skulle se ut som om de ursprungligen kommer från en annan IPadress) eller att **NAT** inte ska utföras överhuvudtaget.

Sådana inställningar är av största vikt tillsammans med inställningar för mer komplicerade nätverk där:

- vissa datorer ska se ut som **en annan** IP-adress än den huvudsakliga som används av **resten** av nätverket
- du har filialer anslutna till **WAN** med privat adressutrymme och du vill att de alla ska dela **en** Internet-tillgång
- du har multipla segment bakom WinRoute där en (eller flera) segment är DMZ-zon med allmänna IP-adresser
- du vill ha allmänna IP-adresser inom ditt privata nätverk (Kom ihåg! Du måste bekräfta med din ISP att dessa IP-adresser kommer att routas genom din huvudsakliga IP-adress.)

Du kan hitta en hel del exempel på användning av "Avancerade NAT-inställningar" i kapitlet Mer Avancerat (Inter)netarbete.



IP-adress för källa, IP-adress för destination

Du kan utföra avancerade NAT-inställningar baserade på den IP-adress från vilken de skickas (källa) eller den de skickas till (destination). Som källa kan du mata in en värd-IP, hela nätverket (begränsat av nätverksmasken) eller den grupp av IP-adresser som du tidigare har skapat i menyn Inställningar->Avancerat->Adressgrupper.

Utför inte NAT

Om du markerar detta kommer paket som passerar genom Internetgränssnittet inte att ändras

Utför NAT med angiven IP-adress

Om du markerar detta kommer paket som passerar genom att ändras som om de ursprungligen kom från önskad IP-adress.

Gränssnittstabell

Gränssnittstabellen är en dialog där WinRoute visar alla i datorn tillgängliga gränssnitt som den har kunnat känna igen. Om du skulle ha fler gränssnitt än WinRoute är det troligt att drivrutinen för dess gränssnitt inte har laddats som de ska av operativsystemet och att WinRoute inte kunde läsa det.

Du kan se:

Gränssnittets namn

du kan ändra namnet genom att markera "egenskaper" och ändra namnet.

IP-adress

det värde som ställts in i TCP/IP-egenskaper för gränssnitt. Om gränssnittet har ställts in på att få en IP-adress från DHCP-servern skulle du kunna se den aktuela IP-adressen som tilldelats gränssnittet.

NAT "på" eller "av"

om NAT har ställts in för att utföras på gränssnittet så visas "på" i denna kolumn

VPN-support

Som tidigare nämnts är WinRoute fullt kapabelt att släppa igenom trafik från de två mest populära VPN-protokollen som används idag : IP Security protocol (IPSec) föreslaget av IETF och Point-to-Point Tunneling-protokollet som blivit populärt under senare år eftersom det ingår i Microsoft Windows mjukvara för klienternas operativsystem.

Brandvägg med paketfilter

I denna avdelning

Översikt över paketfiltrering

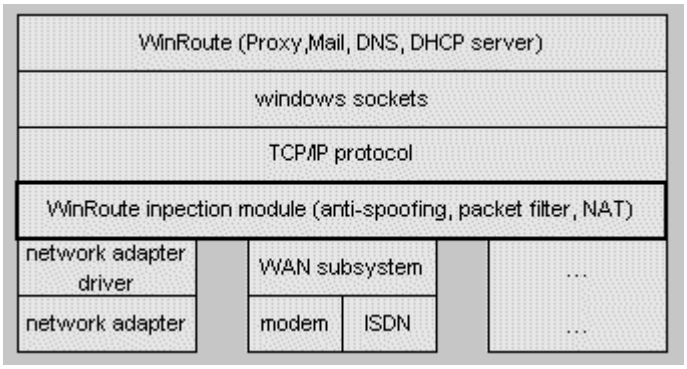
Hjärtat i varje mekanism för kontroll av tillgång till brandvägg är naturligtvis den teknologi genom vilken den tillåter eller nekar paket destinerade för det skyddade nätverket. WinRoute tillämpar en av de vanligaste teknologierna för kontroll över tillgång till nätverk: paketfiltrering. Även om WinRoute implementerar mekanismer för kontoll över tillgång, som till exempel en proxyserver med cacheminne för HTTP, FTP och gopherprotokoll, så är detta primärt avsett som ett element för att höja den utgående prestandan och inte en säkerhetsegenskap.

Paketfilrering har en lång tradition bland dem som arbetar med säkerhet och det används fortfarande i stor utsträckning i produkter som Ciscos IOS operativsystem för nätverksanordningar. Ordentligt konfigurerade kan paketfilter bli helt säkra och är särskilt lämpliga för Internetplatser med mycket trafik eftersom det ger de bästa prestandafördelarna.

Struktur

Brandväggar byggs vanligen på härdade plattformar och själva mjukvaran brukar vara svår att kringgå. En viktig svaghet hos många anordningar för nätverkssäkerhet är emellertid under den korta fönstertid som inträffar från det att hårdvaran aktivt kan routa trafik tills att mjukvaran tar över kontrollen över nätverkets gränssnitt. Under detta kritiska ögonblick kan säkerheten fullständigt sättas ur spel.

WinRoutes drivrutin eller motor aktiveras när internminnets filer i Windows operativsystem (kärnan) laddas in i minnet; speciellt motorn laddas innan NDIS (Network Device Interface Specification)-modulerna laddas så att nätverkets anslutningsbarhet stöds innan WinRoute är aktivt. På så vis är skyddet av gränssnitt aktivt innan illasinnad trafik eller andra angrepp kan sättas in på systemet. Detta kan med fördel jämföras med självständiga produkter för upptäckt av intrång vilka körs som en tjänst och inte är aktiva förrän systemet har startat.



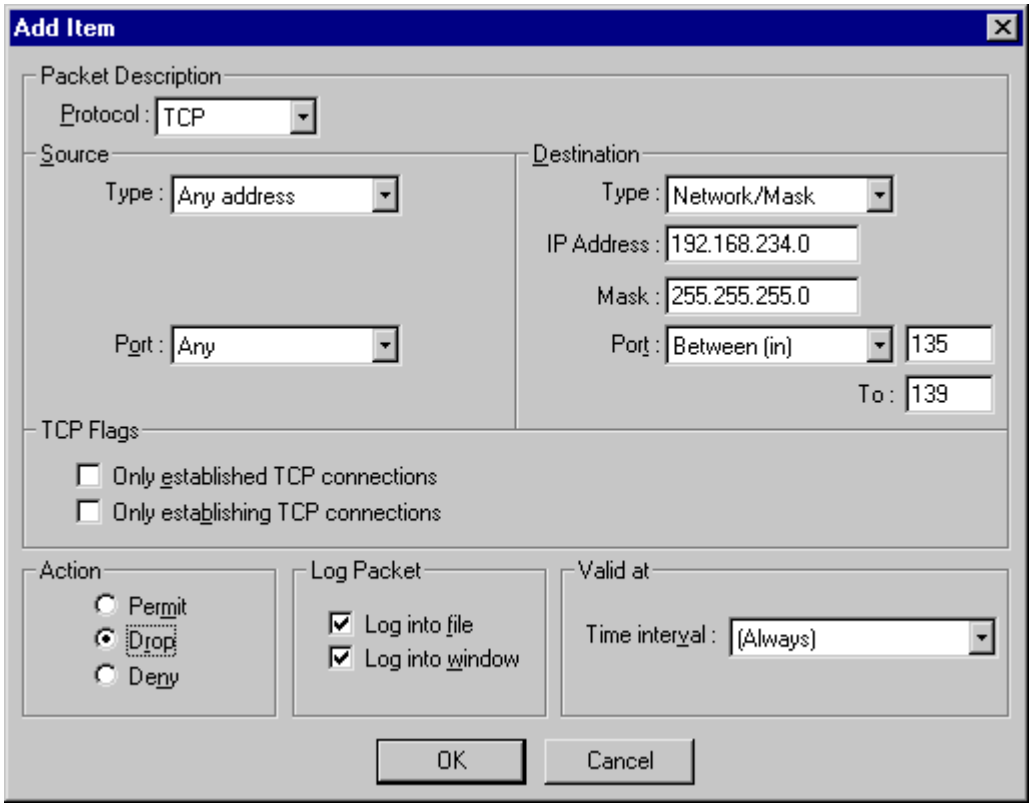
WinRoute "sveper in" NDIS i sina egenskaper på sådant sätt att all TCP/IP-trafik växlas från drivrutinen för nätverkets gränssnisttskort (NIC) till motorn innan den fortsätter in i nätverkets kommunikationsstack till själva operativsystemet.

Detta införande på låg nivå i operativsystemet ger WinRoute-motorn ett unikt perspektiv över all nätverkstrafik som kommer in på något gränssnitt (oavsett om det är in- eller utgående). Som med många brandväggsprodukter av företagsklass som till exempel Check Point's Firewall-1, ges WinRoute tillåtelse att ta det första beslutet om huruvida ett paket ska ges eller nekas tillstånd. Återigen hindrar detta illasinnade angrepp mot andra apekter i operativssytemet eller annan mjukvara som skulle kunna leda förbi den säkerhet som erbjuds av en brandvägg. Detta är förvisso önskvärt för Internet-gateways som är riktade utåt men kan också innebära stora fördelar för självständiga värdar med hög säkerhet eller krav på anonymitet, som till exempel ett system för upptäckande av intrång. Mjukvara för upptäckande av intrång som till exempel Real Secure från Internet Security Systems (ISS) skulle vara praktiskt taget osynlig på en värddator som skyddas av WinRoute.

Till sist ska det sägas att WinRoute-motorn tar över alla funktioner för kommunikationsrouting från det underliggande Windows operativsystem (det må vara Windows 9x, NT, eller 2000). Detta säkerställer att ingen trafik skulle routas mellan nätverk om WinRoute-motorn av någon anledning skulle slås ut. Denna "stängning vid utslagning" har varit den traditionella standarden för brandväggskonfigurationer i många år och tjänar till att skydda privata nätverk i fall av allmänna systemkrascher.

Regler

Trots de teoretiska frågor som omger paketfiltrering så är den främsta orsaken till misslyckande för moderna brandväggssystem felaktig konfiguration, särskilt av administrativ personal utan erfarenhet. WinRoute gör filterkonfigurationen enkel och ändå tillräckligt flexibel för att till och med nätverksadministratörer som är nybörjare med lite kunskap om TCP/IP och ett par musklick kan implementera en säker konfiguration, så som visas på följande skärmbild.



Filterregler kan appliceras på basis av varje gränssnitt till samtliga följande enheter:

- en enda IP-adress

- en administratörsdefinierad lista över IP-adresser
- ett helt nätverk eller undernät

Det är även viktigt att här observera att filter kan ställas in både för inkommande och utgående trafik.

Dessa egenskaper tillåter att man på millimetern skräddarsyr reglerna för åtkomst till säkerhetsbehoven för nästan vilken organisation som helst. En grupp webbutvecklare skulle till exempel kunna garanteras tillgång till specifika externa resurser som anonyma FTP-understödjande servrar eller en specificerad lista över interna adresser kan anges som tillgängliga för externa kompanjonnätverk för avlämning av elektroniska filer. Den ingående/utgående konfigurationen ger skydd mot illasinnade "inifrån-ut-angrepp" som Back Orifice (BO) eller servlets för distribuerat nekande av tjänster (DDOS) som försöker kommunicera med externa angripare via opåitliga protokoll tillbaka ut genom brandväggen .

Regler kan antingen tillåta, negligera eller neka specificerad trafik; åtgärden att att negligera är det som lämnar ut minst information om brandväggen till potentiella angripare eftersom den inte skickar något ICMP Administrative Prohibited Filter eller något TCP Reset/Acknowledge-svar till ett TCP SYN-paket (det första steget i standardsekvensen på tre steg för TCP-handskakning).

Regler kan prioriteras för att agera i en specifik användardefinierad ordning på inkommande eller utgående paket. Den populäraste användningen av denna förmåga är att lägga till så kallade "upprensningsregler" till filterlistor som blockerar all trafik som inte specifikt tillåtits av tidigare regler som har prioritet i listan (för exempel på en upprensningsregel, se Prov på grunduppsättning av regler för paketfilter, längre fram i detta dokument).

Protokoll

Protokoll som stöds av WinRoutes paktefilter inbegriper:

- rå IP
- sju ICMP-typer (eller alla)

- TCP
- UDP
- PPTP.

Förmågan att kunna blockera råa specifika ICMP-typer eller råa IP-protokoll är ovärderlig för nätverksadministartörer som har att göra med en ständigt växande lista över applikationskrav som ska understödjas. Särskilt en del ganska nya VPN-protokoll som IPSec går över de råa IP-protokollen 51 och 52, vilka skulle vara omöjliga att filtrera med användninga av några av de mer begränsade brandväggsprodukterna som finns på marknaden idag och som endast kan kontrollera TCP- elle UDP-baserade protokoll.

Antispoofing

Dessutom ger WinRoute kapacitet för antispoofing, vilket hindrar paket med ogiltiga källadresser från att skapas inom ett nätverk. Antispoofing skulle med det distribuerade nekandet av tjänster ha kunnat förhindra de ICMP-smurfangrepp som rapporterades i februari 2000 på sådana större webbplatser som Yahoo och Buy.com. WinRoute-användare kan sova lugnt i vetskap om att deras nätverk är osannolika källor för sådana angrepp om de har implementerat denna egenskap .

Analys av loggar och paket

I denna avdelning

Om loggar och analys

En kritisk funktion i alla säkerhetsprodukter är förmågan att vid alla tidpunkter registrera händelser på ett tillräckligt detaljerat sätt. WinRoute registrerar sex olika trafikloggar som inverkar på brandväggen, inkluderande paket som passerar genom den, användaraktiviteter, filteråtgärder och så vidare. En beskrivning av varje logg visas i följande tabell:

HTTP-logg	Visar enbart HTTP-data som passerar genom WinRoutes proxyserver; inbegriper källans IP-adress och användarnamn, tidsmärkning och HTTP-förfrågningar och svar
E-postlogg	Registrerar alla åtgärder från WinRoutes inbyggda e-postserver; registrerar sändnings-/mottagningsaktiviteter hos SMTP och POP3
Säkerhetslogg	Visar alla aktiviteter definierade som "Logga till fönster/fil" i paketfiltrets regler (se nedan för detaljerad beskrivning av de uppgifter som registreras)
Uppringningslogg	Registrerar ords användningsinformation för uppringningsgränssnitt styrda av WinRoute
Felsökningslogg	A la carte-inställningar för att installera alla ARP-, ICMP-, UDP-, TCP- och/eller DNS-paket som fysiskt passerar över någon som helst WinRoute router; millimeternogrann konfiguration tillgänglig under Inställningar | Avancerat | Felsökningsinfo, Felsökningstab.
Fellogg	Visar alla ej lyckade åtgärder som händer alla WinRoute-moduler som körs

Loggning kan visas på WinRoute-administratörens konsol, skrivas till en fil eller båda delarna. Loggfilerna lagras i \%installroot%\Logs, vilken endast är tillgänglig för de NT/2000-konton inom Administratörer, Serveroperatörer , SYSTEM och SKAPAREN ÄGAREN som installerade WinRoute.

Den logginformation som registreras av WinRoutes säkerhetslogg är robust, inbegripet all nödvändig information för att påbörja en riktig undersökning om potentiella illasinnade aktiviteter:

- Datum
- Tid
- Regel för paketfilter som påverkats
- Gränssnitt
- Åtgärd (tillåt, ignorera, neka)
- Protokoll
- Källans IP-adress och TCP-port
- Destinationens IP-adress och TCP-port

Testning under ogynsamma villkor med hög trafik påverkar inte WinRoutes loggningsförmåga. Detta är viktigt för att undvika förlust av värdefulla juridiska data såväl som underlätta möjliga situationer med nekande av tjänst där brandväggsfunktionaliteten lägger av om loggningssytemet blir överansträngt.

Felsökningslogg

Felsökningsloggen är den viktigaste loggen i WinRoute. Den gör att du kan se **alla IP-paket** (TCP, UDP, ICMP, ARP, DNS) som rent fysiskt passerar något av de gränssnitt som finns i WinRoute-datorn.

I **Felsökningsloggens** fönster kan du se den uppsättning av händelser som du kanske vill ska visas .

Hur ska loggen läsas?

Från vänster kan du se följande:

Tidsmärkning - datum och tid som visar exakt när händelsen inträffade eller paketet passerade över gränssnittet.

Protokollet - typ av protokoll för paketet

Från/till gränsnittsnamn - namn på gränsnittet och huruvida paketet gick **till** eller kom **från** gränssnittet (tänk att WinRoute körs på datorn och gränssnitten menas vara "grindarna" mellan datorn och nätverket).

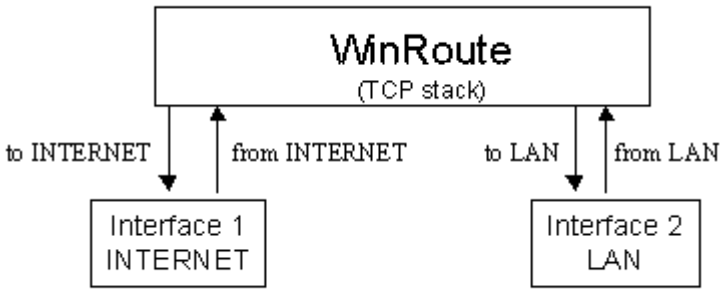
Källans IP -> Destinationens IP-adress - källans och destinationens IP-adresser finns i paketet.

Flaggorna - ytterligare identifiering av åtgärden.

Exempel:

```
[10/Nov/1999 09:32:38] TCP: packet 511464, from lan,
length 1514, 192.168.1.7:2442 -> 192.168.1.1:25,
flags: ACK

[10/Nov/1999 09:32:38] TCP: packet 511465, to lan,
length 54, 192.168.1.1:25 -> 192.168.1.7:2442, flags:
ACK
```


WinRoute
(TCP stack)
to INTERNET
from INTERNET
to LAN
from LAN
Interface 1
INTERNET
Interface 2
LAN

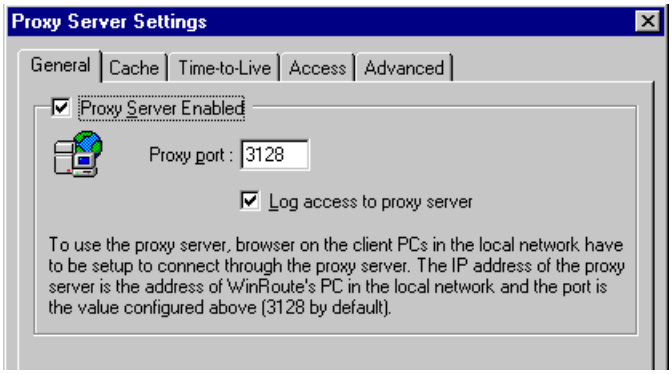
HTTP (proxy) logg

HTTP (proxy)-loggen är ett kraftfullt verktyg som hjälper dig att hålla reda på användarnas aktiviteter på Internet. Den ger en mer användarvänlig information om användare som går ut på nätet än den du skulle få från felsökningsloggen.

När är loggen i gång?

HTTP (proxy)-loggen visar endast data som går genom WinRoutes proxyserver. Det innebär att om du vill få data från proxyservern bör du tvinga användarna att gå genom proxyservern . Se Exempel för brandväggar eller kapitlen om proxyservrar.

Du måste också aktivera loggåtkomsten till proxyserverns konfiguration.



Hur ska HTTP (Proxy)-loggen läsas?

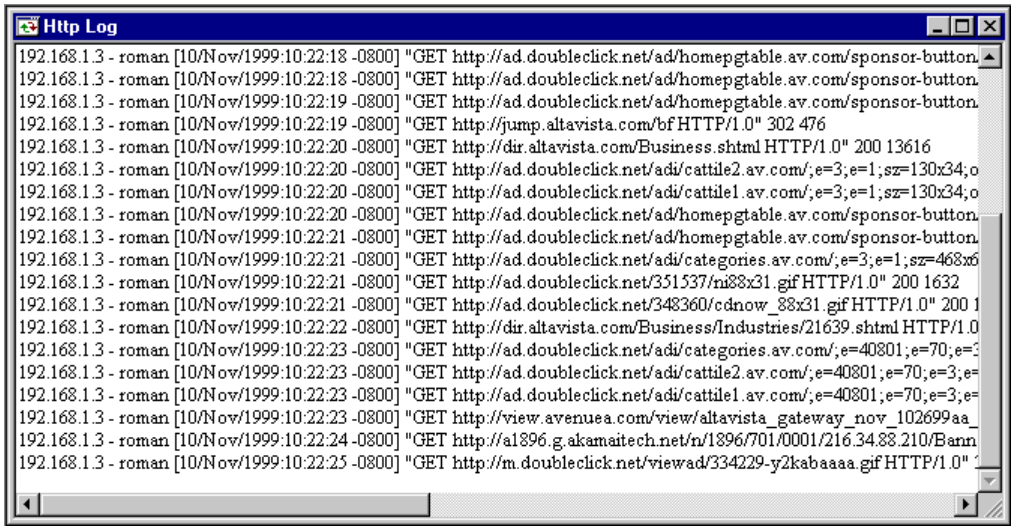
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200
13616
```

Från vänster till höger:

IP-adress - namn - namn och aktuell IP-adress på den användare som har tillgång till Internet

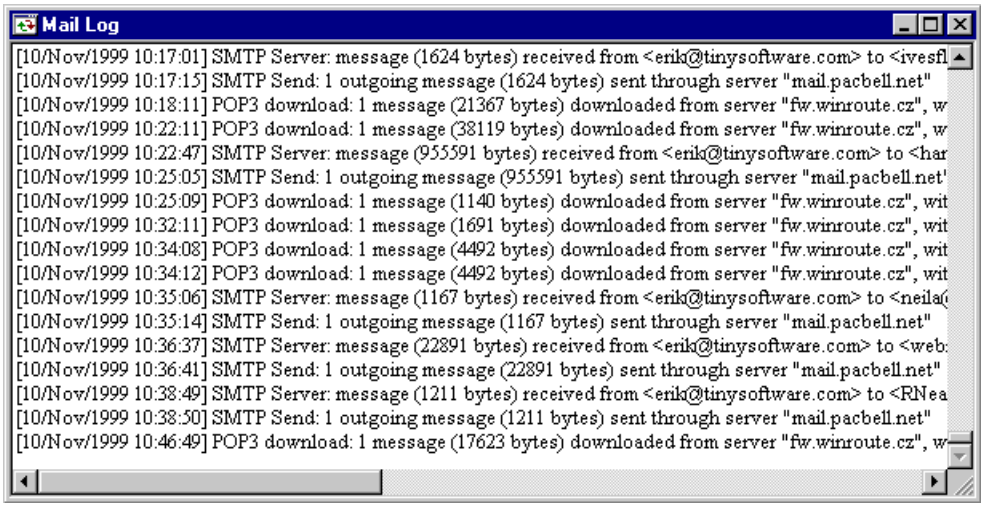
Tidsmärkning - datum och tid för tillgång

GET "http..." - målet för tillgången



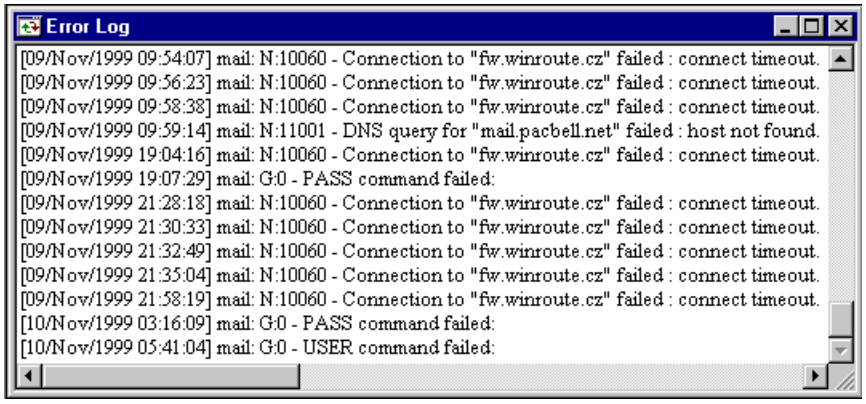
E-postlogg

E-postloggen registrerar alla operationer hos WinRoutes inbyggda e-postservrer. Du kan se hur många meddelanden som har skickats, mottagits, vart meddelandena har skickats etc. Alla operationer har tidsmärknng.



Fellogg

Felloggen visar alla icke framgångsrika operationer i de moduler av WinRoute som är påslagna. Som ett resultat av detta kan du se felen i e-postutbytet, DNS-servern etc.



DHCP-server

I denna avdelning

DHCP översikt

I ett nätverk måste varje dator ha sitt TCP/IP-protokol ordentligt konfigurerat. Detta innebär att IP-adressen, nätverksmasken, adressen till deras standard gateway, DNS-serverns adress, etc. måste vara konfigurerade på varje dator. Om handhavaren måste ställa in parametrarna manuellt på ett större antal arbetsstationer, är det svårt att undgå misstag, dvs. att använda samma adress två gånger - vilket kan orsaka kollisioner och följaktligen också en felaktig funktion i hela nätverket .

Dynamic Host Configuration Protocol är en implementering av WinRoute avsedd att förenkla uppgiften med nätverksadministration. DHCP används för dynamisk konfiguration av TCP/IP-protokollet på datorer. Under uppstart skickar DHCP-klientdatorn en förfrågan. När DHCP-servern tar emot förfrågan, väljer den TCP/IP-konfigurationsparametrar för klienten. Parametrarna är IP-adress, nätverksmask, standard-gateway, DNS-serverns adress, klientens domännamn etc. Med användning av parametrarna skapar servern ett svar och skickar det till klienten.

Servern kan tilldela en konfiguration till klienten för endast en begränsad tid (den så kallade uthyrningstiden). Servern tilldelar alltid IP-addressen på så sätt att den inte kolliderar med någon annan adress som tilldelats en annan klient genom DHCP.

Med en tilgänglig DHCP-server räcker det att aktivera alternativet "Skaffa IP-adress från DHCP-servern" för att DHCP-servern ska ta över ansvaret för rätt konfiguration av TCP/IP på arbetsstationer. Detta kan hjälpa till att avsevärt minska kostnaderna för underhåll och ledning av nätverket.

- ***Om en del datorer i ditt nätverk inte konfigureras dynamiskt av DHCP utan i stället har en fast konfiguration, måste du försäkra dig om att de parametrar som används av DHCP inte kolliderar med dem som används i de fasta konfigurationerna.***

DNS-befordrare

I denna avdelning

Om DNS-befordran

Varje dator som är ansluten till Internet identifieras av en unik numerisk IP-adress. För att ansluta till en dator på Internet måste dess adress vara känd av den dator som skapar anslutningen. Eftersom IP-adresser är svåra att komma ihåg skapades Domain Name Service.

DNS är en databas över beskrivande namn som anses vara lätta att minnas. På så vis behöver inte användaren känna till IP-adressen till den server han/hon önskar kommunicera med. Det räcker med att mata in rätt namn (t.ex. www.yahoo.com) och DNS kommer att hitta den verkliga IP-adressen.

DNS-befordrare i WinRoute

WinRoute är utrustad med en DNS-modul som kan vidarebefordra DNS-förfrågningar till en utvald DNS-server på Internet. DNS-modulen lagrar resultaten av förfrågningarna i sitt interna cacheminne där de finns kvar en viss tid. På varandra följande och upprepade förfrågningar besvaras därefter med användning av uppgifterna i cacheminnet utan att man behöver vänta tills ett svar från Internet kommer.

DNS-befordraren i WinRoute är kapabel att besvara DNS-förfrågningarna i enlighet med de användardefinierade filerna på VÄRDDATORN. När en DNS-förfrågan har kommit in tittar WinRoute först på VÄRDDATORNS filer innan det vidarebefordrar DNS-förfrågan till Internet. Om motsvarande registering hittas besvaras frågan med dess värde, om inte vidarebefordras den till DNS-servern på Internet.

Proxyserver

I denna avdelning

Proxy översikt

Huvudsyftet med en proxyserver är att **spara bandbredden** på din Internetanslutning åt dig. Om användare har tillgång till Internet genom en proxy kan proxyservern **spara** de olika efterfrågade objekt som passerar igenom (som HTML-sidor, bilder, och andra slags filer) i sitt **cacheminne**.

Om sidorna eller bilderna på nytt efterfrågas av samma användare eller av någon annan kommer proxyservern att ta fram det efterfrågade objektet från sitt cacheminne. Detta **minskar** belastningen på Internetanslutningen och hela operationen går också mycket snabbare än en ny nedladdning från Internet.

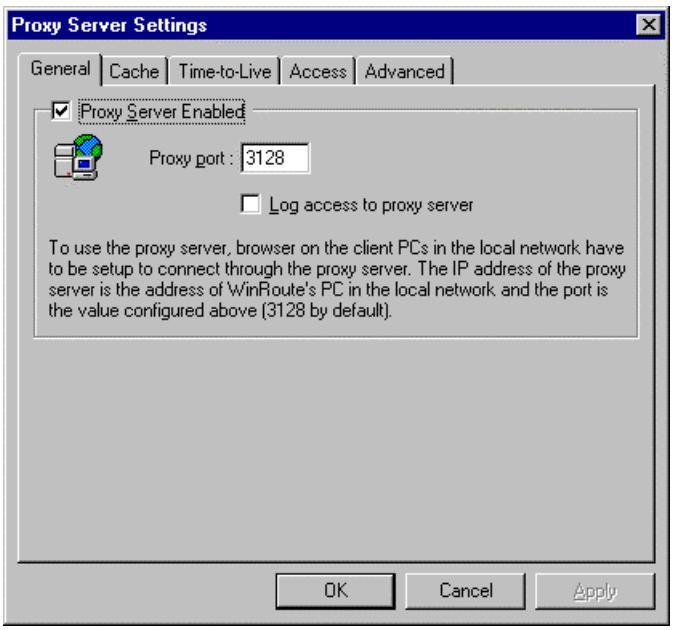
Å andra sidan blir objekt som är lagrade i en proxyservers cacheminne inaktuella. Man måste avväga **TTL** (Time-To-Live) på lagrade dokument noga för att undvika missförstånd som uppstår ur det faktum att du just läst gårdagens CNN-nyheter - till exempel.

Snabb installation

Först och främst - med WinRoute **behöver du inte** proxyservern för att få tillgång till Internet. Din Internetanslutning underhålls väl av en **NAT-router** som WinRoute har i sig. NAT är mycket bättre för delat Internet än vad proxyteknologin är. Men WinRoute har även en proxyserver för att kunna erbjuda cachefunktionalitet när så behövs.

För att börja använda proxyserver i WinRoute, följ dessa enkla steg:

1. I WinRoute Administration väljer du tabben *Inställningar -> Proxyinställningar -> Allmänt*. Markera alternativet "Proxyserver aktiverad". Behåll det ursprungliga portnumret 3128.



2. I din Internetwebbläsare (Explorer, Netscape, Opera...), gå till proxyinställningar, välj en manuell proxykonfiguration och mata in WinRoutes PC-adress som proxyserverns adress för HTTP, FTP och gopherprotokoll. Mata in 3128 som proxyns portnummer för alla protokollen.
3. Testa installationen genom att gå in på någon webbsida från webbläsaren.

Tab för allmänna egenskaper

Proxyserver aktiverad

Använd denna för att slå på och av proxyservern.

Portnummer

Det portnummer på vilket proxyservern lyssnar efter förfrågningar. Vanligen finns det inget behov av att ändra standardnumret 3128.

Loggtillgång till proxyserver

Med detta alternativ aktiverat registrerar webbläsaren alla URL som efterfrågats av proxyn i en logg.

Kontroll av användartillgång

WinRoutes proxyserver tillåter administratören att du kontrollerar tillgången till webbsidor. Administratören kan besluta att tillgången till vissa webbsidor eller domäner endast kommer att tillåtas angivna användare och/eller användargrupper.

Att tvinga användare att använda proxyserver

Om du beslutar dig för att använda proxyns åtkomstkontroll behöver du också blockera direkttillgången till webbsidorna så att åtkomsten via proxyn blir det enda återstående alternativet för sökning på Internet. För att blockera direkttillgång, definiera en regel för paketfiltrering. För information om paketfiltrering se avdelningen ***Paketfilter*** (see "Att tvinga användare att använda proxyserver" on page 123) i WinRoutes användarguide.

Att konfigurera proxyns åtkomstkontroll

För att konfigurera WinRoutes kontroll av proxytillgång gå till "Tillgångstabben" i Inställningar av proxyserver

Tillgångslista

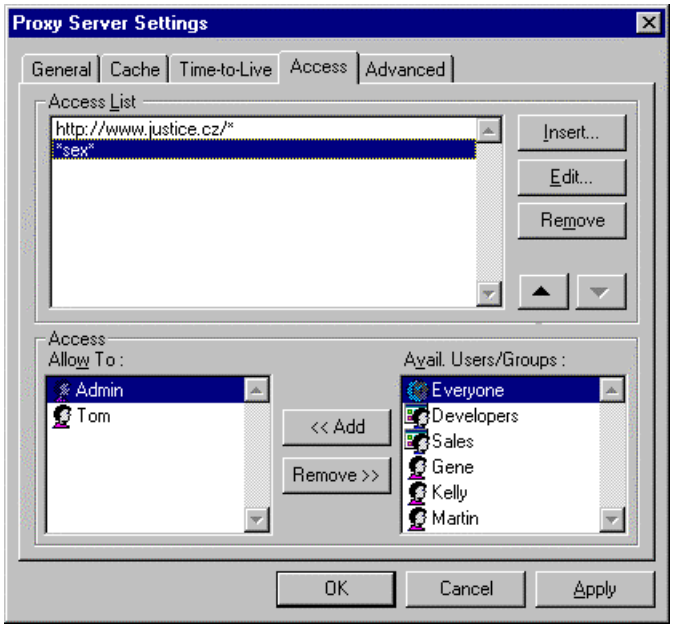
Listan över URL som är begränsade. Du kan använda asterisk som ersättningstecken (wild card) i URL. För att till exempel matcha alla datorer i somedomain.com, använd strängen"*.somedomain.com". WinRoute 4.0 använder även testning av substrings för att matcha URL, så matchar till exempel strängen "sex" samma uppsättning av URL som strängen "*sex*" (enbart den senare varianten stöddes i tidigare versioner av WinRoute)

Tillåta

Listan över användare och/eller användargrupper som får lov att gå in på en särskild URL.

Tillgängliga användare/grupper

Listan över användare och grupper som definierats i WinRoute.



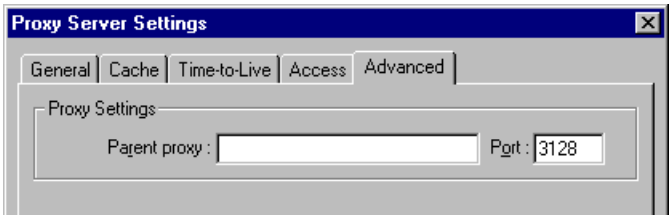
Om en användare försöker få tllgång till en webbsida som faller under kategorin begränsade sidor, kommer användaren att uppmanas till bestyrkande av sin webbläsare. WinRoute kommer att kontrollera om användarnamn och lösenord är korrekta och om användaren tillåts få tillgång till denna särskilda webbsida.

Webbläsaren lagrar användarnamnet och lösenordet i sitt minne. Alla följande förfrågningar om bestyrkande besvarars automatiskt så att användaren inte behöver mata in namn och lösenord om igen.

Å andra sidan bör användaren vara väl medveten om denna egenskap. Om du någon gång under din webbsession matat in ditt användarnamn och lösenord bör du avsluta webbläsaren när du går ifrån datorn för att att på så vis ta bort dina autentiseringsuppgifter från datorns minne.

Avancerade egenskaper

På tabben "Avancerat" för proxyserverns inställningar kan du instruera WinRoute att använda en överordnad proxyserver.



Ibland kan du få tillgång till en proxyserver som har ett ovanligt **stort cacheminne** eller som har en **snabb** Internetanslutning och din anslutning till denna server blir också rimligt snabb kanske med användning av en extra länk förutom den du använder för din egen Internetanslutning.

För att förbättra genomströmningen av data kan du bestämma att WinRoutes proxy ska vidarebfordra alla förfrågningar till denna överordnade proxyserver. För att göra detta mata helt enkelt in den **överordnade proxyns** namn och portnummer i fälten under tabben "**Avancerat**".

Om cacheminnet

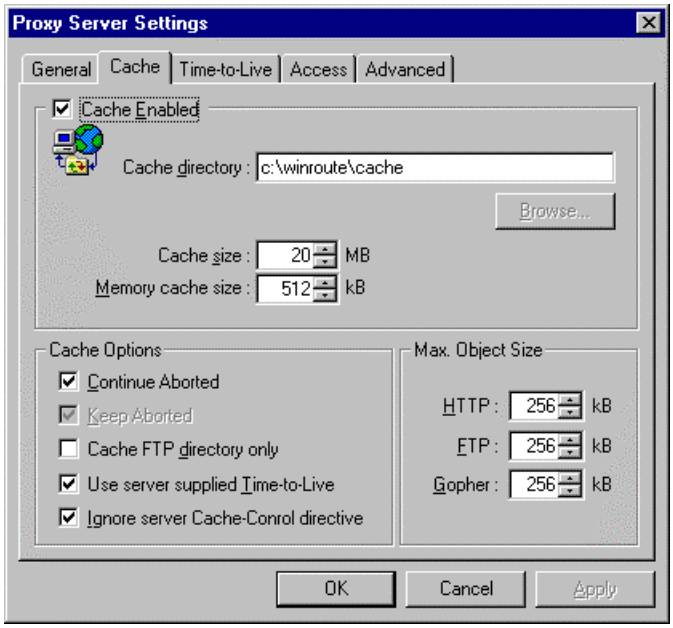
WinRoutes proxyserver har ett **mycket ekonomiskt** sätt att lagra data. Alla cacheobjekt lagras i **en fil av fast längd**. Det vanliga sättet däremot som används av många proxyservrar är att lagra varje objekt i en separat fil.

Om disken använder **stora tilldelningsenheter** (som FAT 16) resulterar denna metod i **avsevärt slöseri** med diskytrymme eftersom en mängd komponeneter för webbsidor är mycket små. Vanligtvis är 50% av objekten mindre än 6 kilobyte medan tilldelningsenheternas storlek på en stor disk är 32 KB (med filsystemt FAT).

Det faktum att WinRoute Cache lagrar data i en enda fil och att ha alla cachelagrade objekt i en fil sparar en mängd utrymme på disken - så mycket som 10 gånger mindre utrymme krävs jämfört med den gängse metoden. Detta innebär att du behöver mindre diskutrymme eller att du kan använda samma utrymme på ett mer effektivt sätt.

Den enda filen av fast längd tillåter också att WinRoute använder mycket effektiva indexeringstekniker som gör cacheminnet i WinRoute mycket snabbt.

Cache-inställningar



Cacheminne aktiverat

Kopplar på och av cacheminnet. Om det inte är aktiverat hämtas alla webbsidor alltid direkt från Internet.

Cachekatalog

Den katalog i vilken cacheminnet lagras.

Cachestorlek

Den mängd diskutrymme som kommer att användas av proxyns cacheminne. När du bestämmer dig för storlek tänk på hur många användare du har, den trafik de genererar etc. Om du har tillräckligt med ledigt utrymme kan du ställa in ett större cacheminne. Maximal storlek är 3072 megabyte (3 GB).

Fortsätt avbruten

Om den markeras kommer proxyservern alltid att avsluta nedladdningen av ett objekt från Internet även om användarens webbläsare avbryter denna begäran (användaren trycker på stoppknappen eller följer en länk till en annan sida utan att vänta på att den aktuella sidan ska laddas ner fullständigt). Följande besök på samma sida går på så vis mycket snabbare.

Håll kvar avbruten

Detta instruerar WinRoutes proxyserver att cachelagra även ofullständiga objekt (webbsidor, bilder). Detta ger åtminstone delvis en snabbar tillgång när webbsidan besöks igen. Om "Fortsätt avbruten" är markerad ignoreras inställningen "Håll kvar avbruten".

Endast cacheminnets FTP-katalog

När du surfar mellan FTPservrar, använd detta alternativ för att endast cachelagra katalogens listor. Om du dessutom önskar cachelagra de filer som laddats ner från en FTP-server, koppla bort dett alternativ. Beslutet huruvida en särskild fil ska cachas beror också på dess storlek , se "Max. objektsstorlek" nedan.

Använd servertilldelad livstid

Livstid är den tidsperiod efter vilken en särskild webbsida anses vara omodern och dess innehåll åter måste hämtas från servern. Detta alternativ instruerar WinRoutes proxyserver att rätta sig efter en Time-to-Live (TTL) som följer med de individuella sidorna. Om en sida inte har någon TTL används proxyns standard-TTL.

Ignorera serverns direktiv om kontroll av cacheminne

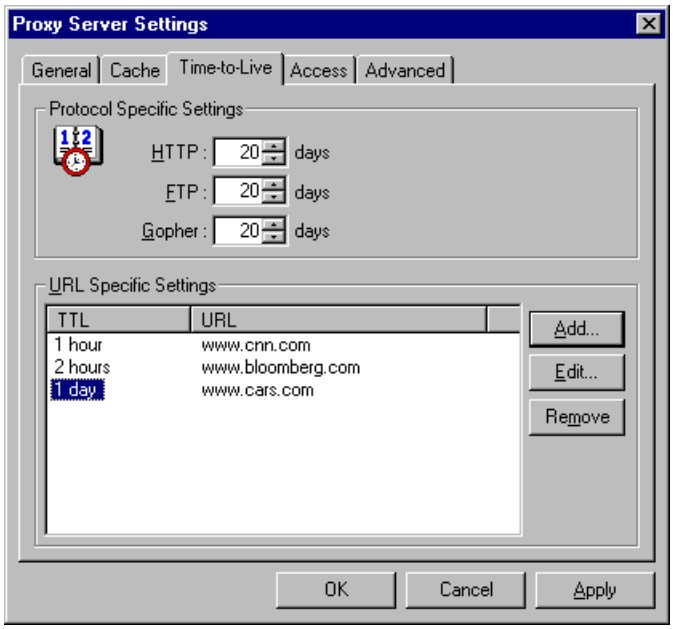
Om innehållet på en webbsida ändras väldigt ofta kan sidans författare besluta att ställa in ett direktiv om "no-cache" för den. Detta är en mycket användbar egenskap men vissa webbplatser använder direktivet alldeles för ofta, ibland för samtliga sina sidor, och eliminerar på så vis syftet med proxyservrar. Om du behöver skydda dig mot sådant uppträdande ska du aktivera detta alternativ.

Max. objektsstorlek

Den maximala storleken av objekt som kan lagras i cacheminnet. Större objekt kommer att skickas till användarens webbläsare men inte att registreras i cacheminnet. Vanligen har du inget behov av att cacha stora objekt (som programarkivfiler) eftersom du inte laddar ner dem upprepade gånger.

Livslängd

Du kan definiera de standardvärden för Time-to-Live (TTL) som används om en webbsida inte har någon definierad TTL för sig eller om du beslutar att ignorera de TTL-värden som servern ger (se alternativet "Använd serverlevererad Time-to-Live" på cachetabben).



Protokollspecifika inställningar

Här kan du ställa in standardtiden för Time-to-Live i dagar för HTTP-, FTP- och gopherprotokollen.

URL-specifika inställningar

Om du behöver ställa in individuella tider för Time-to-Live för vissa domäner, webbservrar eller individuellea sidor, skriv in värdena för individuella URL här. Du kan ställa in TTL i dagar och/eller timmar.

Du kan använda en asterisk som ersättningstecken (wild card) i en URL. Som ny egenskap i WinRoute 4.0 används också en test av substrings för att matcha URL, så du kan bara skriva in "ftp" för att matcha alla servrar som har "ftp" i sina namn. Tidigare var du tvungen att skria in "*ftp*" för att täcka detta fall).

Lägg märke till att om du har aktiverat "Använd serverlevererad Time-to-Live" på cachetabben, så har denna serverlevererade TTL högre priortet än "URL-specifika inställningar".

Hur kan man tvinga användare att använda proxy i stället för NAT?

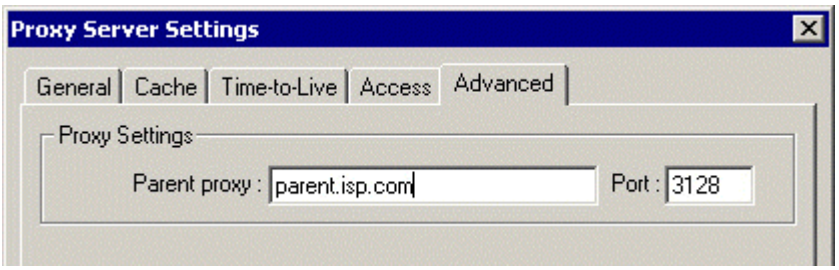
Även om **NAT** ger dig utmärkt anslutningskapacitet till Internet kan du ibland finna det användbart att använda **proxyservrarna** för att få tillgång till **World Wide Web**. Vanligtvis inträffar detta när du har 56K tillgång för hela företaget och cacheminnet blir väldigt användbart eller när du vill **kontrollera användarnas tillgång** genom ett inbyggt **URL-filter**.

För att använda en proxy för att få tillgång till WWW, måste du ställa in alla webbläsarna så att de använder proxyservern. Tänk på att proxyserverns standardport när det gäller WinRoutes proxy är **3128**. Om nödvändigt kan du ändra denna port. Användarna kommer att kunna gå förbi proxyn och gå direkt till Internet genom NAT. För att undvika detta behöver du sätta upp brandväggen. Se exemplet i kapitlet ***Brandväggsinställningar*** (see "Att tvinga användare att använda proxyserver" on page 123).

Att använda en överordnad proxyserver

Överordnad proxyserver

I en del fall kommer du att ha behov av att WinRoutes proxyserver ansluter till en proxyserver av "högre rankning" , den så kallade **överordnade proxyn**. Gå till menyn *Inställningar / Proxyserver*, välj tabben *Avancerat* och mata här in den överordnande proxyserverns IP-adress och port.



Överordnad proxys användarnamn och lösenord

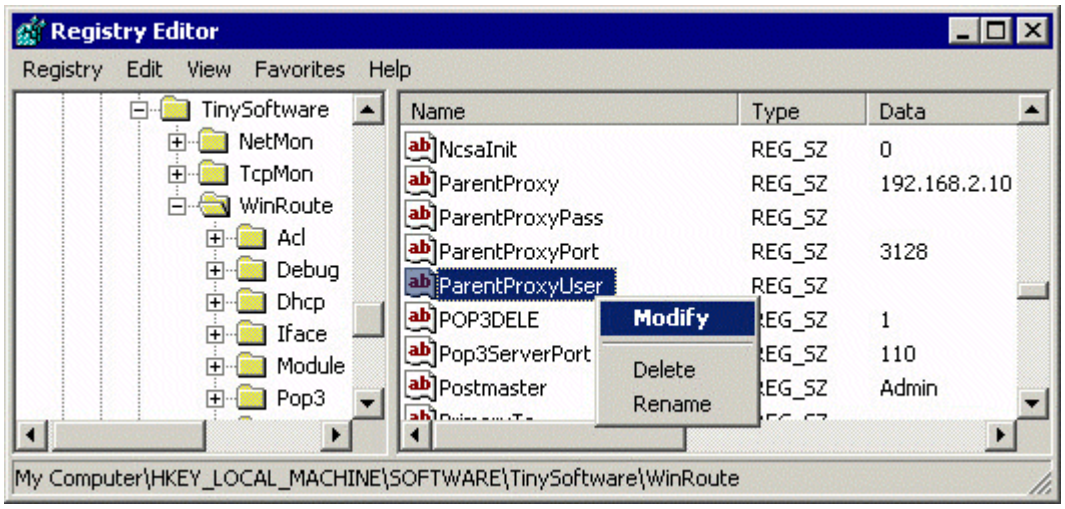
Den överordnade proxyn kan kräva att användaren autentiserar sig för att få tillgång till vissa (eller alla) webbplatser på liknande sätt som WinRoute gör (för detaljer se kapitlet *Kontroll av proxytillgång*). WinRoute Pro 4.1 inkluderar sådan autentisering från version 22.

Att sätta upp autentisering:

- Stoppa WinRoute-motorn (från Windows Tjänster eller med användning av WinRoute-motorns bildskärmsprogram)
- Starta Windows registreringsredigerare (regedit.exe)
- Leta upp nyckeln *HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute*
- Leta i det högra fältet upp enheterna **Överordnad proxyanvändare** och **Överordnat proxypass** och ändra deras innehåll till lämpligt användarnamn och lösenord.

- Stäng registreringsredigeraren och starta WinRoute-motorn.

Efter denna procedur kommer WinRoutes proxyserver att autentisera sig själv vid den överordnade proxyservern.



E-postserver

I denna avdelning

Om WRs e-poststerver

WinRoute inkluderar en fullfjädrad SMTP/POP3 e-postserver. Du kan använda den på samma som du skulle använda e-postservern på din ISP. WinRoutes e-postserver ger dig förmågan att skicka e-post ut till Internet och till lokala användare inom ditt LAN. Den gör också att du kan ta emot e-post och lagra den i WinRoute-användarnas postlådor. WinRoute innehåller också en schemaläggare med vilken du kan schemalägga din utväxling av e-post.

Om du inte använder e-postservern

Det är inte nödvändigt att använda WinRoutes e-postserver. Du kan fortsätta att använda e-postservern på din ISP eller en från tredje part. I vilket fall som helst kommer WinRoute att agera som den router/brandvägg som kommer att få mjukvaran på din e-postklient att kommunicera med e-postservern på din ISP.

- ***Obs! Ställ inte inte in mjukvaran på din e-postklient till att använda proxyn! Du måste använda WinRoutes NAT för tillgång till Internet och ställa in din klientmjukvara på att ha direkt tillgång till Internet. Om du inte lyckas upprätta utbyte av e-post betyder det att NAT inte är ordentligt konfigurerat. Se uppföljningens*** Checklista ***för att konfigurera den ordentligt.***

Användarkonton

I denna avdelning

Om användarkonton

WinRoute - Användarkonton

WinRoute kan programmeras med individuella användarkonton vilka kan grupperas (konfigurerade under tabben Inställningar| Konton… | Användare). Existerande Windows NT/2000-användare kan importeras via tabben Avancerat under menyn Inställningar| Konton… .

Vad är en användare?

Som användare av WinRoute kan du delta i WinRoute-administrationen, ha en postlåda och delta i utformandet av politiken för restriktioner i tillgången till WinRoutes proxy.

Användare kan skapa grupper och applicera ovannämnda privilegier och begränsningar på dem.

Att lägga till en användare

Att lägga till en användare:

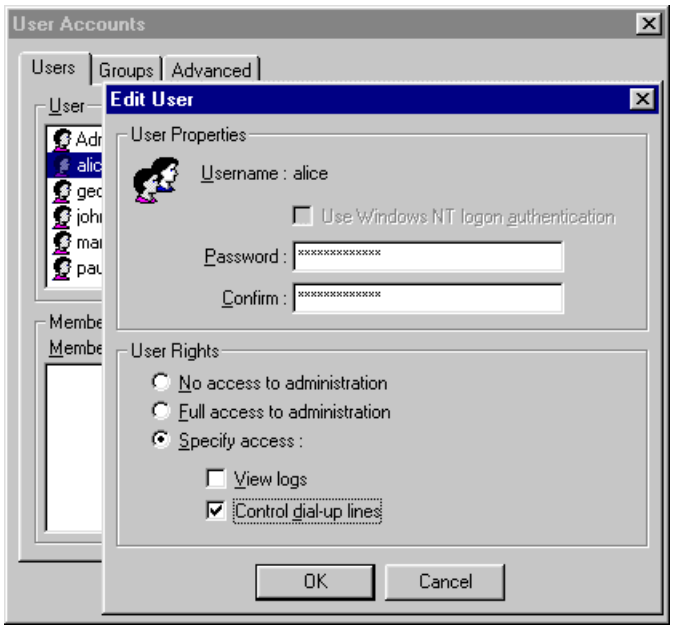
1. Gå till menyn **Inställningar->Konton**
2. Tryck på **Lägg till**-knappen
3. Definiera **användarnamn** och **lösenord**
4. Tilldela användaren **rättigheter**:

   Användaren har ingen rättighet att administrera WinRoute.

   Användaren har full tillgång till administrationen

   - **Visa loggar:** Användaren har rättighet att logga in i WinRoute-administratören och att kunna se loggfönstren enbart (felsökningsinformation, proxylogg, e-postlogg etc.). Användaren har inte vidare tillgång till att ändra de andra inställningarna.

- **Kontroll uppringningslinjer:** Användaren har rättighet att logga in i WinRoute-administratören och att etablera – avbryta anslutningen till Internet. Användaren har inte vidare tillgång till att ändra de andra inställningarna



Användargrupper

I WinRoute kan du gruppera användarna i olika grupper. En kan samtidigt vara medlem i flera grupper.

Du kan tilldela gruppen **rättigheter**.

- ***Obs: de rättigheter som tilldelas en grupp "har företräde framför" de rättigheter som tilldelas en användare.***

Gruppmedlemmar kan ha följande **rättigheter**:

Användaren har ingen rätt att administrera WinRoute.

Användaren har full tillgång till administrationen

- **Visa loggar:** Användaren har rättighet att logga in i WinRoute-administratören och att kunna se loggfönstren enbart (felsökningsinformation, proxylogg, e-postlogg etc.). Användaren har inte vidare tillgång till att ändra de andra inställningarna.
- **Kontroll uppringningslinjer:** Användaren har rättighet att logga in i WinRoute-administratören och att etablera – avbryta anslutningen till Internet. Användaren har inte vidare tillgång till att ändra de andra inställningarna

Fjärradministration

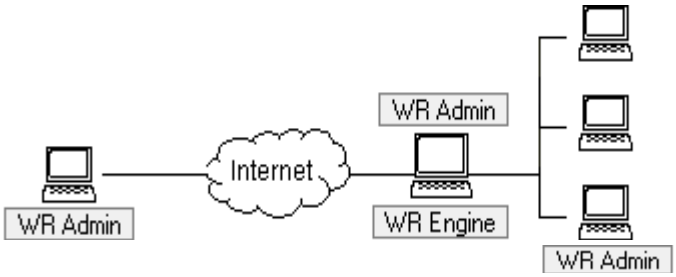
WinRoute Pro förser användarna med fördelen av fjärradministration. Med rätt inställningar och rättigheter på plats är det möjligt att på säkert sätt administrera din brandvägg från vilken plats som helst i världen. Tillgången till motorn är säkrad av starka krypteringar och lösenord.

Komponenter i WinRoute Pro

WinRoute Pro 4.x består av tre moduler:

WinRoute-motorn utför alla routing- och analysåtgärder (NAT, paketfiltrering, portmappning etc.). Du kan starta/stoppa WinRoute-motorn från WinRoute-motorns bildskärm eller om den kör Windows NT, direkt från NT alternativtjänster. WinRoute-motorn körs osynlig som en tjänst under Windows2000/NT/98 eller 95.

WinRoute-motorns bildskärm är den bildskärmsapplikation som visar huruvida WinRoute-motorn körs eller inte. Den visas som en liten blå ikon i nedre högra hörnet på ditt skrivbord.



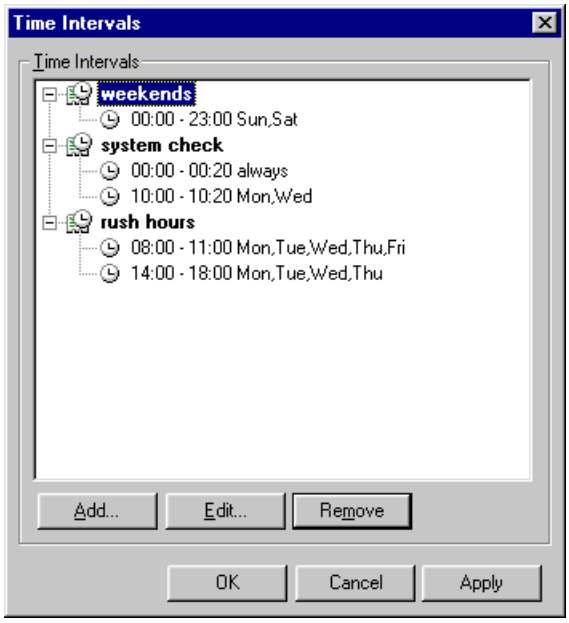
WinRoute-administratören ger konfiguration och inställningar för WinRoute-motorn. WinRoute-administratören är en separat applikation (wradmin.exe) som kan köras på vilken dator som helst och via en TCP/IP-anslutning stå i förbindelse med en dator med WinRoute-motor. För inställningar som är nödvändiga på WinRoute-motorn för att möjliggöra fjäranslutning se de andra kapitlen i denna avdelning.

Tidsintervall

Du kan definiera Tidszoner – fördefinierade tidsintervall – för att utföra vissa åtgärder. Dessa åtgärder kan vara:

- Paketfiltrering
- E-postutbyte (skicka och ta emot)
- Anslutning till Internet
- Avancerade NAT-inställningar

Tidszon är en grupp av tidsintervall. Som resultat härav kan du skapa icke-homogena tidsutrymmem bestående av flera tidsintervall.



- ***Exempel: du kan skapa en tidszon som kallas "Helgdagar och kvällar" som kommer att täcka: lördagar, söndagar, måndagar från 4 f.m. till 6 e.m., tisdagar från 5 e.m. till 7 e.m.***

För att definiera tidszon:

1. Gå till menyn *Inställningar=>Avancerat=>Tidsintervall*
2. Förse tidszonen med namn
3. Lägg till det nya tidsintervallet

KAPITEL 2

ATT FÅ DET ATT FUNGERA

I detta kapitel

Systemkrav

För att installera och köra WinRoute Pro 4.1rekommenderar vi minst:

- Pentium PC (enkel eller dubbel processor)
- Windows 95/98/NT4.0/2000 OS
- 32MB minne
- 1MB ledigt diskutrymme
- Minst 2 gränssnitt tillgängliga. Dessa kan vara: Ethernet, RAS, TokenRing, DirecPC

Snabb checklista

För alla WinRoute-användare finns det en grundläggande lista över inställningar och regler som om de tillämpas säkerställer en framgångsrik anslutning av deras nätverk till Internet. Naturligtvis är en fungerande Internetanslutning ett måste.

Du ska utföra de inställningar som beskrivs nedan om du vill dra nytta av att kunna använda NAT för delad tillgång till Internet. Om du vill använda en proxyserver (inbyggd WinRoute) behöver du inte göra dessa inställningar. I det fallet skulle du behöva rikta dina webbläsare och applikationer mot WinRoutes proxyserver. Vi rekommenderar starkt användning av NAT (Network Address Translation) var än det är möjligt. Det är snabbare, säkrare och mer pålitligt.

Inställningar och regler

1 **På WinRoute-datorn - två gränssnitt(NIC)**
Kontrollera att WinRoute-datorn har (minst) två gränssnitt. Ett för Internetanslutning och ett för lokal /klient-anslutning. Det kan vara nätverksadapter eller RAS-linjer. Ett gränssnitt (Ethernet eller RAS/uppringning) används för Internetanslutning medan det/de andra gränsnittet, -en (Ethernet, symbolprotokoll…) används för anslutning till dina egna nätverk.

2 **Säkerställ att alla IP-adresser är pingbara!** För att WinRoute ska arbeta på rätt sätt, måste klientmaskinerna kunna pinga både de allmänna och privata IP-adresserna till WinRoutes värdmaskin.

3 **På WinRoute-datorn - Aktivera NAT på Internetgränssnittet!**
Säkerställ att NAT har markerats PÅ för gränssnittslänkningen till Internet (Ethernet, RAS-linje). Ställ in detta i menyn **Inställningar=>Gränssnittstabell** och gå till egenskaperna för önskat gränssnitt.

4 **På WinRoute-datorn - Avaktivera NAT på internt gränssnitt!**
Säkerställ att NAT är **AVMARKERAT** på det eller de gränssnitt som länkar till det interna nätverket.
Obs! I väldigt speciella inställningar kan NAT markeras "På" även på det interna gränssnittet. Du ska få se detta exempel här (när det finns tillgängligt).

5 På WinRoute-datorn - Ingen gateway på internt gränssnitt!
Kontrollera att det INTE finns någon standardgateway i nätverksegenskaperna hos det gränssnitt (nätverkskort) som länkar till det interna nätverket. Naturligtvis kommer standardgateway på det gränssnitt som länkar till Internet att ställas in i enlighet med detaljer från din ISP.

6 På WinRoute-datorn - mata in alternativ vid DHCP-konfiguration!
I de flesta fall kommer du att använda WinRoutes DHCP-server för automatiserad nätverkskonfiguration. Dubbelkolla att du har definierat omfånget (omfången) för de IP-adresser som du vill att DHCP-server ska tilldela samtidigt med alternativen. I Alternativ anger du annan information som dina arbetsstationer har fått - som DNS-server, standardgateway etc.

7 På klientdatorn - WinRoute-datorns interna IP-adresser är standardgateway!
WinRoute-datorn agerar som STANDARDGATEWAY för alla datorer i LAN. Använd därför IP-adressen till det interna nätverksgränssnittet på WinRoutes värddator (dvs.192.168.1.1) som gateway på alla interna klientdatorer. Ställ in detta värde på varje "klientdator" ELLER ställ in värdet en gång på WinRoutes DHCP-server och den kommer automatisk att tilldela dina arbetsstationer detta värde!
Se Avancerat (Inter)netarbete Exempel om du behöver använda en annan standardgateway!

8 På kliendatorn - Kontrollera DNS!
I de flesta fall kommer du att anända WinRoutes inbyggda DNS-befordrare som en DNS-server för dina nätverksdatorer. Försäkra dig om att WinRoutes inbyggda DNS-befordrare är PÅ och konfigurerad. Du kan använda DNS-serverns adress på din ISP genom att direkt mata in den i tillämpliga fält i TCP/IP-konfigurationen på varje nätverksdator.

- ***I de falll där WinRoute enbart används som brandvägg eller e-postserver (dvs. utan förfrågan om delat Internet), är det INTE nödvändigt att sätta NAT "PÅ" för något gränssnitt.***

- ***Gränssnitten på WinRoute-datorn måste ha andra IP-adresser från ett annat nätverk. Det är inte möjligt att tilldela gränssnitten en IP-adress från samma nätverk (dvs. 207.181.216.23 på en och 207.181.216.24 på den andra). Det mest troliga är att du kommer att ha ett lokalt (LAN) gränssnitt och ett Internetgränssnitt. Där kommer du inte att få några problem. I det fall du skulle ha tre gränssnitt (2 lokala och ett för Internet)***

bör du tilldela lokala gränssnitt IP-adresser från olika nätverk (en 192.168.1.1 och den andra 192.168.2.1).

Mjukvara i konflikt

Det finns flera kända problem beträffande inkompatibel mjukvara:

Norton Antivirus

Avaktivera port 110 i konfigurationen för Norton Antivirus om du skulle köra WinRoute Mail Server. Att ha kvar port 110 i Norton gör att datorn inte kommer att starta.

WinGate

Avinstallera WinGate före installation. Avinstallera mjukvara både på server och klient.

SyGate

Avinstallera SyGate före installation. Avinstallera mjukvara både på server och klient.

MS Proxy Server

Avinstallera MS Proxy Server före installation. Avinstallera mjukvara både på server och klient. Ta bort TCP/IP, starta om och ta tillbaka det .

Microsoft Internet Connection Sharing

Avinstallera MS ICS före installation, ta bort TCP/IP-protokoll, starta om och ta tillbaka dem.

WinProxy från Ositis

Avinstallera WinProxy före installation, ta bort TCP/IP-protokoll, starta om och ta tillbaka TCP/IP.

All den mjukvara som nämns ovan använder drivruter som arbetar felaktigt med de lägre delarna av det nätverksprotokoll som körs av WinRoute.

Problem med routingtabell

Det kan vara möjligt att du skulle vilja ha samtliga komponenter installerade och konfigurerade framgångsrikt och att du ändå skulle kunna känna av disfunktionalitet. Olyckligtvis är Windows 95/98/NT operativsystem inte så perfekt utformat för networking. Till och med efter det att WinRoute och nätverksinställningar har ställts in korrekt kan du få erfara att installationen inte är funktionell. Om så är fallet måste du titta i Routingtabellen och välja ett av följande:

- rätta till routerna genom att ta bort dem och sen lägga till dem - endast för erfarna användare

eller

- ta bort TCP/IP-protokoll fullständigt, starta om datorn och lägg tillbaka det. Prestanda garanteras.

Problem med mjukvara för Proxy Client

En del proxyservrar kräver att mjukvara ska installeras på alla klientmaskiner. Denna klientmjukvara gör att alla applikationer efterfrågar en proxyserver. Om klientens proxymjukvara inte tas bort kan den maskinen inte anslutas till Internet eftersom WinRoute inte är installerad som proxyserver. Om klienten ändå inte kan ansluta till Internet, installera på nytt TCP/IP med dess inställningar och starta om.

Problem med drivrutiner för Network Card

Försök att använda det vanligaste gränssnittskortet för nätverk. Om du har ett speciellt, ett gammalt eller ett splitter nytt kort i din dator, kan dess drivrutin innehålla särskilda instruktioner som kommer att hindra WinRoute från att kommunicera med det. Försök att hitta det vanligaste Ethernetkortet i ditt nätverk och låt dem helt enkelt skifta position. En hel del ursprungligen "olyckliga" kunder blev "lyckliga " kunder enbart genom att byta ut kortet eller uppdatera drivrutinen.

WinRoute är en fullständigt neutral mjukvara för router/brandvägg som inte kräver att någon klientmjukvara körs på klientdatorer såvida inte fjärradministration används i vilket fall en klient eller extern maskin måste installera WinRoute Administration "wradmin.exe".

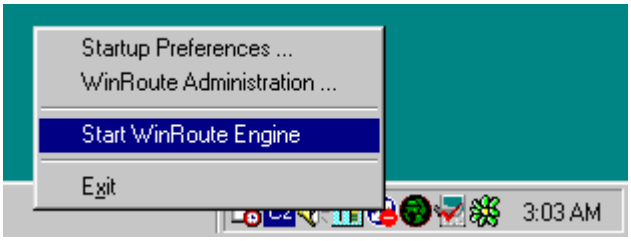
Administration i WinRoute

I denna avdelning

Administration från lokalt nätverk

För att administrera WinRoute från det lokala nätverket eller från den dator som kör WinRoute måste du göra följande:

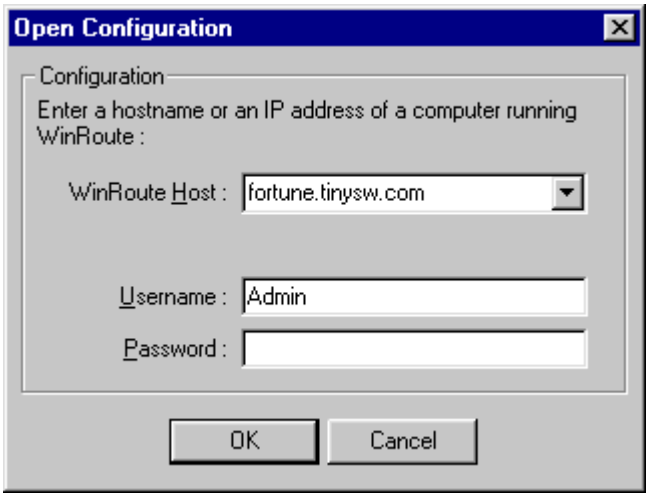
1. **Kontrollera att WinRoute-motorn är installerad och igång**
   För att kontrollera att WinRoute har startats, kör WinRoute-motorns bildskärm från WinRoute 4.0 programgrupp. En liten, rund, blå och vit ikon kommer att dyka upp i systembrickan på uppgiftsraden (nedre högra hörnet på skrivbordet). Detta indikerar att applikationen körs. Ett rött kors över ikonen anger att WinRoute har stoppats. För att starta WinRoute-motorn **högerklicka** helt enkelt på ikonen och välj Starta WinRoute-motorn från den meny som poppade upp.



2. Starta WinRoute-administratören

För att starta modulen för Win Route-administration, starta applikationen från menyn Starta=>Program=>WinRoute 4.0 eller genom att högerklicka på ikonen för WinRoute-motorns bildskärm och välja *WinRoute Administration* från popupmenyn. Du kan också kopiera filen *WRAdmin.exe* till vilken annan dator som helst i ditt nätverk och köra den därifrån.

När Admin-fönstret poppar upp lämna antingen den förinställda lokala värddatorn eller mata in IP-adressen för den dator där WinRoute körs. Mata in användarnamn och det lösenord som används för administration.



Obs: Om du ansluter för första gången kan du använda "Admin" som användarnamn och lämna lösenordet tomt. Se Användarkonfiguration för ytterligare detaljer angående administartionspolicy för användarnamn och lösenord.

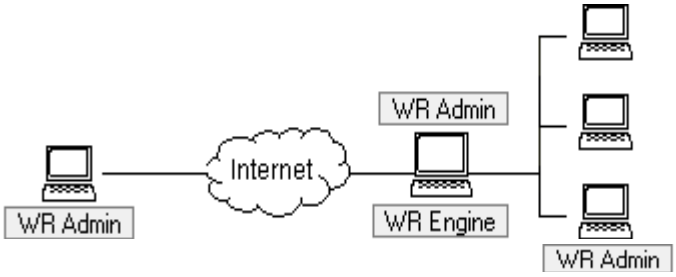
Du måste framgångsrikt logga in som administratör av WinRoute-motorn för att kunna göra inställningar.

Möjliga orsaker till att man inte lyckas logga in från ett lokalt nätverk:

- WinRoute-motorn är inte installerad och igång
- Fel användarnamn och lösenord
- Fel IP-adress har matats in vid anslutning till WinRoutes motor
- Du har inte rättighet att administrera WinRoute
- NAT är påpkopplat på gränssnittslänkningen till ditt nätverk – se kapitlet Checklista och installation av nätverk i denna hjälp

Administration från Internet

Du kan administrera WinRoute Pro-motorn från vilken dator som helst i världen så länge som det finns en TCP/IP-anslutning på plats. Administrationen är säker (krypterad) och kontrolleras via användarnamn och lösenord.



För att administrera WinRoute-datorn från utsidan av LAN (från Internet) måste portmappningen ställas in på WinRoute-datorn. Du måste förstå att med NAT kopplad PÅ vid gränsnittslänkningen till Internet (nödvändigt för delat Internet) är hela ditt nätverk inklusive WinRoute-datorn fullständigt skyddat och därför har inte någon person tillgång till det.

För att ställa in portmappning för fjärradministration gå till menyn *Inställningar=>Avancerat=>Portmappnin*g, tryck på Lägg till och ställ in:

Protokoll: TCP/UDP

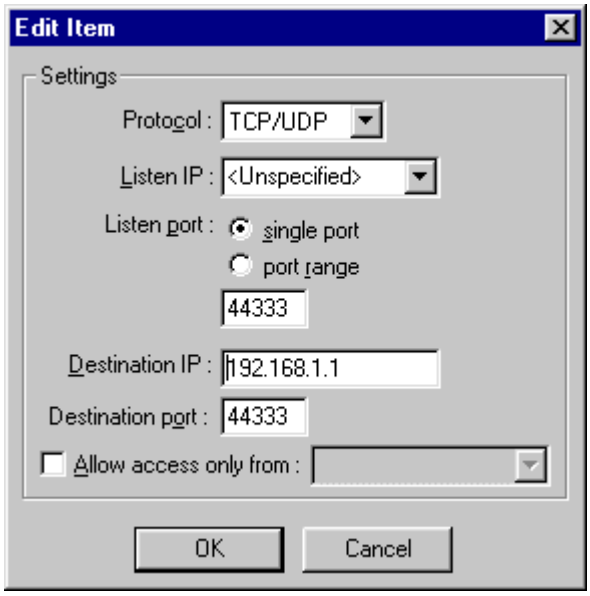
Avlyssnings-IP: <ospecificerat> (rekommenderas) eller IP-adressen för gränssnittet.

Avlyssningsport: 44333

Destinations- IP: IP-adressen för det gränssnitt som länkar WinRoute-datorn till det lokala nätverket (privatklass IP-address)

Destinationsport: 44333

Ge tillgång endast från: Om detta är markerat kan du ytterligare begränsa tillgången till WinRoute-maskinen. Du måste fördefiniera IP-adresser som tillåts få tillgång till WinRoute-motorn från Internet i menyn *Inställningar=>Avancerat=>Adressgrupper*. Du kan gruppera samman separata IP-adresser, följder av IP-adresser och nätverk.



Se exempel för fler detaljer om portmappning. Om du har stält in allting så det stämmer kör bara WinRoutes administrationsprogram fråm någon dator och mata in IP-adressen (registrerad - dvs. 206.86.181.25) för den dator som kör WinRoute och även det användarnamn och lösenord som används för administration på den datorn. Se Användarkonfiguration för ytterligare detaljer angående policy för användarnamn och lösenord vid administration.

Möjliga anledningar till att du inte lyckas logga in från Internet:

- WinRoute-motorn är inte installerad och igång
- Fel användarnamn och lösenord
- Fel IP-adress har matats in vid anslutning till WinRoute-motorn
- Du har inte rättighet att administrera WinRoute
- Ingen eller felaktig portmappning är inställd på en dator som kör WinRoute-motorn

Förlorat administrationslösenord

Om du skulle bli av med lösenordet för administrationen skicka ett e-postbrev till support@tinysoftware.com för ytterligare instruktioner. Av säkerhetsskäl publicerar vi inte lösningen på detta.

Att sätta upp nätverk

I denna avdelning

Om DHCP

Om du använder DHCP-servern kan du avsevärt förenkla konfigurationen av arbetsstationerna inom ditt LAN. När du använder DHCP-servern är den enda inställning du behöver göra på klientarbetsstationerna att ställa in dem så de dynamiskt får en IP-address från DHCP-servern. (Denna inställning kommer som standard när du lägger till TCP/IP-protokollet i nätverksegenskaper)

- ***Du kan antingen använda WinRoutes inbyggda DHCP-server eller någon DHCP-server från tredje part inom ditt nätverk. Försäkra dig om att endast en DHCP-server åt gången körs på ditt nätverk!***

Standardgateway, översikt

WinRoute agerar som en router. Som sådan kräver den två grundläggande TCP/IP-inställningar på varje dator i ditt nätverk:

- Tilldela IP-adress – antingen manuellt eller från DHCP-server (dvs. WinRoutes DHCP-server)
- Ställ in standardgateway

- **En standardgateway** på varje dator som har tillgång till Internet genom WinRoute-datorn måste ställas in på **IP-adressen** för Ethernetgränssnittet på WinRoute-datorns gränssnitt som länkar till LAN.

Exempel:

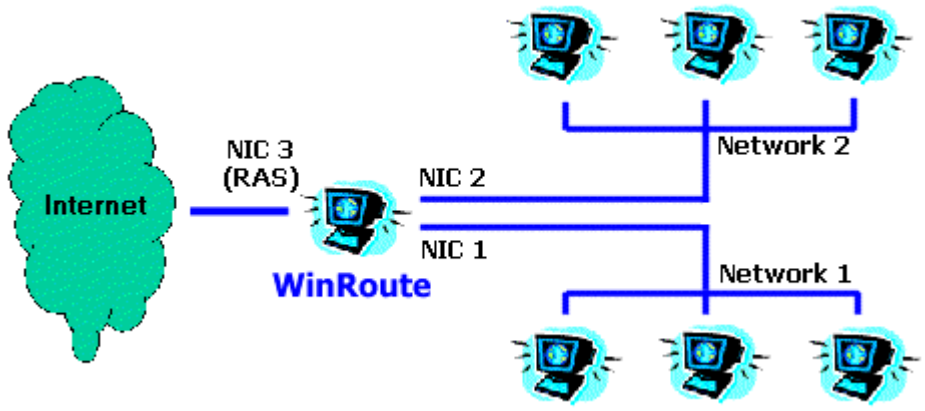
Klientdatorn har IP-adressen 10.10.10.23 medan WinRoute-datorn har två gränssnitt, ett som länkarr till kabelmodemet med en IP från ISP (som 203.23.14.232) och en annan som länkar till det privata nätverket (10.10.10.1). Standardgatewayen på 10.10.10.23 kommer att ställas in på 10.10.10.1.

- ***Obs 1: När du skapar utrymme för en IP-adress inom ditt lokala nätverk måste du använda IP-adressen från samma undernät. Dvs. om den undernätsmask du använder är 255.255.255.0 så måste alla adresser ligga mellan 10.10.10.1 och 10.10.10.255.***
- ***Obs 2: Du kan ha flera nätverk anslutna till Internet genom WinRoute. Du kan ha flera gränssnitt i WinRoute-datorn, ett för varje nätverk. Då representerar vart och ett av dessa gränssnitt (deras IP-adress) standardgatewayen för det övriga nätverk som är anslutet till den.***

Att välja rätt WinRoute-dator

WinRoute **MÅSTE ALLTID** köras på den dator som är ansluten till Internet - genom nätverkskort, kabel, DSL-modem, uppringningslänk eller en router.

WinRoute agerar alltid som gateway mellan två (eller flera) nätverk där varje nätverk representeras av ett gränssnitt. Dessa gränssnitt kan var Ethernet-kort, RAS-adapters, adapters för USB-till-Ethernet, PPPoE-adapters etc.



IP-konfiguration med DHCP-server

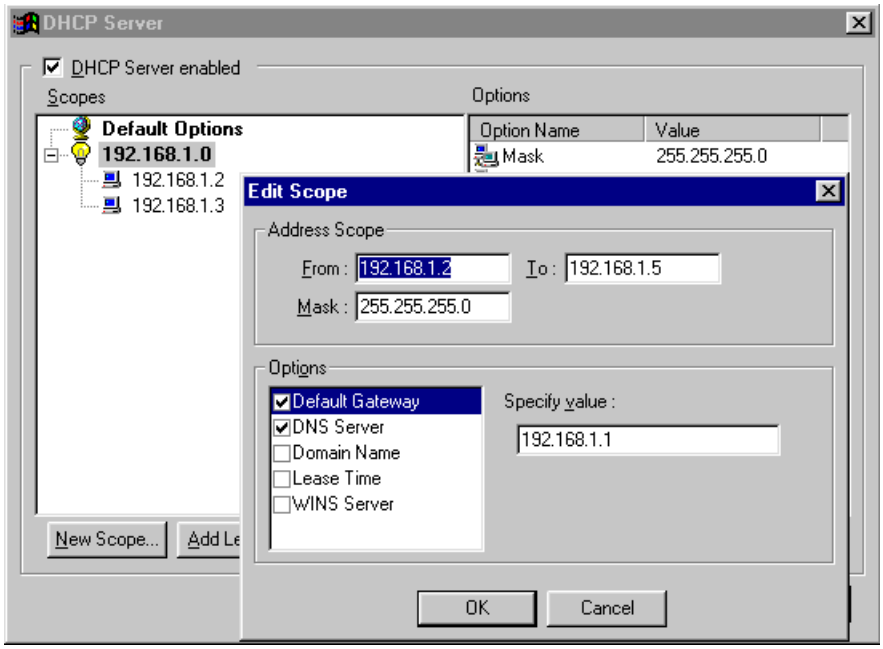
Dubbelkontrollera att dina arbetsstationer har ställts in för att få en IP-adress från DHCP-servern (se *TCP/IP->nätverksgränssnitt-egenskaper* på varje dator) och att alla övriga TCP/IP-egenskaper är omarkerade inklusive information om DNS-server.

Kör därefter programmet WinRoute Administration:

1. Gå till menyn *Inställningar=>DHCP-server*.
2. Ställ DHCP-servern på ON (markera knappen) och tryck på Lägg till **Nytt omfång**-knappen.

3. Lägg till omfång
Här ska du ange omfånget för de IP-adresser som används av DHCP-servern som ges ut till arbetsstationer. Kom ihåg att en IP-adress redan används av WinRoute-datorn så undvik att använda den. Område för IP-adresser måste vara från samma undernät. Se bild för exempel.

4. Specificera alternativ (viktigt!)
I Alternativ kan du ange vilken övrig information som ska ges till arbetsstationer (dvs. standardgateway, DNS-server etc.). Markera knappen bredvid varje komponent i dialogboxen och mata in lämplig information. Mata in information om standardgateway och DNS-server (normalt skulle du använda WinRoute som DNS-server) och använd IP-adressen för WinRoute-datorn (e.g. 192.168.1.1). Övriga alternativ kan du lämna omarkerade.


DHCP Server
DHCP Server enabled
Scopes
Options
Default Options
192.168.1.0
192.168.1.2
192.168.1.3
Option Name
Value
Mask
255.255.255.0
Edit Scope
Address Scope
From :
192.168.1.2
To :
192.168.1.5
Mask :
255.255.255.0
Options
Default Gateway
DNS Server
Domain Name
Lease Time
WINS Server
Specify value :
192.168.1.1
New Scope...
OK
Cancel

- ***Obs: IP-adressen för Ethernetgränssnittet (som länkar till LAN) på WinRoute-datorn måste tilldelas och du ska använda denna IP-adress i andra datorer som standardgateway och (valfritt) som DNS-server! Men standardgatewayen på det gränssnittet ska vara omarkerad.***

IP-konfiguration med tredje DHCP-server

Att använda en tredje DHCP-server för din nätverkskonfiguration kräver att du speciellt uppmärksammar de värden som lämnas av en sådan DHCP-server till klientarbetsstationerna inom ditt nätverk.

Dubbelkontrollera att din DHCP-server lämnar ut korrekt information till dina klientarbetsstationer! Dvs. du måste ställa in DHCP-servern så att den tilldelar andra datorer IP-adressen på WinRoute-datorns LAN-kort som standardgateway och (valfritt) DNS-server.

Även den IP-adress som lämnas ut till klientarbetstationen måste tillhöra samma undernät som WinRoute-datorn.

DUBBELKONTROLLERA (!!!) att det interna nätverkskortet på WinRoute-datorn **har tilldelats** en fast IP-adress (e.g. 192.168.1.1) och att denna adress har lämnats av DHCP som standardgateway för resten av nätverket. DHCP-servern kanske inte tilldelar IP-adress till WinRoutes värddator!

Exemepl:

NT-server med DHCP körs på 192.168.1.1 medan WinRoute körs på 192.168.1.5. Standardgatewayens (och DNS om du skulle använda WinRoute DNS) information som lämnas ut till arbetsstationer blir 192.168.1.5.

IP-konfiguration - manuell tilldelning

I en del fall är det nödvändigt att tilldela arbetsstationerna deras IP-adresser manuellt. När du gör det. tänk på följande regler :

Tilldela IP-adress

Tildela varje dator en IP-adress av "intern typ". Vanligen 192.168.x.x or 10.x.x.x. Tilldela varje system IP-adresser från samma undernät. Till exempel, när väl en IP-adress för WinRoutes värddator har ställts in på 192.168.1.1, måste du fortsätta med sama numreringsschema. (e.g.192.168.1.2., 192.168.1.3 etc.)

Ställa in standardgateway

Använd IP-adressen för WinRoutes värddator som standardgateway på alla dina klientdatorer. Med andra ord, varje klientdator kommer at använda IP-adressen för WinRoutes värddator (intern IP-adress) som standardgateway. Detta matas in i TCP/IP=>Ethernet_adapter i Nätverksegenskaper för datorn.

Ställa in DNS

Slutligen, använd WinRoute-datorernas IP-adress som DNS-befordrare för alla dina datorer (den interna IP-adressen, om du använder WinRoutes DHCP-server). Det enda undantaget kan vara när du använder DNS-adressen för din ISP eller en annan DNS-server. Då ska du mata in DNS-detaljer som du får från din ISP (i TCP/IP->NIC-egenskaper för varje arbetsstation).

Viktigt! Se rekommenderat kapitel i denna manual angående ytterligare DNS-inställningar!

Att installera DNS-befordrare

DNS-servern konfigureras med användning av menyn: *Inställningar => DNS-server*.

"Aktivera DNS-befordran"

Detta alternativ kontrollerar om DNS-servern har slagits på eller av.

"Vidarebefordra automatiskt till servern DNS-förfrågningar som valts från DNS-servrar som är kända av operativssystemet."

Om markerat vidarebefordras alla DNS-förfrågningar till den DNS-server som valts från TCP/IP-konfigurationen på Internetgränssnittet eller uppringningsnätverket.

"Aktivera lookup i VÄRD-fil"

Med detta alternativ markerat tillåts DNS-servern att använda data från VÄRDDATORNS fil när den besvarar förfrågningar.

"Redigera VÄRDDATOR-fil..."

Denna knapp startar en extern textredigerare i vilken du kan redigera VÄRDDATORNS fil.

"DNS-domän"

Mata in ditt domännamn (dvs. "acme.com") här. Vid besvarande av DNS-förfrågningar fästs domännamnet vid det värdnamn som erhållits från VÄRDATOR-filen eller från DHCP-tabellen över uthyrning.

"Vidarebefordra DNS-förfrågningar till"

Mata in den numeriska IP-adressen för den DNS-server som du vill vidarebefordra DNS-förfrågningarna till. Välj en av adresserna för dina ISP DNS-servrar eller til en server som du har snabb tillgång till.

"Aktivera DNS-cacheminne"

Detta gör att svar på DNS-förfrågningar kan lagras i internt cacheminne. Efterföljande förfrågningar behandlas sedan med användning av innehållet i cacheminnet utan att invänta svar från DNS-servern utanför ditt nätverk.

"När du upplöser namn från VÄRD-fil eller uthyrningstabell, kombinera den med DNS-domän"

Denna egenskap kan bäst förstås genom ett exempel - du kan vilja lösa en DNS-förfrågan för datorn JOHN. I VÄRD-filen har du matat in att din domän OFFICE är asocierad med en specifik IP-adress. Därefter kan JOHN.OFFICE-förfrågan upplösas korrekt.

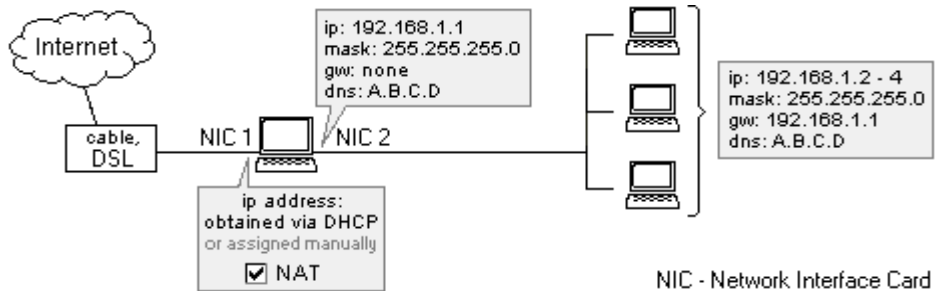
- ***Lägg märke till att cacheminnet endast lagrar svar som är av typen "Namn => IP address". Svaren lagras till tiden för dem går ut. Denna tid tillhandahålles av DNS-servrarna tillsammans med varje svar.***

Att ansluta nätverket till Internet

I denna avdelning

DSL-anslutning

DSL (ADSL, SDSL)-anslutning kräver att två kort för nätverksanslutning (NIC) har installerats i WinRoute-datorn . Ett NIC kommer att länka till Internet (DSL-modem) medan ett annat NIC lommer att länka till det interna nätverket.



WinRoute-konfiguration

För att ansluta till Internet

1. Gå till menyn Inställningar->Gränssnittstabell
2. Välj det NIC som länkar till Internet, klicka på Egenskaper och markera ON "Utför NAT med IP-adress för gränssnittet på all kommunikation som passerar". När du öppnar gränssnittstabellens dialogruta kommer du att kunna läsa NAT ON bredvid denna externa linje.
3. Kontrollera att NAT är NOT ON för det gränssnitt som länkar till det interna nätverket (gä till egenskaper för detta gränssnitt i Gränssnittstabell)
4. Kontrollera att INGEN gateway har ställts in i TCP/IP-egenskaper för det interna NIC (gå till nätverksinställningar) och att NIC har tilldelats en intern IP-adress.
5. Kontrollera att det NIC som länkar till Internet har tilldelats data från din ISP. I det fall du har dynamiskt tilldelade IP-adresser lämna inställningar för IP-adress tomt.

För andra nätverksinställningar se lämpliga kapitel , speciellt ***Checklista*** .

PPPoE DSL-anslutning

PPPoE är en nyligen utvecklad teknologi för många DSL-abonnenter. Fast den har utvecklats långt av flera ISP förser den användare med stympad prestanda och den är inte (i dagens läge) den allra bästa lösningen för att ansluta ditt nätverk till Internet. Kunder bör kräva standardlösningen DSL när helst så är möjligt.

Utvecklandet av PPPoE med WinRoute liknar standard-DSL vad gäller TCP/IP-inställningar. WinRoute Pro bör installeras på samma dator som PPPoE-adaptern. WinRoute Pro kommer att känna igen PPPoE-adaptern som ett nätverksgränsnitt. Du bör aktivera NAT på detta gränssnitt. Du kommer också att se Ethernetadaptern (kopplad till kabelmodemet) som gränssnitt i WinRoute Pro gränssnittstabell. Du bör inte aktivera NAT på det gränssnittet.

WinRoute Pro fungerar väl med alla PPPoE-adapters som finns på marknaden. Emellertid kan kunden- då och då - upplev problem med prestandan hos vissa PPPoE-adapters:

Enternet 100, 300, 500 PPPoE klient

WinRoute Pro 4.1 fungerar väl med Enternet PPPoE klienten från NTS om du har kopplat in Protokollets drivrutin i stället för standarden filterdrivrutin. För att göra det kör Enternet PPPoE-klienten, gå till menyn Inställningar->Avancerat och ändra önskade värden.

Om du skulle få känning av prestandaproblemet kan du också behöva ställa ner MTU på klientmaskinerna till 800.

WinPoet från Ivasion

WinRoute Pro 4.1 fungerar väl med WinPoet under följande omständigheter: IP huvudkompression (är nätverksinställningar för RAS/uppringning) har stängts av.

Att ställa ner MTU:

PPPoE-adaptern lägger till extra information till huvudet i varje utgående paket. Som standard använder fönster den maximalt tillåtna paketstorleken. PPPoE-adaptern kompenserar för detta genom att säkerställa att MTU på den lokala maskinen sänks något för att kompensera för den extra information som läggs till varje paket. Olyckligtsvis använder fortfarande alla andra maskiner den maximala storleken för överföring. Detta kommer att resultera i förlust av paket. Följande länkar kommer att visa hur du ska sänka MTU på alla klienter.

För användare av Windows 95/98 :

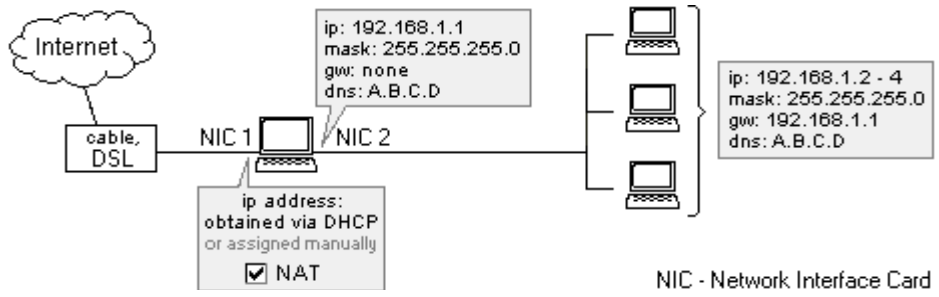
http://www.microsoft.com/support/kb/articles/Q158/4/74.asp

För användare av Windows NT4/2000 :

http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnbd/cnbd_trb_vcfx.asp

Anslutning av (tvåvägs) kabelmodem

Anslutning med kabelmodem kräver två kort för nätverksgränssnitt (NIC) inkluderade i WinRoutesdatorn. Ett NIC kommer att länka till Internet (kabelmodem) medan ett annat NIC kommer att länka till det interna nätverket. För UNI-riktade kabelmodem (modem upp, kabel ner) se lämpligt kapitel.



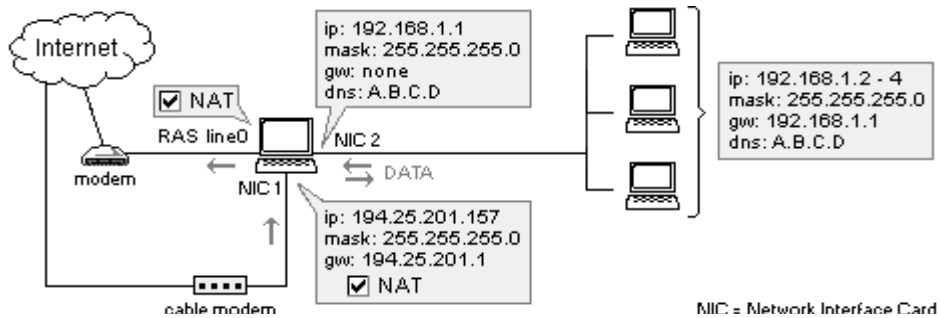
WinRoutekonfiguration

1. Gå till menyn Inställningar ->Gränssnittstabell
2. Välj NIC som ska länka till Internet, klicka på Egenskaper och markera ON "Utför NAT med IP-adress för gränssnittet på all kommunikation som passerar igenom". När du öppnar gränssnittstabellens dialogbox kan du läsa NAT ON bredvid den externa linjen.
3. Kontrollera att NAT är NOT ON för det gränssnitt som länkar till det interna nätverket (gå till egnskaperna för detta gränsnitt i Gränssnittstabellen)
4. Kontrollera att INGEN gateway har ställts in i TCP/IP-egenskaper för det interna NIC (gå till nätverksinställningar) och att NIC har tilldelats en intern IP-adress.
5. Kontrollera att det NIC som länkar till Internet har tilldelats data från din ISP. I det fall du har dynamiskt tilldelade IP-adresser lämna inställningar för IP-adress tomt. För andra nätverksinställningar se lämpliga kapitel , speciellt ***Checklista*** .

Envägs kabelmodem (modem upp, kabel ner)

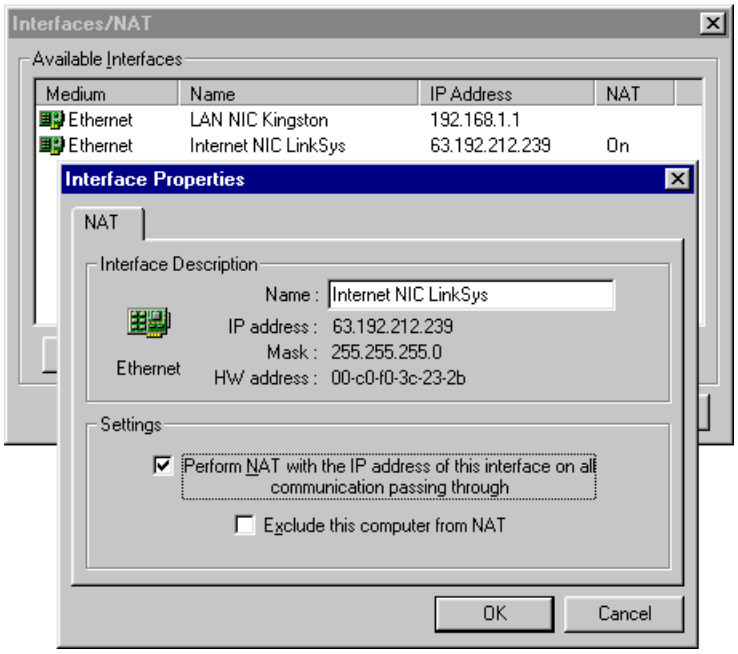
OBS: Denna typ av Internetanslutning är **inte en "officiellt understödd konfiguration"** eftersom inställningarna **kan variera** från ISP till ISP. men vi försöker ge lösningar för åtkomst vid så många scenarier som möjligt. Många av våra användare har haft framgång med följande inställningar när de försökt upprätta en anslutning.

I allmänhet är dataflödet **liknande det i Direc PC**. Utgående paket går igenom ditt gränssnitt för **uppringning**. På vägen tillbaka routas de **genom en kabel**. I verkligheten måste ditt ISP associera dina två gränssnitt tillsammans. Detta verkar knepigt men är det enda sättet att upprätta en fungerande länk. Av den anledningen råder vi dig att kontrollera med din ISP innan du går vidare med köpet av WinRoute



1. Gå till menyn *Inställningar>gränssnittstabell*. Du kommer att se gränssnittet för en **RAS-linje** (ditt modem) och två gränssitt för **nätverkskort** - ett som länkar till Internet och ett som länkar till lokalt nätverk

2. Klicka på det gränssnitt på nätverkskortet som länkar till Internet och gå till *"Egenskaper."* Markera ON för *"Utför NAT med IP-adressen för gränssnittet på all kommunikation som passerar genom."*



3. Klicka på **RAS-gränssnittet** och gå till *"Egenskaper."* Markera ON *"Utför NAT med IP-adress för gränssnittet på all kommunikation som passerar genom"*. I **RAS tab** väljer du den anslutning som du vill använda för att ansluta din ISP, mata in ditt användarnamn och lösenord.

4. Kontrollera att NAT är **INTE PÅ** för det det gränssnitt som länkar till det interna nätverket (gå till egenskaper på detta gränssnitt)

5. Kontrollera att **INGEN gateway** ställts in i TCP/IP-egenskaperna för det interna NIC (gå till nätverksinställningar) och att NIC har tilldelat en privatklass **IP-adress** (dvs.10.10.1.1).

6. Kontrollera att det NIC som länkar till Internet har tilldelats rätt data från din ISP (TCP/IP-egenskaper) Obs: I det fall du har en dynamiskt tilldelad IP-adress så lämna inställningarna för IP-adress tomma.

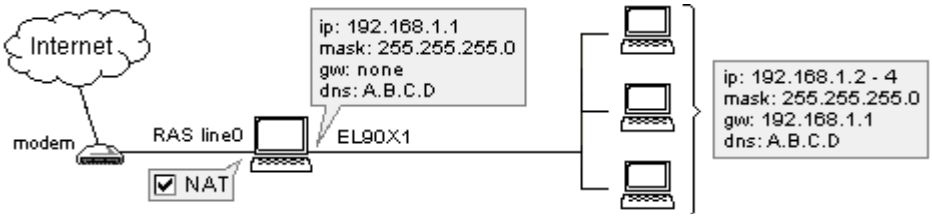
- ***I allmänhet ska NAT slås "PÅ" på båda de gränssnitt som länkar till Internet - RAS och Uppringning.***

Uppringnings- eller ISDN-anslutning

Anslutning via Uppringning eller ISDN

Om du har en uppringningstillgång till Internet (vanlig 56K eller ISDN) på en PC som kör Win95, Win98 eller NT4.0 så har du vad som behövs för att köra WinRoute. WinRoute måste köras på en dator som innefattar:

- modem förbundet med telefon eller ISDN-linje
- Kort för nätverksgränssnitt (NIC) som leder till det interna nätverket.



I det fall du har ett ISDN-modem anslutet till din dator via Ethernet-kort se kapitlet Anslutning via DSL. I det fallet kommer du att konfigurera WinRoute för att arbeta med två Ethernet-kort.

Före anslutningen

Innan du ansluter till Internet, dubbelkontrollera följande:

- · TCP/IP-protokollet är rätt installerat och konfigurerat (se checklistan eller kapitlet Sätta upp nätverk)
- · Uppringningsnätverk (Windows 95/98) eller RAS-tjänst (WindowsNT) är riktigt installerat och konfigurerat
- · Modemet är anslutet till WinRoutes värddator.

WinRoute använder Uppringningsnätverk eller RAS-tjänster som finns tillgängliga i ditt operativsystem för Internetanslutning.

Det rekommenderas att du ansluter Internet till den dator där WinRoute ska installeras INNAN du installerar och kör WinRoute för att säkerställa att anslutningen är korrekt konfigurerad och uppringningsnätverket eller RAS fungerar som de ska.

WinRoute-konfiguration

1. När du utfört all den konfiguration som beskrivits ovan:
2. Gå till menyn Inställningar->Gränssnittstabell - du bör se alla nätverksgränssnitt som finns tillgängliga i din dator. Uppringningsgränssnitten kallas RAS i WinRoutes (både på 95/98 och NT) operativsystem.
3. Gå till Egenskaper på valt RAS-gränssnitt
4. Markera knappen "Utför NAT med IP-adressen för detta gränssnitt på all kommunikation som passerar genom"

- ***Gå till RAS-tabellen i dialogen Egenskaper, välj eller skapa din anslutning och ställ in alternativ efter dina behov. Se RAS-tabellen för ytterligare detaljer.***

Kom i håg! NAT måste markeras "ON" på RAS-gränssnittet men "OMARKERAT" på de gränssnitt som länkar till det interna nätverket.

1. Ethernet-gränssnittets konfiguration
2. Kortet för nätverksgränssnitt som leder till det interna nätverket har en tilldelad IP-adress (privat klass) och NO-tilldelad gateway!

DNS-uppgifterna som används för detta gränssnitt baseras på data från din ISP. Om du inte har fått dessa data, kontakta din leverantör av tjänster.

Du kan ställa in WinRoute så att den ger dig egenskapen nummertagning på begäran där anslutningen har upprättats automatiskt baserat på den trafik (data) som går ut ur det lokala nätverket. Klicka här för ytterligare detaljer.

AOL-anslutning

När du använder WinRoute Pro kan du ansluta ditt nätverk till Internet via enkelt AOL-uppringningskonto. Obs - AOL stöder endast Win95/98-datorer. För att ansluta via AOL följ dessa steg:

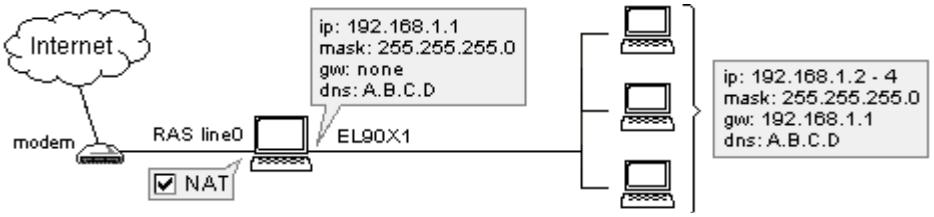
1. Installera AOL-klient (helst AOL 5.0 och högre)
2. Anslut till Internet för att säkerställa att anslutningen fungerar
3. Installera WinRoute Pro
4. I WinRoute Administration gå till menyn *Inställningar->Gränssnittstabell*
5. Du bör kunna se AOL-adaptern bland tillgängliga gränssnitt. Klicka på egenskaper för ett sådant gränssnitt och välj "utföra NAT" på det gränssnittet.

Sätt upp din WinRoute-dator och klientdatorer i enlighet med checklistan (se annat kapitel).

- ***Obs! Ring på begäran kommer inte att fungera. Du måste initiera anslutningen till AOL manuellt.***

T1- eller LAN-anslutning

T1 eller LAN-anslutningar kräver två kort för nätverksgränssnitt (NIC) installerade på WinRoute-datorn. Ett NIC kommer att länka till Internet (dvs routern) medan ett annat NIC kommer att länka til det interna nätverket.



För att ansluta till Internet:

1. Gå till menyn Inställningar->Gränssnittstabell
2. Välj NIC som länkar till Internet, klicka på Egenskaper och markera ON "Utför NAT med IP-adress för gränssnittet på all kommunikation som paserar genom". När du öppnar gränssnittstabellens dialogruta kommer du att kunna läsa NAT ON bredvid denna externa linje.
3. Kontrollera att NAT är NOT ON för det gränssnitt som länkar till det interna nätverket (gå till egenskaper för detta gränssnitt i Gränssnittstabellen)
4. Kontrollera att INGEN gateway har ställts in i TCP/IP-egenskaper för det interna NIC (gå till nätverksinställningar) och NIC har tilldelats en intern IP-adress.
5. Kontrolera att det NIC som länkar till Internet har tilldelats data från din ISP. I det fall du har en dynamiskt tilldelad IP-adress lämna inställningar för IP-adress tom.

För andra nätverksinställningar se lämpliga kapitel, särskilt ***Checklista*** .

DirecPC-anslutning

DirecPC använder ett modem (analogt, ISDN, ...) eller NIC (Ethernet, symbolprotokoll) för upplänkning medan det använder en satellitdisk för att ladda ner data. Din Internetanslutning levereras av DirecPC själv eller du kan använda din existerande ISP för uppringningsanslutning.

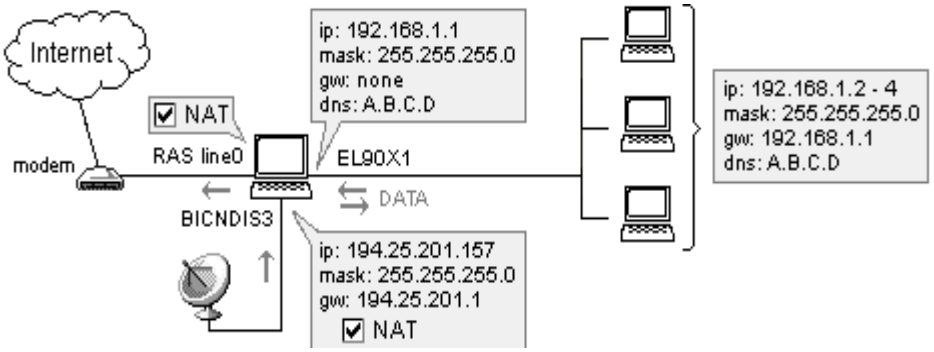
Data går från din dator via modem till DirecPC Internettjänst där data routas till sin slutliga destination. På vägen tillbaka associerar DirecPC paketen (data) som kommer till din dator med annorlunda data för att routa dem via satellitdisken.

WinRoutekonfiguration

Först av allt måse du ha all mjukvara och alla komponenter från DirecPC korrekt installerat. Fortsätt därefter att konfigurera WinRoute i enlighet med dina specifika krav.

Du kan välja antingen DirecPC-dialer eller WinRoute RAS för upplänkning. Om du använder WinRoute kommer du att kunna dra fördel av egenskapen Uppringning på begäran, detta kommer att spara pengar åt dig på din räkning.

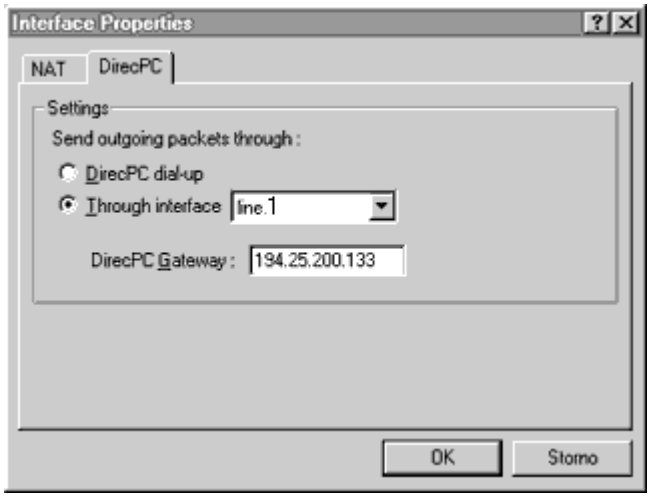
1. Att använda(RAS-linje) för upplänkning



Gå till menyn *Inställningar->Gränssnittstabell*. Du kommer att se RAS-linjens gränssnitt (ditt modem) och gränssnittskortet för DirecPC.

Klicka på gränssnittskortet för DirecPC och gå till "Egenskaper". Du kommer att se två tabbar - **NAT** och **DirecPC**.

- På NAT-tabben markerar du ON *"Utför NAT med gränssnittet på all kommunikation som passerar genom"*.
- På DirecPC-tabben väljer du att du kommer att använda *linje 0* för upplänkning. Mata in *IP-adressen för gateway* som du fick av DirecPC.

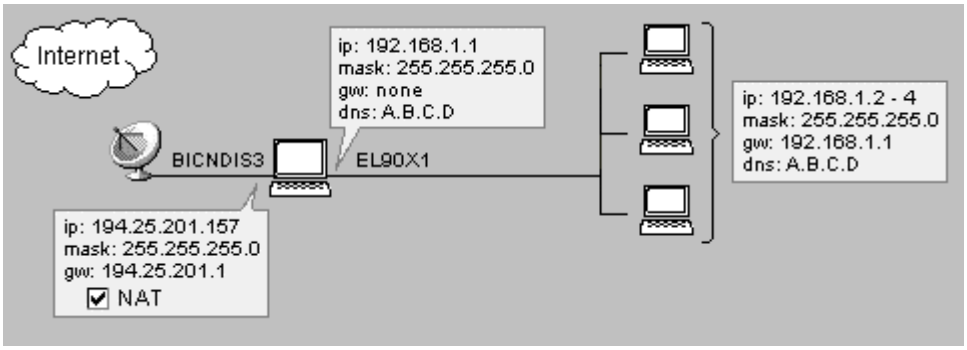


3. Klicka på RAS-gränssnittet och gå till "Egenskaper". Markera ON "Utför NAT med gränssnittets IP-adress på all kommunikation som passerar genom".På RAS-tabben väljer du den anslutning du vill använda för att ansluta till din ISP, därefter matar du in ditt användarnamn och lösenord.

- ***Obs! Du måste AVMARKERA "Använd standardgateway på fjärrnätverk" i egenskaper för uppringningsnätverkets konto som skapts för att ansluta ISP. Ställ in detta alternativ i TCP/IP-egenskaper för ditt uppringningsgränssitt.***

2. Att använda DirecPC-dialer för upplänkning

Du kan använda DirecPCs inbyggda dialer där den finns tillgänglig. Vi rekommenderar dig emellertid att använda WinRoutes RAS-linje där så är möjligt.



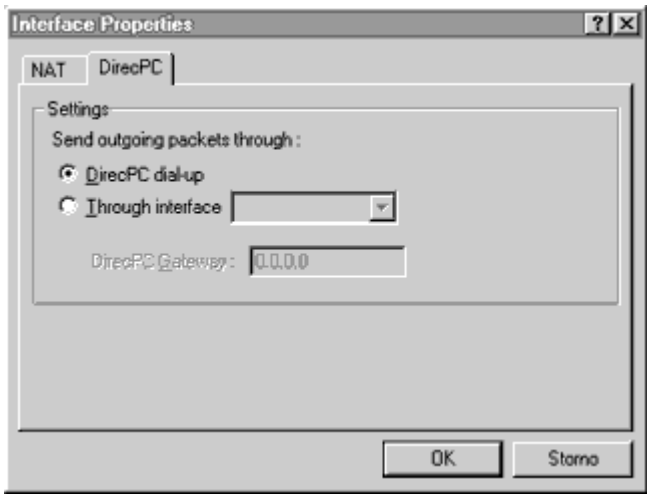
Att använda DirecPC-dialer:

Gå till menyn *Inställningar->Gränssnittstabell*. du kommer att se RAS-linjens gränssnitt (ditt modem)och gränssnittskortet för DirecPC

Klicka på gränssnittskortet för DirecPC och gå till "Egenskaper". Du kommer där att se två tabbar - NAT och DirecPC.

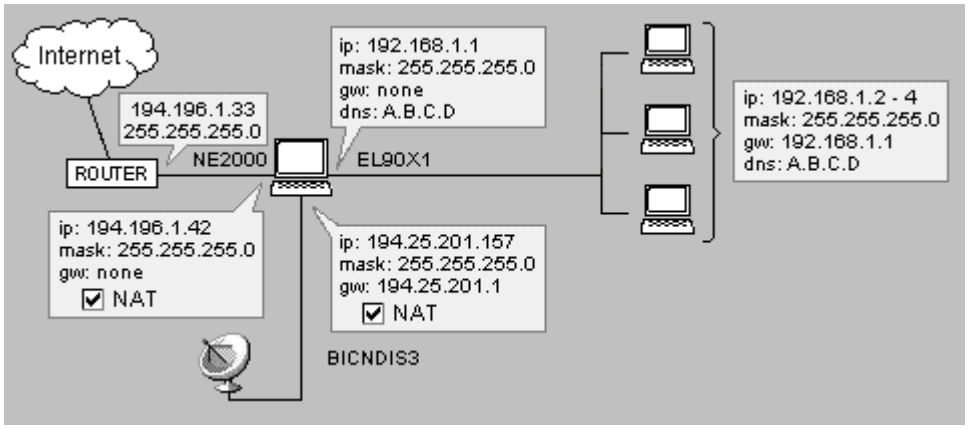
- På NAT-tabben markerar du ON "Utför *NAT med IP-adresser för gränssnittet på all kommunikation som passerar genom*".

- På DirecPC-tabben väljer du "Använd *DirecPC-dialer för upplänkning*".

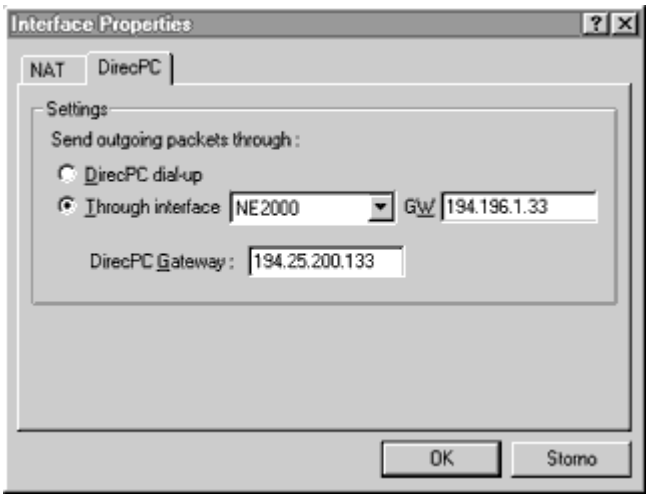


3. Att använda Ethernet-gränssnittet för upplänkning

Ibland kanske du vill använda Ethernet-gränssnittet för upplänkning. Detta händer normalt om upplänkningen genomförs via en ISDN-anslutning (och du har ISDN-router eller modem) eller V-SAT-anslutning (disk med Ethernet-adapter).



Gå till dialogen egenskaper i gränssnittskortet för DirecPC.



- På NAT-tabben markerar du ON "utför *NAT med IP-adressen för gränssnittet på all kommunikation som passerar genom*".
- På DirecPC-tabben väljer du "*Genom gränssnitt* " och väljer det gränssnitt som länkar mot Internet. Därefter matar du in standardgatewayen för din ISP till "GW-fältet" (dvs. 194.196.1.33).

Ökande genomströmning

För att uppnå högsta möjliga genomströmning av data när du är ansluetn till Internet med användning av DirecPC, minskar du **TCP receive window** på alla datorer som kommer att använda DirecPC:

På Windows NT:

1. Go till Registret HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
2. Lägg till (om det finns, redigera det) ett inmatningsnamn som "TcpWindowSize" (det är av typen DWORD) i registret. Ställ in värdet på 0xBB80.

På Windows 95:

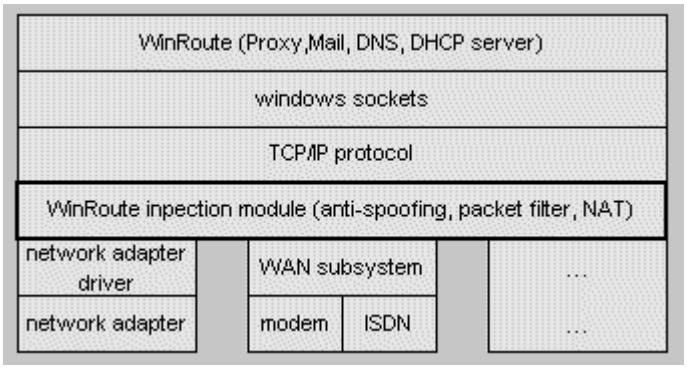
1. Gå till Registret HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP.
2. Lägg till (om det redan finns, redigera det) ett inmatningsnamn "DefaultRcvWindow" (om det är av typen sträng) i registret. Ställ in värdet på "0xBB80".

Att installera säkerhet

I denna avdelning

NAT-säkerhet

WinRoute utför NAT-operationerna på en så låg nivå för nätverksprotokoll som möjligt. WinRoute kontrollerar trafiken mellan drivrutinen för NIC (kortet för nätverksgränssnitt) och TCP-stacken. WinRoute har absolut kontroll över Internettrafiken och fångar upp både utgående och inkommande paket vilket minimerar chanserna att bli avbruten. Detta är en egenskap som är unik för WinRoutes NAT-implementering.och den ger också extra förhöjd säkerhet som paktefilterbaserad brandvägg eller antispoofing. Med WinRoutes NAT är hela nätverket fullständigt skyddat inklusive den dator som har WinRoute.



Alternativ för NAT-säkerhet

I de avancerade inställningarna för WinRoutes modell 20 och högre finns en NAT-meny för säkerhetsalternativ som inbegriper **tyst modus**. **Tyst modus** innebär att för speciella typer av förfrågningar, kan WinRoute "släppa" paket så att ditt nätverk kan verka osynligt för världen utanför.

Inkommande ICMP-ekoförfrågningar:

Internet Control Message Protocol (ICMP) är protokollet för att helt enkelt sända ut en förfrågan om information (pinging, exempel - ping 206.86.211.32). När någon dator försöker **pinga** WinRoutes värddator, erbjuder **NAT Säkerhetsalternativ** två reaktioner:

- Om du väljer *"skicka ICMP-ekosvar"* kommer den frågande datorn att få ett svar.
- Om du väljer *"släpp förfrågningar (tyst modus)"* kommer datagrammet att släppas, helt enkelt försvinna under trafik. Den part som frågar kommer då att få meddelandet *"destinationsvärd kan inte nås."*

Inkommande paket utan post i NAT-tabellen:

WinRoute inspekterar all trafik som kommer ut eller in från LAN. Om WinRoute ska utföra NAT eller inte på ett särskilt paket så kommer det först att undersöka paketet och och registrera viss information som portnummer och IP-adress till NAT-tabell. På så vis kan WiRoute när paketet kommer tillbaka jämföra det med NAT-tabellen för att avgöra vem paketet ska routas tillbaka till. Om paketet är oinitierat, vilket innebär att det inte är ett paket som kommer tillbaka, kommer WinRoute att jämföra det med NAT-tabellen och fastställa detta. Om ingen portmappning har skapats kommer inte WinRoute att kunna skicka paketet till någon innanför LAN.

- Alternivet "skicka förnekande paket" kommer helt enkelt att returnera ett paket till avsändaren och säga att förbindelse inte kunde upprättas.
- Alternativet "släpp paket" (tyst modus) kommer att eliminera paketet utan att skicka något paket i retur. På så vis kommer WinRoute-värden, liksom LAN bakom den, att se ut att inte existera.

Om inkommande UDP-paket:

En del applikationer som använder **User Datagram Protocol** (UDP) kräver att du skickar UDP-paket till en central server. WinRoute registrerar källa och destination för alla UDP-paket som går ut till den server som tilldelats av den applikation som skickar paketet. I en del fall kan servern ge ut din IP och port till en annan dator som sedan skickar dig en UDP-paket som innehåller den information du efterfrågade. Även om denna slumpdator har en annorlunda IP-adress än servern kan den ändå skicka UDP-pakettill ditt nätverk eftersom den känner till vilken IP och port den ska använda.

- Med användning av detta exempel om du väljer “kan passera genom *NAT utan någon IP-adress för källa*” kommer UDP-paketet att passera genom WinRoute.
- För att höja säkerheten kan du välja “kan passera genom *NAT endast om den kommer från säker ursprunglig IP-adress som registrerats när det första utgående paketet skickades från LAN* .” Detta skulle endast tillåta att UDP-paket från den centrala servern passerade genom WinRoute.

Alternativ för NAT-loggning:

Inom de avncerade säkerhetsalternativen finns möjligheten att registrera information om paket som kommer in till LAN men som ursprungligen inte efterfrågats av någon innanför LAN. Detta gäller normalt nätverk som kör Web, FTP, DNS eller andra typer av servrar bakom WinRoute och är av nytta för att avgöra källan till ett problem.

Att logga inkommande paket utan uppgift i NAT-tabellen:

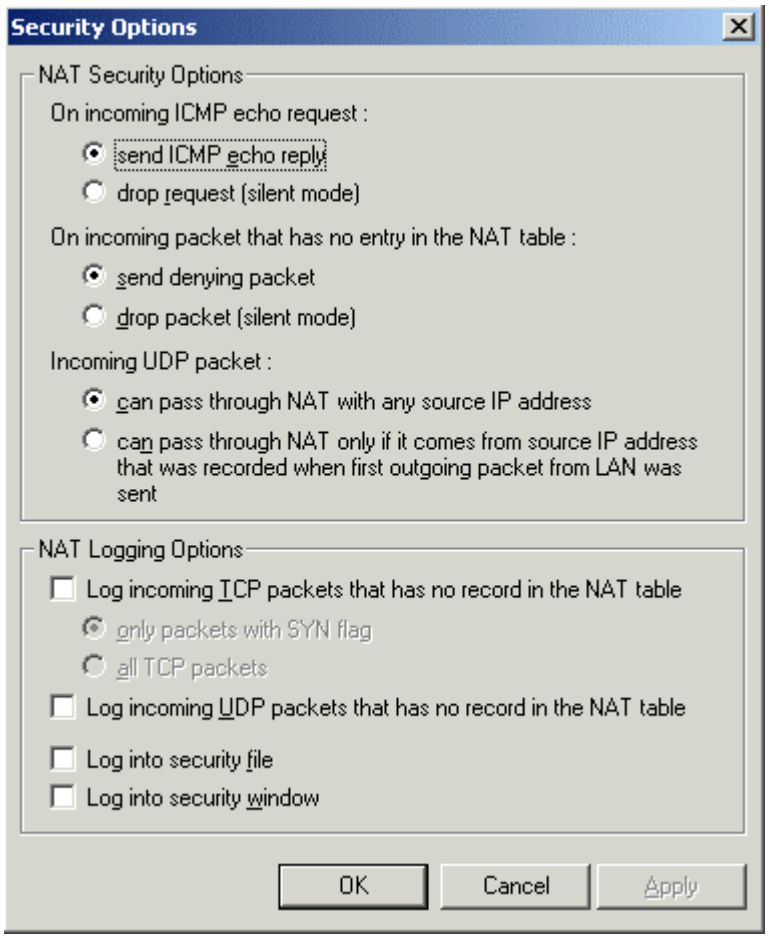
WinRoute erbjuder två alternativ för att logga TCP-paket som inte återfinns i NAT-tabellen.

- Om du väljer att logga "*endast paket med SYN-flagga*" (synkronisera), kommer TCP-paketet att loggas endast om en anslutning har upprättats mellan avsändare och mottagare.

- Alternativet "*alla TCP-paket*" loggar helt enkelt alla inkommande TCP-paket oavsett om en förbindelse upprättats eller ej. Eftersom UDP-paket inte använder flaggor kommer alla oinitierade UDP-paket att loggas om du väljer att logga UDP-paket.

Att logga till en fil eller ett fönster:

- Om du väljer "*logga till säkerhetsfönster*" kan du välja att visa logginformation från WinRoutes administrationsapplikation med angivelse av loggen visa loggsäkerhet.
- Om du väljer att "*logga till en fil*", kommer WinRoute att logga informationen till den säkerhetslogg som finns i loggmappen för WinRoute Pro (normalt c:/Program Files/WinRoute Pro/Logs)


Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Inställningar för paketfilter

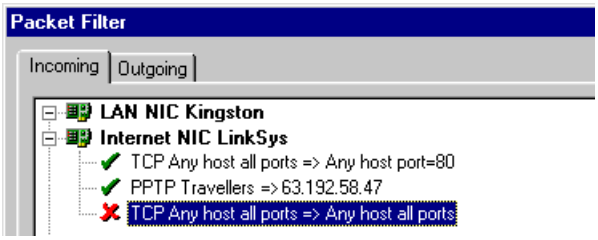
Konfigurationen för WinRoute Pros paketfilterportion för brandväggen är mycket enkel. Den kräver emellertid god förståelse av logiken bakom paketfiltreringens funktionalitet i WinRoute.

Regler att ställas in per gränssnitt

Användare kan initiera separata säkerhetsregler för individuella datorgränssitt som du har i din dator. Detta är en mycket viktig egenskap vid administration av multisegmenterade nätverk.

Exempel: följande bild visar exempel på nätverk som:

- *tillåter vem som helst från Internet att få tillgång till webbservern innanför nätverket*
- *endast tillåter vissa individer inom fördefinierade adressgrupper som kallas Travellers att få tillgång till PPTP-servern innanför nätverket för att komma in i det*



Separata regler för utgående och inkommande paket

WinRoute tillämpar särkilda regler för utgående och ingående paket. En tabell skapas inom WinRoute för varje gränssnitt. I denna tabell registreras både inkommande och utgående paket. Med andra ord, varje paket har två uppgifter, en för utgående och en för inkommande.

Vad är UTGÅENDE/INKOMMANDE paket?

WinRoute betraktar alltid sin motor som navet i hela systemet. Detta innebär att alla paket som lämnar WinRoute är UTGÅENDE oavsett om de går till Internet eller till LAN. På liknande sätt är alla paket som kommer TILL WinRoute-datorn INKOMMANDE oavsett var de kommit från. Tänk på detta när du bygger upp säkerhetsregler.

TILLÄMPNING AV REGLER:

UPPIFRÅN och NER

Regler definieras i en lista och tillämpas uppifrån och ner. När ett paket har kommit till gränssnittet kontrolleras det mot listan av definierade kriterier. Granskningen tittar först på det översta kriteriet och går sedan neråt i listan för att till sist kontrollera den lägsta regeln. När paketet svarar mot kriterierna, tillämpas regeln och resten av reglerna lämnas därhän.

Regler kan tillämpas på:

- enskilda användare
- urval av IP-adresser
- en användardefinierad grupp av IP-adresser (för att definiera en grupp av användare se referensdelen i denna manual)

- hela undernät eller nätverk

Regler kan tillämpas i fördefinierad tidszon

I en del fall kan det vara användbart att tillämpa specifika regler under kontorstid och andra kriterier för tillgång på andra tider. Eller, du kanske vill ge vissa användare tillgång till nätet under lunchtid och under arbetstid och begränsa tillgången endast till specifika resurser.

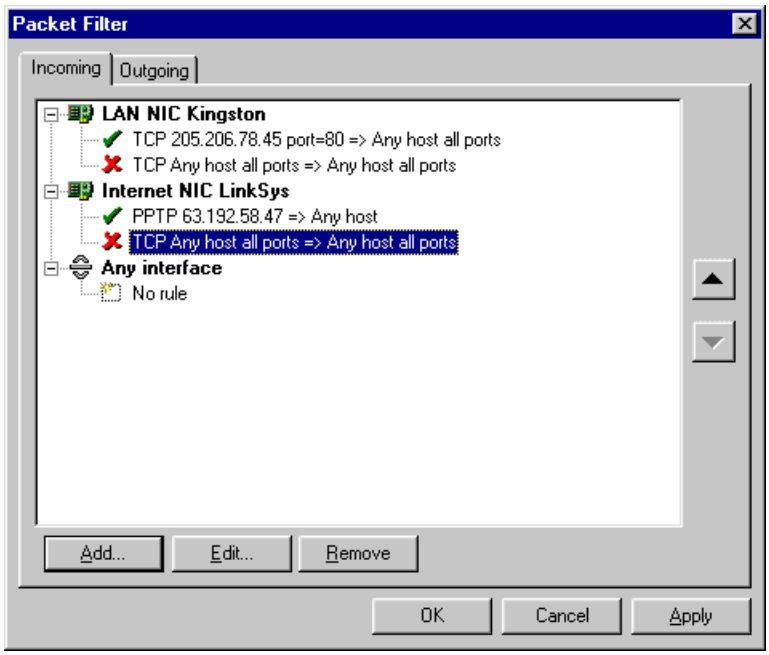
Exempel:

Total kontroll över användartillgång: nätverksadministratören vill ha användargaranterad tillgång till ditt nätverk för att få gå in. Emellertid har många nätverksuppsättningar Webb- eller FTP-servrar bakom WinRoute-systemet som kräver tillgång för allmänheten.

I ovanstående fall skulle reglerna för inkommande paket ställas in i följande ordning :

1. tillåt paket från vilken värd som helst som går till port 80
2. tillåt paket från vilken värd som helst som går till port 21
3. neka alla paket

Om det ankommande paketet träffar på regel 1. eller 2. tillåts det passera och regel 3 tillämpas inte. Om det inte motsvarar 1 eller 2 nekas det tillgång.



Exempel på grunduppsättning av filterregler

Inkommande regler (försäkra dig att de kommer i denna odning)

Protokoll	Källa	Destination	ICMP-typer	Åtgärd	Logg	
UDP	Alla adresser, Port = 53	Alla adresser, Port > 1023		Tillåt		
TCP	Alla adresser, alla portar	Alla adresser, Port > 1023		Tillståndsetablerad TCP		
ICMP	Alla adresser	Alla adresser	Ekosvar	Tillåt		
IP	Alla adresser	Alla adresser		Släpp	Till fönster	

Obs: Denna sista "upprensningsregel" kommer att inverka på alla fångstverktyg för nätverkspaket som används på denna värddator.

Exempel på grundupsättning av regler för ingående HTTP och FTP

Protokoll	Källa	Destination	ICMP-typer	Åtgärd	Logg	Be
TCP	Alla adresser, alla portar	[denna värddator], Port = 80		Tillåt	(valfritt)	Til (W der
TCP	Alla adresser, alla portar	[denna värddator], Port = 21		Tillåt	(valfritt)	Til kor vär
TCP	Alla adresser, alla portar	[denna värddator], Port = 20		Tillåt	(valfritt)	Til dat (en krä 10

Att tillåta kommunikation på vissa portar

Du vill tillämpa följande regler:

- maximal säkerhet
- tillåta tillgång till din webbserver
- tillåta kommunikation till din SMTP-server
- tillåta att e-post hämtas från Internet vid din Mail Server
- tillåta tillgång till din FTP-server

Maximal säkerhet:

Inkommande tabb

Protokoll: TCP, Neka alla inkommande paket

Ursprunglig IP - alla	Destinations-IP - alla
Ursprunglig port - alla	Destinationsport - alla

Denna regel kommer alltid att vara den lägsta av alla tillgängliga regler på gränssnittet.

Tillåt tillgång från Internet till din webbserver:

Inkommande tabb

Protokoll: TCP

Ursprunglig IP - alla	Destinations-IP - IP-adress för webbservern
Ursprnglig port - alla	Destinationsport - 80

Tillåt tillgång från vissa adresser på Internet till din FTP-server.

Inkommande tabb

Protokoll: TCP

Ursprunglig IP - alla	Destinations-IP - IP-adress för FTP-servern
Ursprunglig port - alla	Destinationsport - 21

Ursprunglig IP - alla	Destinations-IP - IP-adress för FTP-servern
Ursprunglig port -alla	Destinationsport - 20

Tillåt din SMTP-server att kommunicera endast via din relay SMTP-server (vid ISP):

Inkommande tabb

Protokoll: TCP

Ursprunglig IP - ISPs relay SMTP-server	Destinations-IP - IP-adress för SMTP-server i ditt LAN
Ursprunglig port - alla	Destinationsport - 25

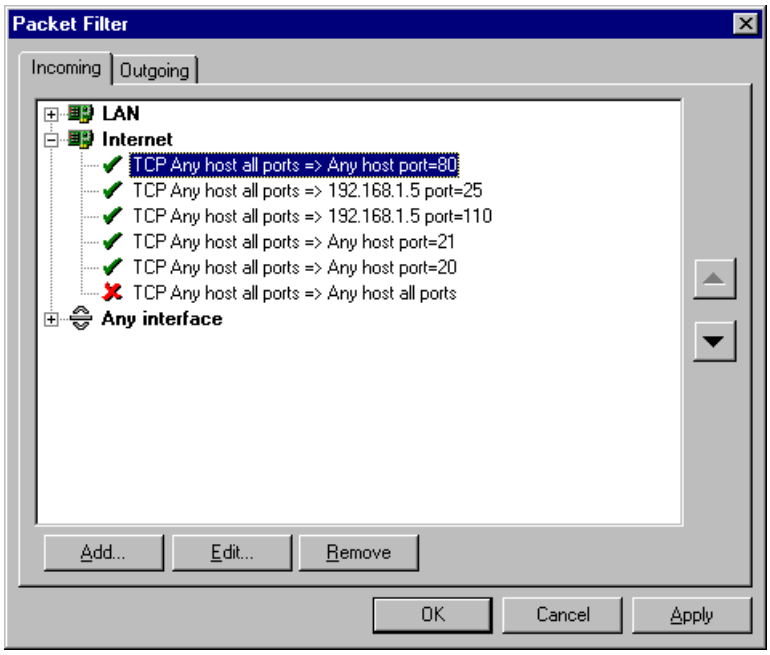
Utgående tabb

Ursprunglig IP - din SMTP-server	Destinations-IP - IP-adress för SMTP-server vid ISP
Ursprunglig port - alla	Destinationsport - 25

Tillåter dig att hämta e-post från Internet vid din Mail Server

Inkommande tabb

Ursprunglig IP - din SMTP-server	Destinations-IP - IP-adress för SMTP-server vid ditt LAN
Ursprunglig port - alla	Destinationsport - 110


Packet Filter
Incoming
Outgoing
LAN
Internet
TCP Any host all ports => Any host port=80
TCP Any host all ports => 192.168.1.5 port=25
TCP Any host all ports => 192.168.1.5 port=110
TCP Any host all ports => Any host port=21
TCP Any host all ports => Any host port=20
TCP Any host all ports => Any host all ports
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

Att tvinga användare att använda proxyserver

Ibland kan du tycka det är praktiskt att använda WinRoutes **inbyggda proxyserver**. Detta har man nytta av när man vill **övervaka** användaraktivitet när de har tillgång till webbsidor eller om du vill **tillämpa restriktioner** för kunder som har tillgång till vissa webbsidor eller när du skulle vilja att de använder **cacheminnet**.

- ***Obs! Du kan använda** paketfilter **för att kontrollera webbtrafik; men det är lättare att använda det** inbyggda proxyfiltret för URL **eftersom det löser upp domännamn vilket innebär att du endast behöver mata in URL i stället för den associerade IP-adressen.***

Inställningar:

Du måste skapa två säkerhetsregler för **utgående** paket:

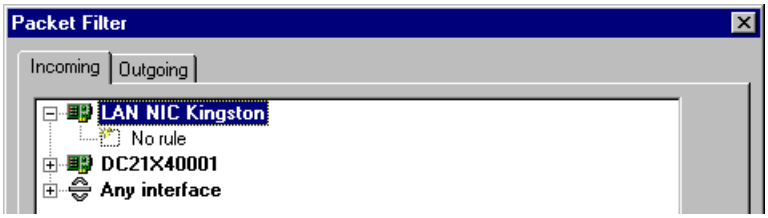
1. **Tillåt** utgående paket med *destinationsport 80 och ursprunglig IP* för WinRoutes värddator
2. **Neka** alla utgående paket med *destinationsport 80*

Reglerna måste tillämpas exakt i den ordning som förklaras ovan. WinRoute tillämpar reglernna i ordning **uppifrån och ner**. Reglerna tillämpas på basis av kommer-först-betjänas-först, dvs. söks mot reglerna där toppen kommer först och botten sist. Den första regel som motsvarar paketbeskrivningen tillämpas medan resten av reglerna förbises.

Att konfigurera regler:

1. I WinRoute-administratören går du til menyn *Inställningar=>Avancerat=>Paketfilter*. Gå till tabben *Utgående*.

2. Dubbelklicka på ditt externa (Internet) gränssnitt. Listan över regler eller "Inga regler" visas.



3. Tryck på knappen *Lägg till* för att lägga till en ny regel som kommer att göra att WinRoute-värden kan upprätta förbindelser med webbservrar på port 80.

Välj protokoll: TCP

Typ av källa: värddator

IP-adress: extern adress för din WinRoute-brandvägg (dvs. 204.23.43.26)

Destinationsport: Lika med (=) 80, under Åtgärd: välj Tillåt.

4. Tryck åter på knappen *Lägg till* för att lägga till en andra regel som kommer att neka alla andra TCP-förbindelser till port 80.

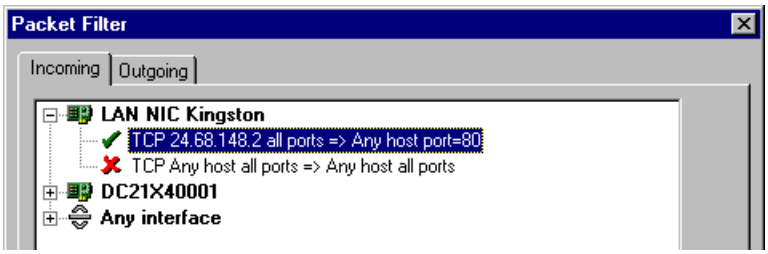
Välj protokoll: TCP

Typ av källa: alla

Destinationsport: Lika med (=) 80

Åtgärd: neka.

Om du skulle vilja logga försök markerar du rutan vid Inloggningsfil.



- ***OBS: när du konfigurerar extra regler kom ihåg att bygga rgelerna UPPIFRÅN och NERÅT.***

Att installera e-postserver

I denna avdelning

E-postanvändare

Det finns flera grundläggande regler om användare, e-postadresser och postlådor i WinRoute.

En användare = en postlåda...

Varje användare av WinRoute får en **postlåda**. Postlådan har användarens namn. I det fall du inte har registrerat någon Internet-domän och matat in i WinRoute är användarens e-postadress automatiskt användare@domän.com.

En användare = flera adresser

För att använda olika e-postadresser och bygga upp allmänna postlådor som sales@..., support@...., info@... kan du definiera olika alias. Kombinationerna är praktiskt taget oändliga.

Att lägga till användare:

1. Gå till menyn **Inställningar=>Konton**
2. Lägg till **användare**
3. Gruppera användare i **grupper** om nödvändigt

Exempel:

Ett företag har domänen brutus.com. Användaren John kommer att få e-postadressen john@brutus.com. För andra adresseringsalternativ se Alias.

- ***Obs: postlådorna finns i en separat katalog. Normalt i c:/Program files/WinRoute/Mail. Postlådorna har fysiskt skapats EFTER att det första e-brevet har kommit in.***

Att skicka e-post till andra WinRoute-användare i ditt nätverk

Får att skicka e-post till andra användare **inom** ditt LAN använd **WinRoutes användarnamn** på mottagaren snarare än hans fullständiga **Internet e-post** adress.

Exempel: Mottagarens användarnamn är John oh hans fullständiga e-postadress är john@company.com. Du kan mata in enbart *john* i *To-fältet* på e-postmeddelandet.

Problem med alias

Om du använder den **fullständiga e-postadressen** för en lokal användare kommer meddelande att gå **genom** Internet, dvs. till relay SMTP-servern för WinRoute och sedan tillbaka till WinRoute. För att undvika detta måste du ange olika alias.

- ***Kom ihåg! Du måste ställa in WinRoute-datorn som din utgående e-postserver (SMTP).***

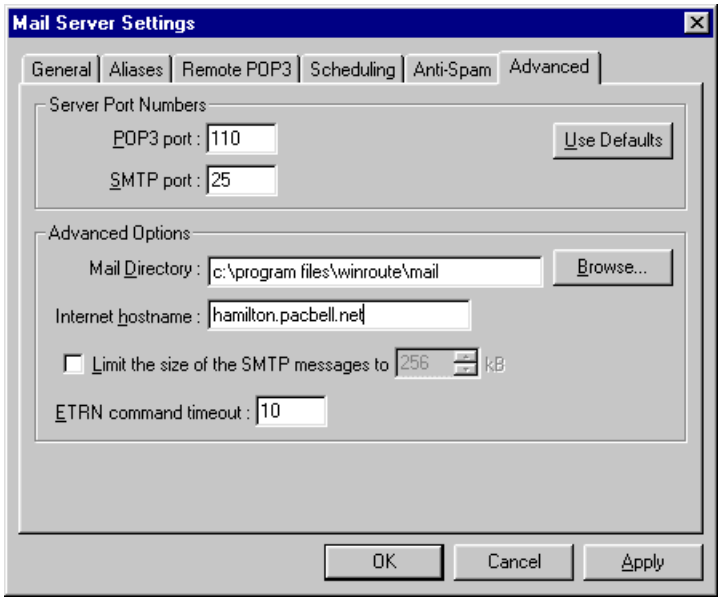
Autentiseringsproblem

Autentisering

En del ISP utför autentisering för e-post som kommer genom för att undvika skräppost. Då måste du förse din ISP med tillräcklig information.

1. Gå till *E-postserver->Avancerattabbens* fönster

2. Mata in önskat **värddatornamn** i fältet för Internetvärd. Vanligen är detta namnet på datorn som är ansluten till Internet, t.ex. *host.isp.com*.



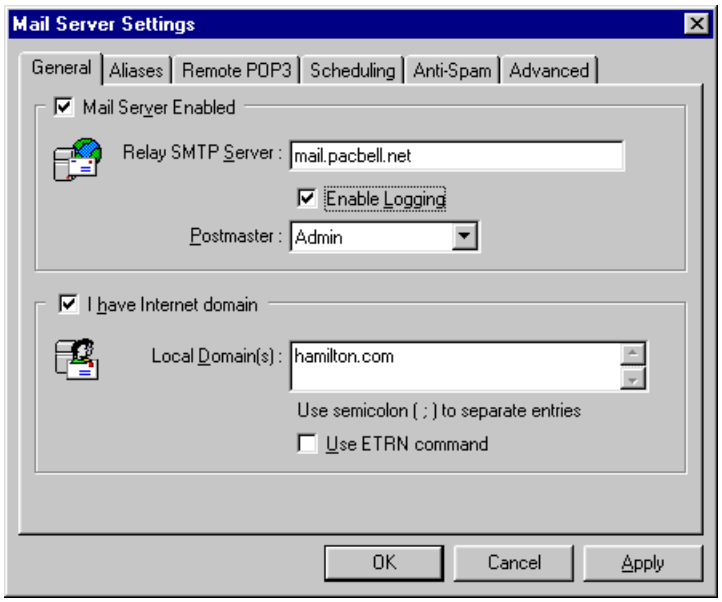
Att skicka e-post till Internet

Du kan använda WinRoute som din **SMTP-server för utgående post**. WinRoute använder **relay SMTP-servern** för din ISP för att skicka ut e-post i stället för att använda MX records. Med andra ord - all utgående e-post kommer att skickas genom den andra e-postservern som du matar in (vanligen e-postservern för din ISP). Samma regler kan tillämpas på dina e-postklienter - WinRoutes e-postserver kan vara deras relay SMTP-server.

För att ställa in relä SMTP-servern för utgående post:

1 Gå till menyn *Inställningar>E-postserver*

2 Mata in den utgående e-postservern för din ISP i fältet *Relay SMTP-server*

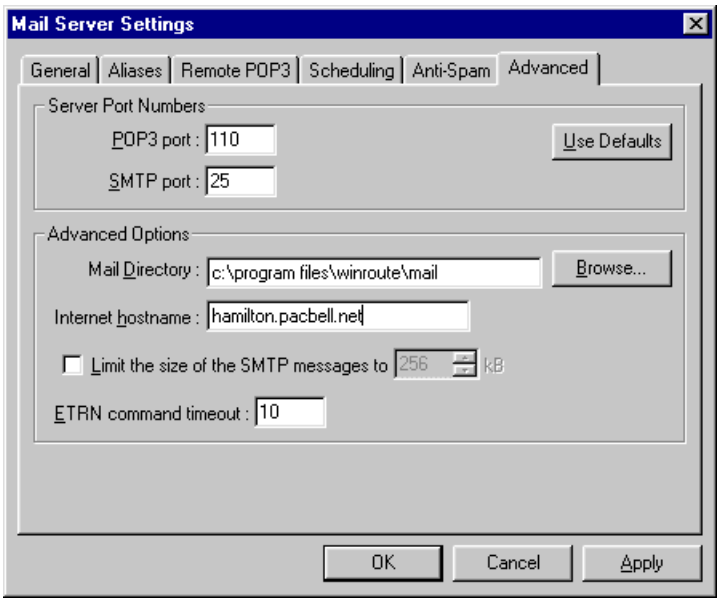


Autentisering

En del ISP utför autentisering av e-post som kommer in för att undvika skräppost . Då måste du förse din ISP med tillräcklig information.

1. Gå till *E-postserver->Avancerattabbens* fönster

2. Mata in det önskade **värddatornamnet** i fältet för namn på Internetvärd. Vanligen är detta namnet på datorn som är ansluten till Internet , t.ex.. *host.isp.com*.



Alias

Alias i WinRoute används för **extra** adresser åt användare av WinRoute och också för **ersättning**av e-post adresser

genom **alias** kan du:

- tilldela en användare flera adresser
- tilldela en e-postadress till flera användare
- tilldela en e-postadress till en grupp av användare
- tilldela en grupp adresser

Exempel:

Detta exempel visar att möjligheterna praktiskt taget är oändliga.

Företaget har 2 domäner:

- company.com
- company2.com

Användaren *John* bör få e-post till:

john_speaker@company.com

john@company2.com

sales@company.com

support@company.com

E-post till *sales@company.com* bör också levereras till gruppen *[Sales]*.

Lösning:

1. Gå till menyn *Inställningar=>E-postserver=>Alias tabb*.

2. Läg till följande alias:

*john** leverera till *John* -

detta skulle leverera all e-post som kommer in från Internet där john finns med som mottagare. Dvs. *john_speaker@company.com* lika väl som *john@company2.com* kommer att levereras till en användare *John.* Detta kommer alltså att hindra e-post som skickas från lokal användare till mottagaren *john@company.com* från att gå ut via Internet och e-posten kommer att levereras rätt till Johns postlåda på WinRoute.

sales leverera till *John* -

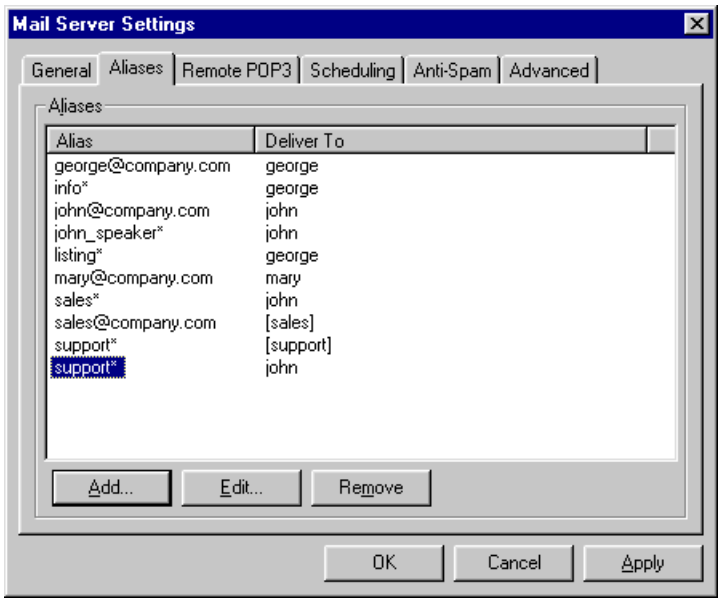
detta kommer att leverera all e-post till *sales@…..* till en användare *John*

Support leverera till*John* -

detta kommer att leverera all e-post till *support@……* till *John*

Sales leverear till *[Sales]* -

detta kommer att leverera e-post till *sales@….* till alla medlemmar i gruppen *[Sales]*



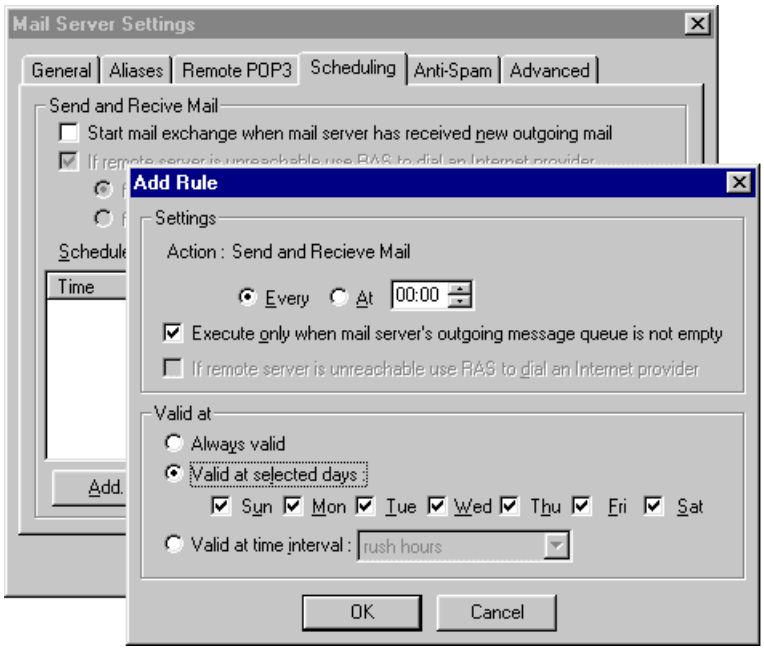
Att schemalägga e-postutbyte

Schemaläggning med Mail Server-inställningarna ger dig alternativ för att ställa in:

- regelbundna intervaller för att kontrollera e-post på din ISP (om det är POP3 eller SMTP med användning av ETRN)
- regler för att skicka e-post
- tidsintervaller när reglerna är giltiga Du kan fördefiniera tidsintervaller vid menyn *Inställningar->Avancerat->Tidsintervaller*

Du kan bestämma om du vill skicka ny utgående e-post omedelbart efter att den kommer till e-postservern eller att skickad den inom en fördefinierad tidsperiod.

Du kan också välja om e-postservern ska ringa upp ifall det finns ny utgående e-post eller inte. Om du väljer detta alternativ kommer WinRoutes e-psotserver att upprätta förbindelsen varje gång någon av dina användare ska skicka ny e-post.



För att te emot e-post måste du specificera hela kalendern och säga exakt när du skulle vilja hämta e-posten. Du kan kombinera olika regler för att göra din e-psothämtning så effektiv som möjligt.

1. Gå till menyn *Inställningar->E-postserver->Schemaläggning*
2. Ange de alternativ som du vill ha och lägg till nya regler för att kontrollera e-posten.

- ***Obs! Reglerna för "tidsintervall" måste ställas in i menyn Inställningar->Avancerat->Tidsintervall***

Att ta emot e-post

I denna avdelning

Du har en domän (SMTP)

WinRoutes e-postserver är fullt överensstämmande med ***SMTP***[1] och ***POP3***[2]. Du måste ha registrerat din egen **Internetdomän** och ta emot e-post via SMTP och/eller WinRoute för att automatiskt hämta e-post från POP3-kontot på din ISP.

Om du har registrerat en Internetdomän för din externa (allmänna) IP-adress kan WinRoute ta emot e-post via SMTP-protokoll. Mata in namnet på den domän du har registrerat under tabben allmänt i e-postserverns dialogruta.

- ***Glöm inte att mappa TCP-protokollet port 25 till den privata klassens IP-adress i din WinRoute-box! Annars kommer inte SMTP-protokollet att tillåtas gå genom WinRoutes NAT!***

---

[1] **SMTP** (Simple Mail Transfer Protocol) används för direkt kommunikation mellan e-postservrar (så som e-postservern i WinRoute och e-postservern för din ISP) och för att skicka ut e-post från e-postklientens mjukvara. SMTP är ett "envägs"-protokoll - dvs. e-post kan skickas eller tas emot av e-postservern men den kan inte hämta e-post vid någon annan e-postserver som använder detta protokoll.

SMTP-protokollet är ett TCP-protokoll som arbetar på **port 25**. Om du vill få tillgång til detta protokoll med den e-postserver som körs bakom eller på WinRoute-datorn (för att tillåta en annan e-postserver att skicka e-post till dig eller för att använda denna e-postserver för din utgående e-post om befinner sig på ditt LAN) så måste du utföra **portmappning** för TCP-protokoll, port 25 skickas till **privatklass** IP-adress för den dator som kör e-postserver.

[2] **POP3**-protokoll används mest av e-postklientens mjukvara för att hämta e-post från postlådor vid POP3-kompatibla e-postservrar. WinRoute har också denna förmåga, dvs. det kan automatiskt hämta e-post vid vilken POP3-kompatibel e-postserver som helst och distribuera den vidare till postlådor för lokala mottagare.

POP3-protokoll är ett **TCP**-protokoll som arbetar på **port 110**. Om du vill ha tillgång till denna e-postserver för protokoll som körs på eller bakom WinRoute-datorn (för att hämta din e-post FRÅN Internet) måste du utföra **portmappning** för TCP-protokoll, port 110 skickas till **privatklass** IP-adress för den dator som kör e-postservern.

Baserat på din Internetanslutning kan du begrunda följande:

1 Du har en permanent anslutning

Ingen specifik inställning krävs. Bara domän(er) matas in

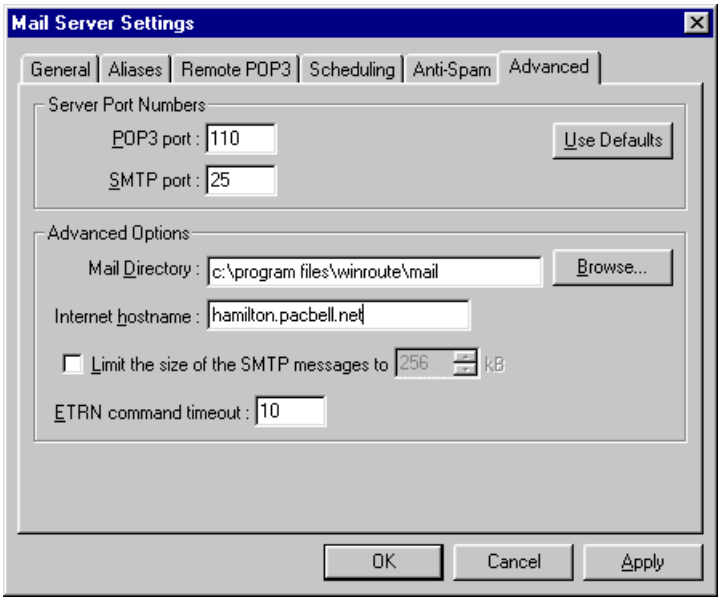
2 Du har en uppringnings- eller ISDN-anslutning (ETRN-kommando)

I det fall du inte är permanent ansluten lagras din e-post tillfälligt vid ISP. E-posten överförs när du är ansluten. En del ISP kräver användning av ***ETRN***[3]-kommando för att efterfråga e-post. WinRoutes e-postsever stöder ETRN-kommandot. Du kan kontrollera på tillvalet under *Allmän tabb* i **e-postserverns** dialogruta.

[3] ETRN är ett kommando som används av SMTP-servrar för att förhandla om längre tid, efter att ha etablerat en anslutning bör SMTP-server göra en förfrågan om SMTP-post.

ETRN-kommandot används alltid där en SMTP-server inte är "online" 24 timmar om dygnet och e-post till en sådan SMTP-server måste lagras på en tillfällig plats på en annan SMTP-server.

Om du behöver kan du ställa in time-outintervall för ETRN (gå till *Avancerattabben*).



Time-out för ETRN-kommando

Denna uppgiftt anger hur lång tid efter upprättandet av anslutning som WinRoutes SMTP-server ska göra förfrågan om SMTP-post.

Multipla domäner

Multipla domäner

Du kan ha flera domäner tilldelade till dina Internetanslutningar. Om du har flera domäner mata in dem alla i menyn *Inställningar=>E-postserver=>Allmänt*-tabben och skilj dem åt med semikolon.

Problem med multipla domäner

Det finns två sätt att ordna multipla domäner som tilldelats ditt nätverk:

1 Varje domän är associerad med sin egen IP-adress

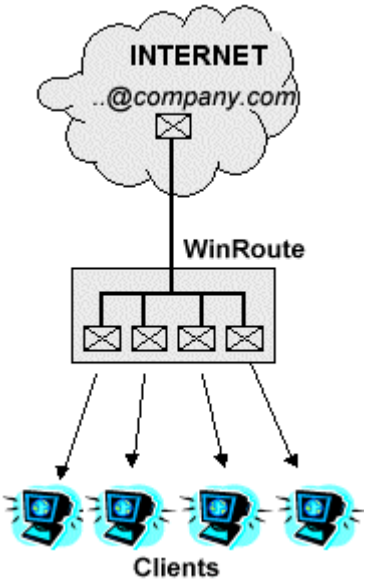
I detta scenario måste du ha flera allmänna IP-adresser mappade till det gränssnitt till Internet som används av WinRoute förr Internetanslutningar. Sedan måste du använda fler inställningar för portmappning - en för varje IP-adress - med samma IP-adress för destination på WR-datorn.

2 Alla domäner är associerade med en och samma IP-adress

Inga speciella inställningar krävs annat än att sätta upp portmappningen för TCP-protokollet på port 25 till den lokala IP-adressen för din WinRoute-dator.

Du har domän tilldelad POP3-konto

Du kan ordna med din ISP så att all e-post för din domän kommer in till ett enda konto. WinRoute kan kontrollera ett sådant konto, hämta meddelandena och automatiskt distribuera till de lokala användarnas postlådor.

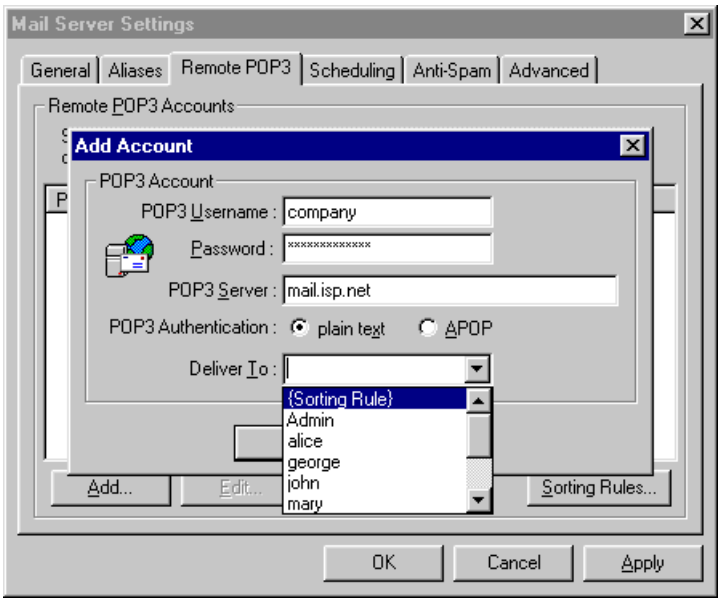


Exempel

Din ISP har upprättat postlådan company@mail.isp.net. Du har domänen company.com men all e-post till din domän (sales@domain.com, john@domain.com) kommer till postlådan company@mail.isp.net vid ISP.

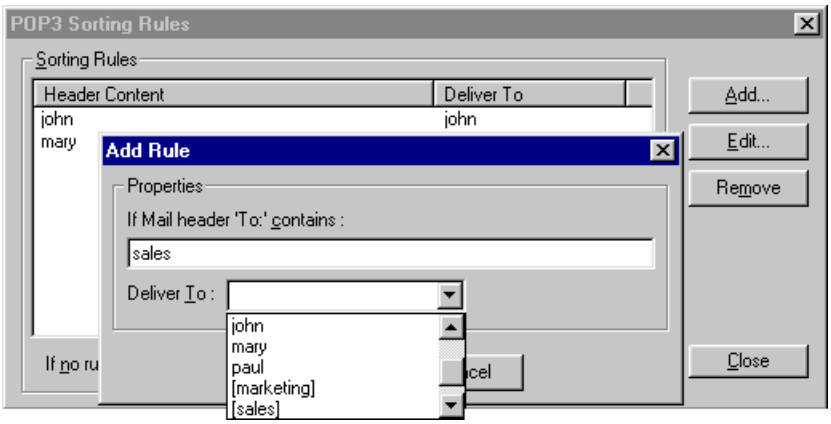
1 Gå till menyn *Inställningar=>E-postserver=>Fjärr-POP3*, lägg till nytt konto och ändra dess detaljer

2 Under "Leverera till:" välj "Sorteringsregler"



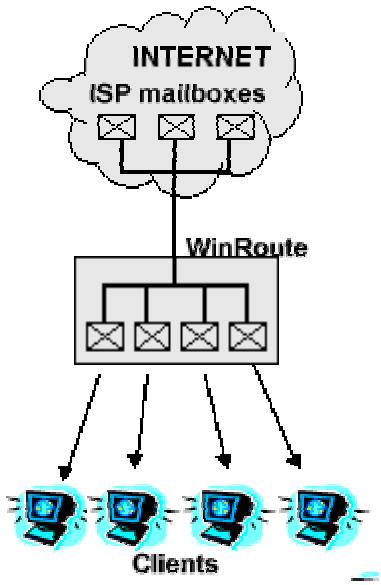
3 Tryck på knappen Sorteringsregler och lägg till nya kriterier. WinRoute kommer att leverera e-post baserat mottagarens e-postadress, avsändare eller ämne.

4 Välj i samma dialog en användare eller grupp användare som e-posten ska levereras till.

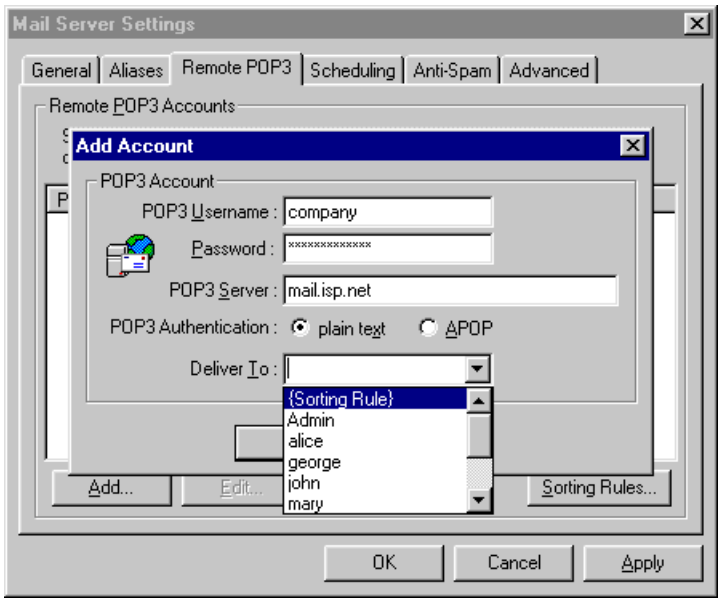


Ta emot e-post - Du har flera postlådor vid ISP

WinRoute kan kontrollera flera konton vid flera olika ISP och automatiskt leverera mottagen e-post till lokala mottagares postlådor.



1. Gå till menyn *Inställningar>E-postserver=>Fjärr-POP3*, lägg till nytt konto och mata in dess detaljer.
2. Under "leverera till:" välj mottagare eller grupp av mottagare



Inställningar för e-postklientens mjukvara

I denna avdelning

Att gå via WinRoutes e-postserver

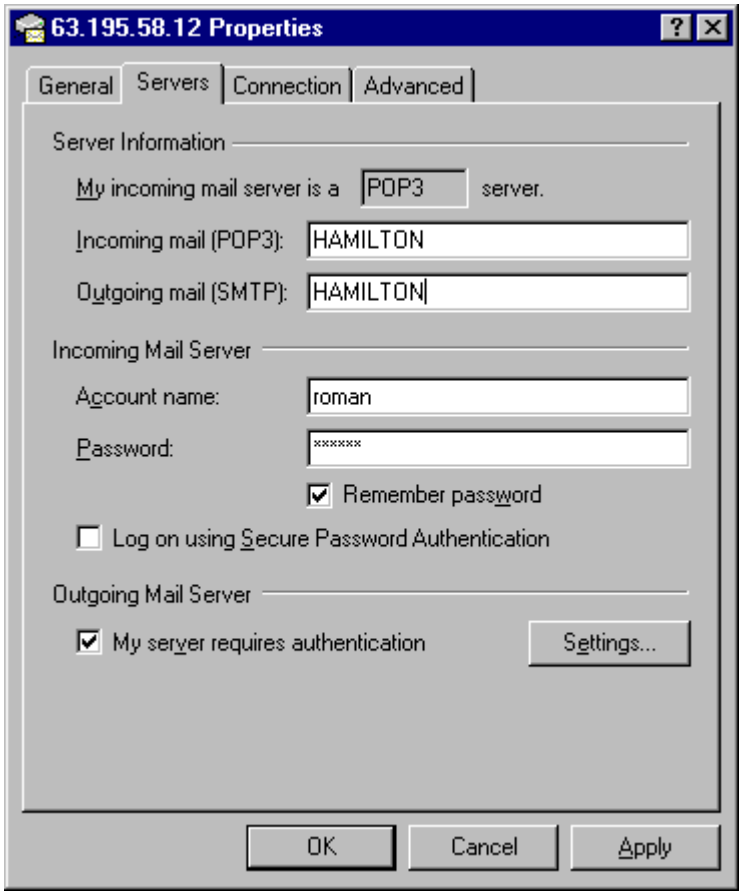
E-post genom WinRoutes e-postserver

För att använda WinRoutes e-postserver måste du konfigurera **mjukvaran för din e-postklient**. WinRoute-datorn kommer att agera som den **Inkommande** och **Utgående** e-postservern. Därför måste du mata in WinRoutes datornamn i rätt fält på din e-postmjukvara. Om du får problem med att skicka och ta emot e-post, rekommenderar vi att du matar in IP-adressen istället för datorns namn innan du gör ytterligare undersökningar. Ibland finns problemen med DNS-upplösning i ditt lokala nätverk, det kan se ut som om du inte använder WinRoutes DNS-server.

Exempel:

WinRoutes e-postserver körs på en dator med dynamiskt tilldelad allmän IP-adress och en privat IP-adress på 192.168.1.1. Datorns namn är Hamilton (se Nätverk i Kontrollpanelen).

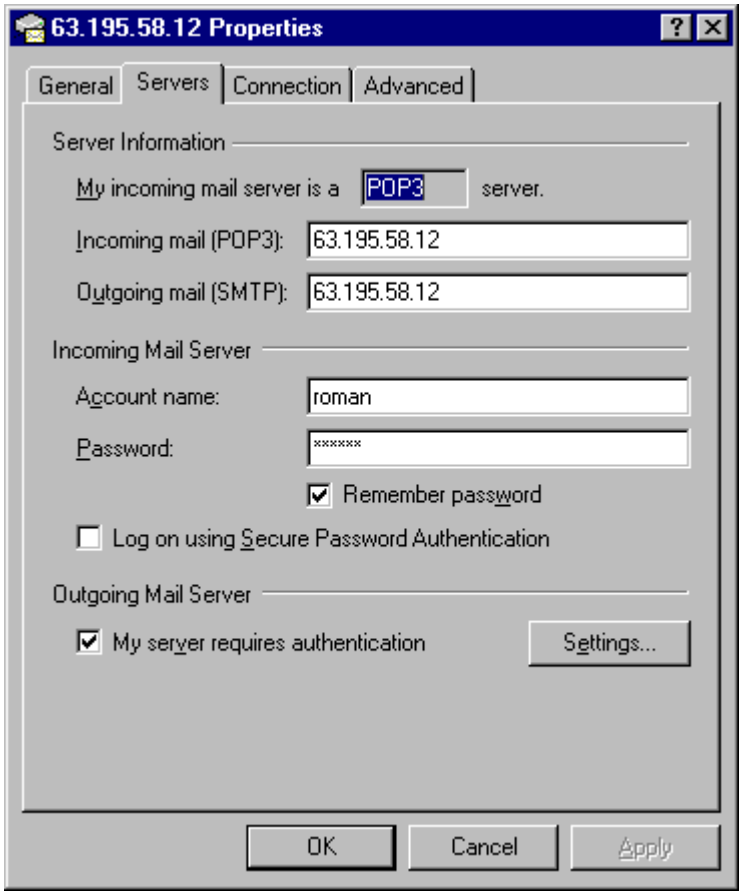
Du kan mata in antingen HAMILTON eller 192.168.1.1 i fälten för inkommande (POP3) och utgående (SMTP) e-postserver på din e-postmjukvara.


63.195.58.12 Properties
General
Servers
Connection
Advanced
Server Information
My incoming mail server is a
POP3
server.
Incoming mail (POP3):
HAMILTON
Outgoing mail (SMTP):
HAMILTON
Incoming Mail Server
Account name:
roman
Password:
******
Remember password
Log on using Secure Password Authentication
Outgoing Mail Server
My server requires authentication
Settings...
OK
Cancel
Apply

Att gå förbi WinRoutes e-postserver

Du kanske vill gå förbi WinRoutes e-postserver och ta emot eller skicka e-post direkt från en e-postklient genom e-postservern för din ISP.

I sådant fall var vänlig mata in inställningarna för utgående och inkommande e-postserver, det riktiga namnet på e-postservrarna för din ISP.



- ***Obs! Ställ inte in mjukvaran för din e-postklient på att använda proxy! Du måste använda WinRoutes NAT för tillgång till Internet och ställa in din klientmjukvara på att få***

direkt tillgång till Internet. Om du inte kan upprätta e-postutbyte innebär det att NAT inte är rätt konfigurerat. Följ Checklista ***för att konfigurera rätt!***

KAPITEL 3

EXEMPEL PÅ UTVECKLING

I detta kapitel

IPSEC, NOVELL och PPTP VPN-upplösningar

I denna avdelning

IPSEC VPN

WinRoute Pro 4.1 stöder IPSEC i så kallat "**Tunnelmodus**". "**Tunnelmodus**" bör stödja alla IPSEC-klienter som tillåter att IP-adressen för transport ändras.

Obs: WinRoute stöder inte klientmjukvaran Checkpoint Secure Remote VPN.

WinRoute-inställningar:

Skapa en mappad port för ESP:

Protokoll: annat än 50

Avlyssnings-IP: <ospecificerat>

Destinations-IP: den privata IP-adressen för klientdatorn

Vi föreslår ochså att man skapar en mappad port för IKE. Detta är inte nödvändigt i de fall kommunikatioenn initieras FRÅN ett ställe bakom WinRoute till Internet men vissa tillämpningar av IPSEC kan kräva denna inställning:

IKE portmappning:

Protokolll: UDP

Avlyssnings-IP: <Ospecificerat>

Avlyssningsport: 500

Destinations-IP: den privata IP-adressen för klientdatorn

Destinationsport: 500

Att köra multipla IPSEC-sessioner samtidigt

Skulle det finnas flera IPSEC-klienter behöver du använda separata IP-adresser för varje klient. Obs - WinRoute NAT kommer att låta så många klienter passera genom samtidigt som du önskar så länge som anslutningen har initierats FRÅN det lokala nätverket och varje klient "använder" en IP-adress som tilldelats WinRoutes externa gränssnitt.

Allmän information om IPSEC

IPSec är ett krypteringsprotokoll som används för säker kommunikation melan två datorer.

IPSec använder antingen AH (Authentification Header) eller ESP (Encapsulating Security Payload). AH kontrollerar endast avsändarens identitet och innehållet i paketet. Data krypteras inte.

ESP krypterar data. ESP tillåter användning av så kallat "Tunnelmodus" vilket liknar PPTP-protokollet. Paketet inkluderar IP-rubriken (nödvändigt för transport) som inte är krypterad och den portion data som innehåller det krypterade ursprungliga paketet.

Protokollet IKE (ibland kallat ISAKMP) används för autentisering (utbyte av säkerhetsnycklar). IKE körs på protokollet UDP port 500. Denna port används som källa och destination.

AH använder protokoll 51, ESP använder protokoll 50. IPSec kan dessutom kommunicera med hela certifikationsenheten med användning av andra protokoll som inte inverkar på NAT.

Vi kommer att bygga in protokoll 50 i WinRoute automatiskt så att det inte alls kommer att finnas något behov av portmappning. Det enda villkoret för att upprätta förbindelsen automatiskt skulle bli att initeringen av den FRÅN det lokala nätverket.

De flesta försäljare av IPSec använder algoritmen MD5 och SHA1 för autentisering och DES, 3DES och Blowfish för kryptering. IPSec är inte nära ansluten till någon specifik algoritm så lösningarna från olika försäljare kan vara inkompatibla.

Novell Border Manager VPN

Att använda WinRoute Pro med Novell BorderManager VPN (IPSEC)

Detta dokument beskriver den installation som gör det möjligt att ansluta till ett lokalt nätverk som använder NAT för att dela en enda IP-adress som fåtts av ISP till et fjärrnätverk som använder Novell BorderManager Enterprise Server för VPN-ansluyningsbarhet.

Enligt den README.TXT-fil som kommer med installationsdisketten till Novell BorderManager VPN Client så

"kan du inte använda NAT på sökvägen emellan en VPN-klient och en VPN-server. Detta på grund av att då IP- och IPX-paketen förkortas och krypteras vid VPN-klineten är den ursprungliga IP-adressen som används för fökortningen adressen till VPN-klienten. Uträkningen för IPSEC autentiseringsrubrik baseras på denna adress och på VPN-serverns destinationsadress. Därför, om endera adressen modifieras (VPN-klient eller VPN-server) av NAT,kommer uträkningen inte att stämma när den den kommer till destinationens VPN-server och paketet kommer att kasseras. Mest troligt emellertid kommer NAT att släppa IPSEC-paketerna eftersom det endast hanterar TCP-, UDP-, Internet Control Message Protocol- (ICMP)paket.

När du har arbetsstationer i ett intranät som måste kommunicera säkert med nätverk som skyddas av en VPN-server över Internet, föreslår vi att du använder VPN-egenskapen sajt-till sajt på Novell BorderManager Enterprise Edition (istället för klient -till-klient VPN)."

Emellertid är Novell BorderManager Enterprise Server mycket dyr för hemmaanvändaren. Dessutom kräver den omfattande installation av de statiska routerna på fjärrnätverket som det ansluts till. Den lösning som föreslås här ovan av Novell är därför inte genomförbar för den person som vill ansluta sitt lokala nätverk som använder NAT till ett fjärrnätverk via Novell BorderManager VPN.

Förvånansvärt nog är det möjligt att ansluta det lokala nätverk som använder NAT till ett fjärrnätverk som använder WinRoute Pro och Novell BorderManager VPN Client. Denna konfiguration tillåter alla datorer på det lokala nätverket att få tillgång till resurserna på fjärrnätverket när VPN-tunneln upprättats på routerdatorn. Ingen konfiguration för fjärrnätverket krävs.

Nedan hittar du konfigurationstegen för det lokala nätverket.

Steg 1: Installera och konfigurera mjukvaran för Novell BorderManager VPN Client på den dator som ska användas som router. Försäkra dig om att VPN-anslutningen till fjärrnätverket kan upprättas med framgång och tillgång kan fås till resurserna på fjärrnätverket.

Steg 2: Installera WinRoute Pro på routerdatorn. Följ de instruktioner som återfinns i Administratörsguiden för att konfigurera WinRoute Pro och konfigurera datorerna på det lokala nätverket för att arbeta med WinRoute Pro. Använd vanlig konfiguration enkel delning av IP-adress. Försäkra dig om att resurserna på Internet kan kommas åt från alla datorer på det lokala nätverket.

Steg 3: När du behöver tillgång till resurserna på fjärrnätverket kör du Novell BorderManager VPN-klineten på routerdatorn och loggar in i fjärrnätverket.

Detta möjliggörs av WinRoute Pros konstruktion. Eftersom det arbetar på IPSEC-nivån, sker adressöversättning innan paketet routas till den verkliga nätverksadaptern. Därför har de paket som skickas till VPN-servern den riktiga ursprungliga IP-adressen. På vägen tillbaka passerar de paket som tas emot från den verkliga nätverksadaptern genom lagret för adressöversättningen och routas till rätt dator på det lokala nätverket.

Begränsningarna i denna installation är att VPN-inloggningen måste utföras manuellt på routerdatorn och att VPN-anslutningen kommer att löpa ut efter en vis tid av inaktivitet som har ställts in på VPN-servern. Inte heller IPX-paket kommer att routas även om VPN-tunneln har aktiverat IPX- protokoll. Därför kommer tunnelförfarande med IPX att finnas tillgängligt endast på routerdatorn.

Sammanfattningsvis ger denna installation ett kostnadseffektiv och bekvämt sätt att ansluta ett lokalt nätverk som använder NAT till ett fjärrnätverk som använder Novell BorderManager VPN.

Att köra en PPTP-server bakom NAT

För att köra en PPTP-server på nätverket bakomWinRoute (inbegripet den dator på vilken WinRoute körs) måste du installera Portmappning.

Viktigt: om VPN-servern är lokaliserad på WinRoutes värddator, måste du mappa destinations-IP till den **allmänna adressen***, inte den privata. Avlyssnings-IP bör kvarstå ospecificerad.*

För kontrollanslutningen:

- Protokoll: TCP
- Avlyssnings-IP:
- Avlyssningsport: 1723
- Destinations-IP: IP-adress för din PPTP-server (t.ex.192.168.1.12)
- Destinationsport: 1723

För GRE (PPTP)-paketen:

- Protokoll: PPTP
- Avlyssnings-IP:
- Destinations-IP: IP-adress för din PPTP-server (t.ex.192.168.1.12)

Efter installation av portmappning som visats ovan kommer du att kunna placera din PPTP-server varsomhelst bakom WinRoute INKLUSIVE på datorn MED WinRoute. Användarna kommer att få tillgång till din PPTP-server genom "inringning" till den externa (allmänna) IP-adressen på ditt nätverk. När paketen når WinRoutes dator kommer de automatiskt att vidarebefordras till rätt dator bakom brandväggen.

Exempel på PPTP-upplösning

WinRoute tillåter ett mycket kostnadseffektivt sätt att skapa ditt eget WAN mellan filialer som är anslutna till Internet. Vi antar att läsarna av detta dokument har grundlägande kunskaper om nätbyggnad och WindowsNT.

Det är möjligt att skapa ett sådant WAN i flera lätta steg:

1 Kontrollera omgivningarna:

NT-server i båda ändarna

WinRoute Pro installerad i båda ändrana

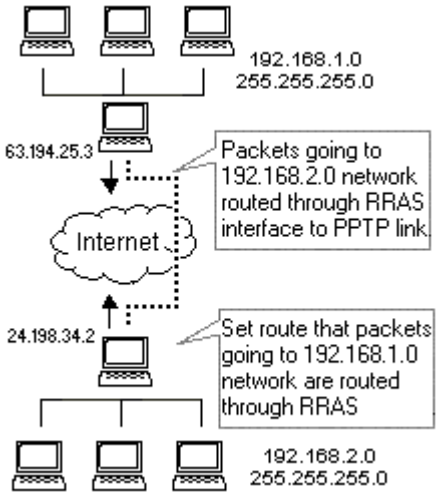
RRAS (Stealhead) installerat på båda NT-servrarna

2 Skapa en statisk route på båda NT-servrarna och ange att paket som går till det motsatta nätverket går genom RRAS-gränssnittet. Därefter - om du visar TCP-egenskaper i felsökningsloggen på WinRoute-administratören bör du kunna se inringningsgränssnittet listat bland tillgängliga gränssnitt.

3 Gå i WinRoutes administration till gränssnittstabellen och visa egenskaper för RAS-gränssnittet som används för PPTP-länk. Försäkra dig om att du inte kommer att utföra NAT på det gränssnittet.

4 Under RAS-tabben på RAS-gränssnittets egenskaper väljer du PPTP-anslutning bland RAS-uppgifterna. Om du inte ser RAS-anslutningen bland RAS-uppgifterna försäkra dig om att du har ställt in rätt telefonbok. Gå till menyn *Inställningar->Avancerat->Diverse alternativ* och välj rätt RAS-bok som du ska använda.

5 Testa anslutningen - du bör kunna pinga till det motsatta nätverket och samtidigt bör du kunna ha tillgång till Internet.



Att köra PPTP-klienter bakom NAT

Inga inställningar krävs för att köra PPTP-klienter bakom WinRoute (NAT) med tillgång till PPTP-servern utanför Internet. Du kan upprätta så många samtidiga anslutningar som behövs.

DNS-upplösning

I denna avdelning

DNS-server på WinRoute-dator

Att köra en verklig DNS-server på en WinRoute-dator kommer inte att medföra några svåra problem. Alla DNS-förfrågningar som kommer till din DNS-server kommer att besvaras av den vanliga Internet IP-adressen som är associerad med den domänen. En sådan IP-adress måste vara associerad med det nätverksgränssnitt som länkar den från WinRoute-datorn till Internet WWW-servrarna lyssnar på både de allmänna och de privata gränssnitten.

Om den lokala datorn skickar en DNS-förfrågan för att upplösa www.mydomain.com, får den en allmän IP-adress associerad med denna domän och ansluter till webbservern med en IP-adress (som har tilldelats Internet-gränssnittet).

- ***Försäkra dig om att portmappningen för DNS-förfrågningar har ställts in även om du kör DNS-servern på WinRoute-datorn! Mappa UDP-protokoll och port 53 till IP-adressen för Internetgränssnittet.***

DNS-server bakom WinRoute-dator

Du kan köra en verklig DNS-server på vilken dator som helst inom ditt lokala nätverk. För att göra det kommer du att behöva installera portmappning:

Protokoll: UDP

Avlyssnings-IP: ospecificerat eller den IP-adress som är associerad med DNS-servern (mappad som andra IP-adress)

Avlyssningsport: 53

Destinations-IP: den privata IP-adressen för datorn med DNS-servern

Destinationsport: 53

DNS-server och WWW bakom NAT

Om du kör din egen DNS-server och WWW-server på samma privata nätverk kan du behöva ställa följande frågor:

Hur hanterar jag DNS-förfrågningar för www.mydomain.com som kommer från mitt LAN, hur komme de att besvaras av webbserverns privata nätverks-IP-adress eftersom DNS-förfrågningar som kommer från Internet kommer att få en vanlig Internet- IP-adress associerad med www.mydomain.com?

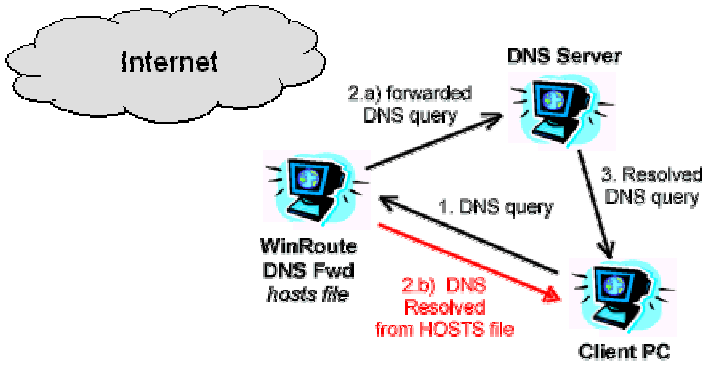
Lösningenär ganska enkel och du kommer att använda WinRoutes inbyggda **DNS-befordrare** för att lösa problemet. På alla klientdatorer ska du ställa in WinRoutes DNS-befordrare som DNS-server. På WinRoute-datorn ska du utföra följande inställningar:

- Slå PÅ WinRoutes DNS-befordrare
- Redigera HOSTS-filen:

  Lägg i HOSTS-filen till en uppgift som säger att www.mydomain.com är en specifik privat IP address (den där din webbserver körs - t.ex. 10.10.10.8). HOSTS-filen återfinns i roten på din windowskatalog (där Windows har installerats - c:\Windows or c:\win98 etc.). Du kan också komma till HOSTS-file från WinRoute DNS-befordrares dialog genom att klicka på knappen "Redigera HOSTS-fil".

Hur kommer det att fungera?

Alla DNS-förfrågningar som skickas av klientdatorerna från ditt LAN kommer först att upplösas av WinRoute DNS-befordrare. Alla förfrågningar kommer att kontrolleras mot uppgifterna i HOSTS-filen först. Om motsvarande registering hittar förfrågan kommer den att besvaras i detalj i sådana registreringar (privat IP-adress i vårt scenario).



Om det inte kommer at finnas någon registrering som motsvarar förfrågan i HOSTS-filen kommer förfrågan att kontrolleras ytterligare mot registreringarna i WinRoutes DNS-cacheminne (som ingår i WinRoutes DNS-befordrare). Om DNS-cacheminnet inte innehåller någon matchande registrering kommer förfrågan att sändas vidare till den DNS-server som har ställts in i WinRoutes DNS-befordrare för att skicka DNS-förfrågningar till.

Alla DNS-förfrågningar som kommer från Internet kommer att vidarebefordras baserat på portmappningens inställningar direkt till DNS-servern och upplösas baserat på sina registeringar.

- ***Obs! I ett sådant scenario kan du inte köra DNS-servern på samma dator som WinRoute. Det är för att båda tjänsterna - WinRoutes DNS-befordrare och din DNS-server skulle köra på samma port - UDP 53. Detta skulle orsaka fatala problem.***

DNS-problem

Att köra en webbserver (eller FTP etc.) och DNS-server på samma privata nätverk bakom WinRoute NAT

Det kan hända att du vill köra en webbserver med domänen www.mydomain.com bakom NAT och använda din DNS-server som kör på samma nätverk för samma upplösning.

Att köra en webbserver (eller FTP etc.) på WinRoute-datorn.

Om du kör en webbserver på WinRoute-datorn kommer du inte att få några som helst problem med lokala förfrågningar Alla DNS-förfrågningar www.whatever.com som kommer till din DNS-server kommer att besvaras av den vanliga Internet IP-adressen som är associerad med denna domän. En sådan IP-adress måste vara associerad med det nätverksgränssnitt som länkar från WinRoutes dator till Internet. WWW-servrarna kan lyssna på både allmänna och privata gränssnitt.

Om den lokala datorn skickar en DNS-förfrågan för att upplösa www.whatever.com får den en allmän IP-adress associerad med denna domän. Som ett resultat härav ansluter den webbservern till IP-adressen (som tilldelats Internetgränsssnittet så som beskrivits ovan).

Att köra en webbserver (eller FTP etc.) på en dator bakom WinRoute

Du kan vilja köra din webbserver på en dator bakom WinRoute (med en privat IP-adress t.ex. 10.10.10.8). Webbservern med www.mydomain.com finns rent fysiskt på en privat IP-adress 10.10.10.8 men din DNS-förfrågan kommer att upplösas med en vanlig IP-adress (som 206.86.181.25) som till följd därav associeras med denna domän.

Därefter kommer din webbläsare eller ftp-klient att vända sig till den allmänna adressen när ingen server körs eftersom webbservern finns inne i ditt nätverk.

Lösning

För att lösa denna fråga måste du använda WinRoutes inbyggda **DNS-befordrare** som DNS-server för dina datorer.

I **HOSTS-**filen ska du lägga till ytterligare en uppgift där du säger att **www.mydomain.com** opererar på den tillämpliga **interna** (privatklass) IP-adressen.Du kommer att låta DNS-befordraren titta på dina HOSTS-filer innan den skickar en DNS-förfrågan till den vanliga servern .

Varje gång någon användare skickar en begäran till **www.mydomain.com** kommer denna därefter att besvaras av lämplig lokal adress.

WWW-, FTP-, DNS- ochTelnetservrar bakom WinRoute

I denna avdelning

Att köra en WWW-server bakom NAT

För att köra webbservern bakom NAT:

1. Gå till menyn *Inställningar ->Avancerat ->Portmappning*
2. Lägg till ny portmappning:

   Protokoll: TCP

   Avlyssnings-IP: ospecificerat eller IP-adress associerad med domänen. En sådan IP-adress måste associeras med gränssnittet

   Avlyssningsport: 80

   Destinations-IP: mata in IP-adressen för WEBB-servern (t.ex.192.168.1.10)

   Destinationsport: 80

Användare som får tillgång till dessa tjänster kommer att få det med användnig av antingen domännamn eller allmän IP-adress för ditt nätverk. Sedan paketen nått WinRoute skickas de automatiskt vidare till den interna datorn med riktig intern IP-adress.

Att köra en DNS-server bakom NAT

WinRoutes inbyggda DNS-befordrare hjälper dig att vidarebefordra DNS-förfrågningar till en vanlig DNS-server för upplösning av domännamn. Den har kapacitet att upplösa lokala DNS-förfrågningar (vid användning av namnet på den lokala datorn). Emellertid måste DNS-förfrågningar sådana som *www.whatever.com* upplösas av den vanliga DNS-servern. WinRoutes **DNS-befordrare** kommer att **vidarebefordra** DNS-förfrågningar till **DNS-servern**.

Att köra DNS-servern bakom NAT (WinRoute)

För att köra DNS-servern bakom NAT/WinRoute måste du ställa in portmappning så som beskrivs nedan. DNS-servrarna kommunicerar med varandra via **UDP-**protokollen på **port 53**. Om du inte gör dessa inställningar kommer inte din DNS-server att vara funktionell. Du måste alltså göra denna inställning. När du kör DNS-servern på samma dator som WinRoute, utför WinRoutes inspektionsmodul NAT **INNAN** paketen når någon applikation, inklusive DNS-servern.

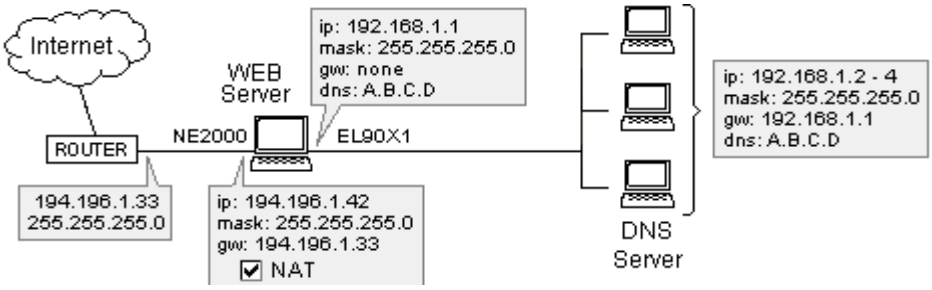
Protokoll: UDP

Avlyssnings-IP: ospecificerat eller allmän IP-adress för den DNS-server du vill köra

Avlyssningsport: 53

Destinations-P: allmän eller privat IP-adress för domännamnsserver

Destinationsport: 53



- ***Obs! Det är** inte möjligt **att köra en vanlig DNS-server på samma dators som WinRoutes DNS-befordrare. Båda tjänsterna använder UDP-protokoll port 53. Att köra båda DNS-tjänsterna på samma dator skulle orsaka fatala problem för IP-routingen. Emellertid kan du ställa WinRoutes befordrare på OFF om du vill köra DNS-servern på WinRoute-datorn.***

Att köra en FTP-server bakom NAT

Att köra en FTP-server bakom NAT:

1. Gå till menyn *Inställningar ->Avancerat ->Portmappning*
2. Lägg till ny **Portmappning**:

   Protokoll: TCP

   Avlyssnings-IP: ospecificerat eller IP-adress associerad med domänen. Sådan IP-adress måste vara associerad med Internetgränssnittet

   Avlyssningsport: 21

   Destinations-IP: mata in IP-adressen för FTP-servern (t.ex.192.168.1.10)

   Destinationsport: 21

Att köra en FTP-server med en port som inte är standard:

Justera portmappningen så att den matchar den port som används av FTP-servern.

Att köra en e-postserver bakom NAT

För att köra e-postserver bakom WinRoute rekommenderas det att du skapar två portmappningsuppgifter - en för SMTP-protokollet (som körs på port 25) och en för POP3- protokollet (som körs på port 110). Detta kommer att tillåta andra SMTP-servrar att nå din SMTP-server och du kommer också att kunna hämta din e-post vid POP3 från Internet.

Det är nödvändigt att sätta upp portmappning i det fall e-postservern körs på WinRoute-datorn. Detta på grund av positionen för WinRoutes inspektionsmodul som arbetar nedanför TCP-stacken så att paketen ändras/nekas innan de når operativsystemet.

SMTP-protokoll:

Protokoll: TCP

Avlyssnings-IP:

Avlyssningsport: 25

Destinations-IP: mata in IP-adress för SMTP e-postserver (t.ex. 192.168.1.10)

Destinationsport: 25

POP3-protokoll:

Protokoll: TCP

Avlyssnings-IP:

Avlyssningsport: 110

Destinations-IP: mata in IP-adressen för POP3 e-postserver (t.ex.192.168.1.10)

Destinationsport: 110

Att köra en Telnet-server bakom NAT

Telnet används i stor utsräckning av många företag för att manipulera data på avstånd. Särskilt AS400-servrar använder detta protokoll.

För att köra en Telnet-server bakom WinRoute är det nödvändigt att sätta upp portmappning för TCP protokoll på port 23. Inga inställningar krävs för att köra den Telnetklient som får tillgång til Telnet-servern på Internet.

Protokoll: TCP

Avlyssnings-IP: ospecificerat eller IP för Telnet-server

Avlyssningsport: 23

Destinations-IP: Mata in IP-adressen för Telnet-servern (t.ex.192.168.1.10)

Destinationsport: 23

FTP-problem vid användning av icke standardportar

I denna avdelning

Tillgång till FTP-server med icke standardportar

Om du befinner dig bakom WinRoute och försöker få tillgång till en FTP-server med ett portnummer annat än 21, kommer du inte att få någon kataloglistning. För att detta ska fungera måste du göra följande:

1. Gå till WinRoute-maskinen
2. Stäng av WinRoute-motorn
3. Gå till menyn Starta->Kör på skrivbordet
4. Skriv regedit för att hämta Registerredigeraren;
5. Sök HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Module/0
6. Modifiera SpecParams så att värdet blir det samma som portnumret för den FTP-server du skulle vilja få tillgång till
7. Slå åter på WinRoute-motorn.

Detta bör göra att alla bakom WinRoute kan få tillgång till en FTP-server på Internet med en port som inte är standard.

➢ ***Obs! Du kan ange flera portar genom att placera ett blanksteg mellan varje värde.***

FTP-server bakom WinRoute som använder en icke standardport

Under vissa omständigheter (till exempel en företgasklient bakom en brandvägg) kan en användare begränsas till tillgång till FTP endast i **passivt** modus. Om en FTP-server bakom WinRoute använder en port som inte är standard, kan ingen tillgång upprättas från **passivt** modus. Detta för att WinRoute (som standard) betraktar port 21 för FTP, så att om användaren önskar använda en annan port måste WinRoute justeras. Följande lilla procedur kommer att rätta till detta problem och ge tillgång också i **passivt** modus.

1. Gå till WinRoute-maskinen
2. Stäng av WinRoute-motorn
3. Gå till menyn Starta->Kör på skrivbordet
4. Skriv regedit för att hämta Regiserredigeraren;
5. Sök HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Mport. Du kan se undermappar där som innehåller information om portmappningar. Om det inte finns några undermappar, så finns det inga portmappningar.
6. Sök mappen med portmappningen baserad på port som används av FTP-servern
7. Ändra nyckeln *"flaggor"* till ‘1’
8. Ändra nyckeln *"NatApp"* till ‘FTP’
9. Slå åter på WinRoute-motorn.

Dessa inställningar kommer att "tala om för" WinRoute att de paket som kommer på den port du definierat kommer att tillhöra FTP-protokollet och av den anledningen kommer WinRoute att vidta ytterligare åtgärder när det gäller att låta detta komplexa protokoll passera genom.

Speciella nätverk

I denna avdelning

Token Ring-nätverk

Att ansluta Token Ring-nätverk

Token Ring är en mycket speciell typ av nätverk. Av den anledningen ugår vi från att endast professionella personer sysslar med Token Ring och går inte här in på någon detaljerad förklaring.

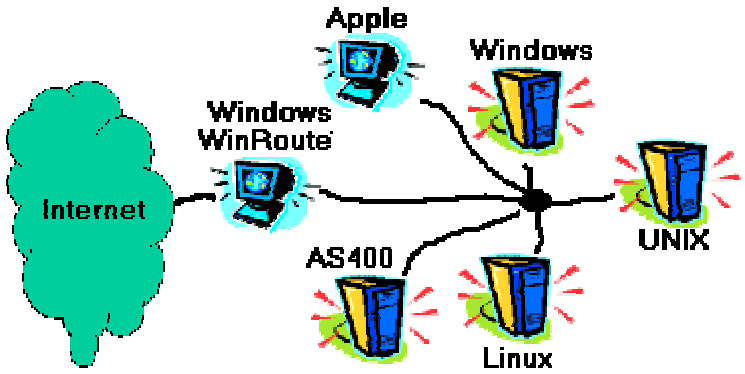
- Alla datorer inom Token Ring behöver MTU (maximum transmission unit) inställd på 1500
- På WinRoute-datorn går du till menyn Inställningar->Avancerat->Diverse alternativ och kontrollerar "Support för Token Ring-nätverk"
- Följ upp andra inställningsinstruktioner som är specifika för varje typ av Internet-anslutning

Multioperativ systemomgivning (Linux, AS400, Apple)

Att ansluta multipla operativsystemsomgivningar (Linux, Unix, AS400, Apple)

WinRoute är lämpad för anslutning av multipla operativsystemsomgivningar till Internet. WinRoute agerar som en mjukvarurouter. Som sådan stöder den alla standarder av TCP/IP-omgivning.

- ***OBS: Ett Windowsbaserat operativsystem måste vara värd för WinRoute-applikationen. Därför krävs det minst en Windows 95/98/NT-baserad dator i WinRoutes nätverk. Ett UNIX-system kan inte vara värd . Däremot kan UNIX operera som klientsystem.***



Att ansluta multipla nätverk

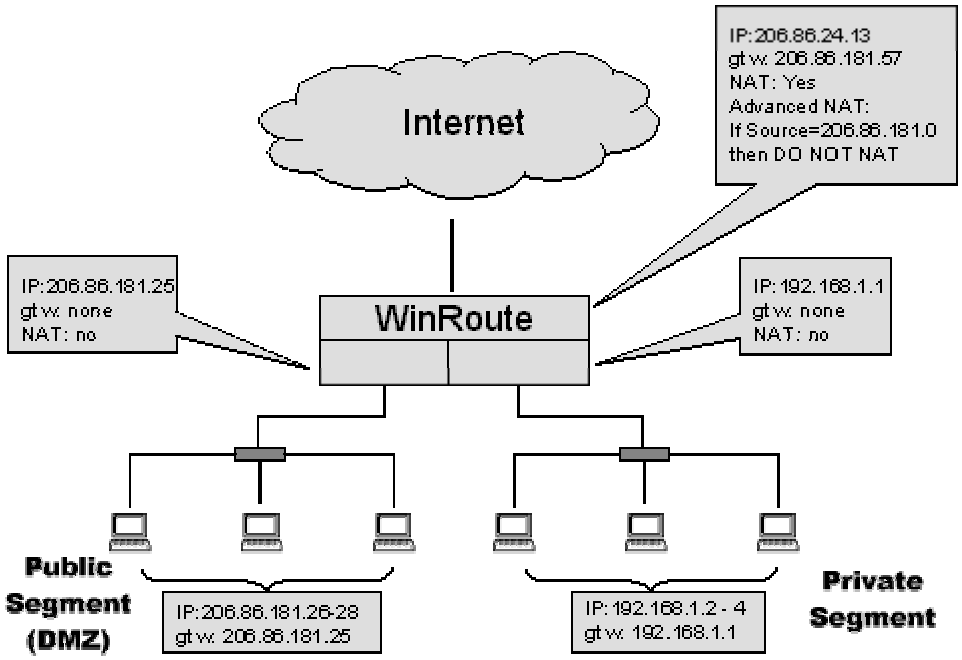
I denna avdelning

Att ansluta allmänna och privata segment (DMZ)

Ett privat segment består av datorer som använder privat typ av Internet-adresser. Sådana adresser är avsedda för privata nätverk och kan inte användas på Internet. Det är därför du behöver WinRoute som översätter dessa privata adresser till allmänna vilket ger dig en möjlighet att ansluta till Internet. Datorerna med privat adress är inte direkt tillgängliga från utsidan (Internet).

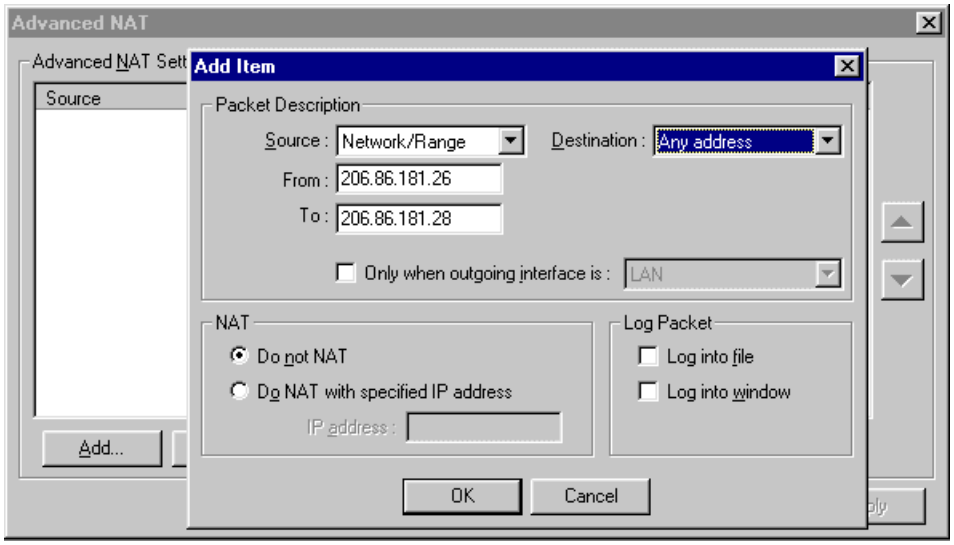
Ett allmänt segment består av datorer där varje dator har en allmän IP-adress. Dessa system kan vara direkt tillgängliga från Internet om dina säkerhetsregler tillåter det

Varje segment måste ha sitt eget nätverksgränssnitt i WinRoute-datorn. Då tillåter WinRoute-motorn dina privata och allmänna segment att dela på en Internetanslutning.



WinRoute-inställningar

Det är nödvändigt att utföra avancerade NAT-inställningar så att WinRoute inte kommer att utföra NAT för paket som går från det allmänna segmentet. För att göra detta går du till menyn Inställningar=>Avancerat=>NAT.



Allmänna och privata nätverksinställningar

Dessa nätverk kommer att sättas upp på samma sätt som beskrivits i andra delar av denna manual. För allmänna segment är den enda skilnaden att du kommer at använda allmänna IP-adresser på den. Se främst till att hålla följande regler:

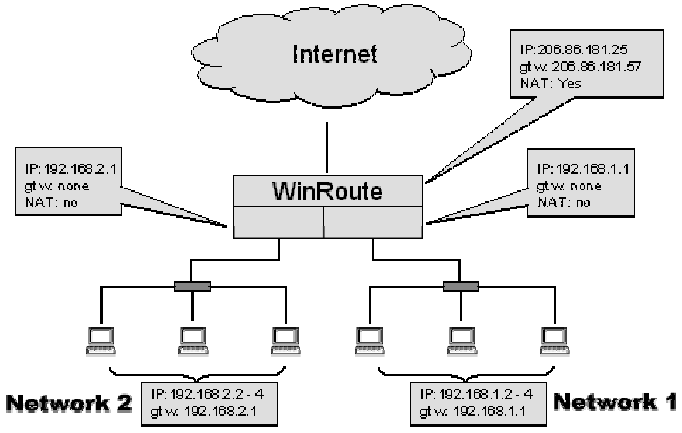
- INGEN standardgateway på gränssnitten i WinRoute
- IP-adressen för dessa gränssitt kommer att användas som standardgateway för resten av deras nätverk.
- INGEN NAT på gränssnitten i WinRoute

…se ***Checklista*** för ytterligare förklaringar

Två nätverk delar anslutning med en IP-adress

I det fall du har två nätverk anslutna till Internet via en dator som kör WinRoute finns det inga specifika inställningar att göra. I grunden finns det flera segment som leder till WinRoute-datorn, vart och ett har ett separat nätverksgränssnitt. I vårt exempel finns det tre nätverksgränssnitt på WinRoute-datorn:

- Internet-gränssnitt
- Gränssnitt för nätverk 1
- Gränssnitt för nätverk 2



De enda inställningar som det är nödvändigt att tänka på är:

Internet-gränssnitt

NAT är aktiverat
IP-adress är uppsatt i enlighet emd din ISP
Gateway är uppsatt i enlighet med din ISP

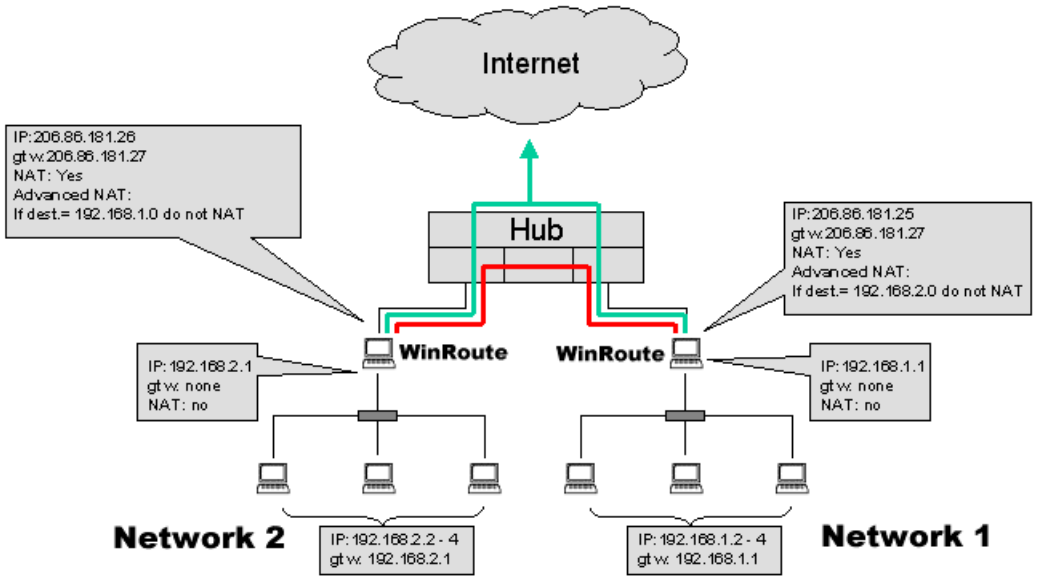
Interna gränssnitt

NAT är INTE aktiverat
Det finns INGEN standardgateway som satts upp på båda gränssnitten
IP-adress är inställd på intern typ (t.ex.192.168.1.1)

Övriga inställningar är de samma som de som beskrivits i andra avdelningar av denna manual. Den trafik som kommer från varje undernät routas till det andra undernätet eller till Internet och vice versa.

Två nätverk delar anslutning med två IP-adresser

Du kan vilja dela en Internettillgång mellan två nätverk när varje nätverk befinner sig bakom separat allmän IP-adress. Samtidigt kan du vilja ha tillgång till datorerna i båda de privata nätverken.



Då är det MYCKET viktigt när du utför följande routing-scenario:

- UTFÖR INTE NAT med alla paket som går till det andra nätverket.
- UTFÖR NAT med alla paket som går till Internet

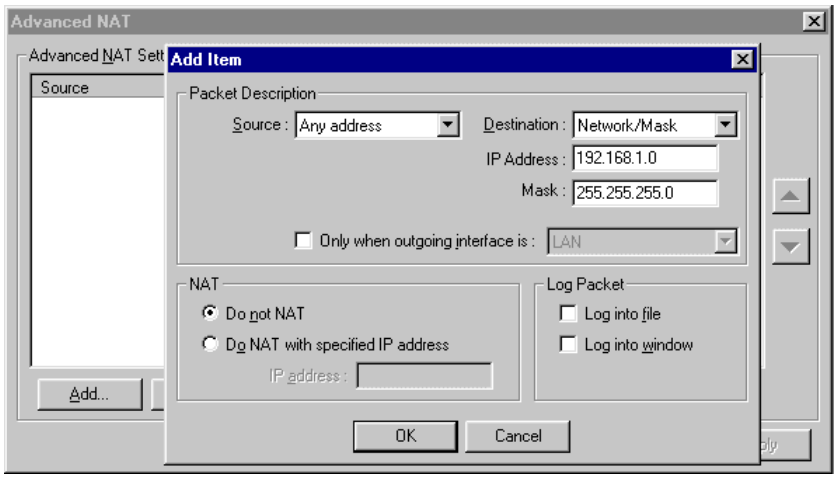
Med andra ord så kommer WinRoute att utföra NAT baserat på destinationen för passerande IP-paket. Paket som går till fjärrnätverket kommer inte att ändras medan paket som går till Internet NATas fullt och helt.

Router eller nav?

Grundat på dina behov måste du bestämma om du önskar ha en router mellan dina nätverk eller om ett nav skulle vara tillräckligt. I vårt scenario finns det ett nav som ger tillräckligt med funktionalitet för att tillåta två nätverk att dela på en (höghastighets-) Internet-anslutning.

För att ställa in WinRoute på att inte utföra NAT grundat på paketets destination:

1. Gå till menyn Inställningar->Avancerat->NAT.
2. Mata in destinationskriterier - vanligen undernätet eller område av IP-adresser
3.Välj alternativet "Utför inte NAT"



Tips: När du ställer in avancerat NAT kommer du att hitta ett annat alternativ som säger att NAT inte ska utföras baserat på ursprunglig IP-adress. Denna inställning kan vara användbar när du vet vilka arbetsstationer som inte kommer att behöva tillgång till Internet. Du kan då hellre än att ställa in kriterier för brandväggen hitta en annan lösning i de avancerade NAT-inställningarna.

Om du inte utför NAT med specifika paket, dvs. källan skulle kvarstå som den interna IP-adressen, kommer de aldrig att få några svar tillbaka. Med andra ord en sådan användare kan försöka ansluta till Internet i all evighet utan ha en chans att få tillgång till det.

Server för fjärrtillgång (inringning och tillgång till Internet)

Lösning för Remote Access Server

Ibland kan det vara nödvändigt att få tillgång till ditt företagsnätverk från världen utanför via telefon och använda denna tillgång till Internet. WinRoute ger denna funktion på WindowsNT med RAS-tjänster installerade och konfigurerade.

Det finns specifika regler som måste tillämpas:

- Ditt företagsnätverk har ett undernät (t.ex. 192.168.1.0)
- WindowsNT DHCP-server ger användare som kommer genom RAS IP-adresser från ett annat undernät (t.ex. 192.168.2.0)
- NAT kommer att utföras endast på det gränssnitt som leder till Internet

Med andra ord, det nätverkskort (NIC) som leder till ditt lokala nätverk måste ha IP-adress från ett undernät (t.ex. 192.168.1.1) medan den användare som ansluter till din server via RAS måste få en IP-adress från ett annat nätverk (t.ex. 192.168.2.1). WinRoute agerar som router - det kan routa paketen mellan två eller flera gränssnitt från olika nätverk - inte från samma.

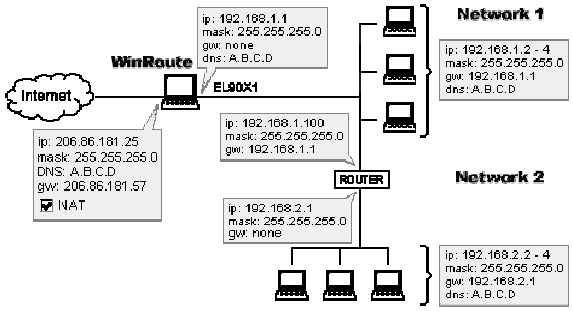
Denna typ av installation speglar den för en liten ISP. WinRoute begränsar inte antalet användare som samtidigt får tillgång till din NT-server. Så länge som din NT-server lämnar fjärranvändares IP-adresser från olika undernät (andra än huvudnätverket) begränsar det antal RAS-gränssnitt du har installerat antalet användare.

Att ansluta kaskadkopplade segment via 1 IP-adress

Nätverksuppsättningen där alla nätverk som ska anslutas inte leder direkt till WinRoute-datorn medan de ansluts genom en router kallas Cascaded Segments.

Figure 1: Connecting cascaded segments to the Internet

Routern mellan de två nätverken kan vara vilken hårdvarurouter som helst, WindowsNT eller någon Windows 95/98-dator med WinRoute. WinRoute kommer at agera som router med eller utan utförande av NAT.



I allmänhet är det nödvändigt att "tala om för" WinRoute-datorn dit de inkommande paketen till de andra nätverken kommer att sändas, medan det för de utgående paketen måste finnas en liknande länk på routern (som delar på två nätverk) som specificerar vart paketen som utgår från det andra nätverket ska skickas. Detta kan göras genom att lägga till nya routes - en vid WinRoute-datorn (för inkommande paket) och en för routern (för utgående paket).

- ROUTE vid WinRoute-datorer (medlem av nätverk 1) kommer att routa IP-paket till det andra nätverket (nätverk 2) till den routerns specifika IP-adress för nätverk 1. Denna router kommer at vidarebefordra dessa paket.
- STANDARDROUTE vid routern (som ansluter de båda nätverken) kommer att routa alla paket som kommer från nätverk 2 till Win Route-datorns IP-adress för nätverk 1. Sedan kommer WinRoute att förse dessa paket med NAT och skicka dem till Internet.

Exempel

Vårt exempel har två nätverk 192.168.1.x och 192.168.2.x., routern är vid 192.168.1.100.

Obs! Som router kan du använda vilken hårdvarubaserad router som helst men också någon Win95/98-dator med WinRoute eller WindowsNT.

Inställningar för nätverk 1 (primärt nätverk)

- Du måste tala om för WinRoute-datorn : "Alla paket som går till nätverk 192.168.2.0 måste gå genom routern 192.168.1.100":
- 1. Gå till MS-DOS-prompten
- 2. Mata in följande kommando:

```
Route -p add 192.168.2.0 mask 255.255.255.0
192.168.1.100
```

- På routern 192.168.1.100, måste standardrouten leda till datorn med WinRoute, dvs.. 192.168.1.1. Med andra ord , du måste säga till din router att routa alla paket som går till Internet genom WinRoute-datorn.

- Alla andra nätverksinställningar ska göras så som beskrivits i övriga kapitel (Sätta upp nätverk).

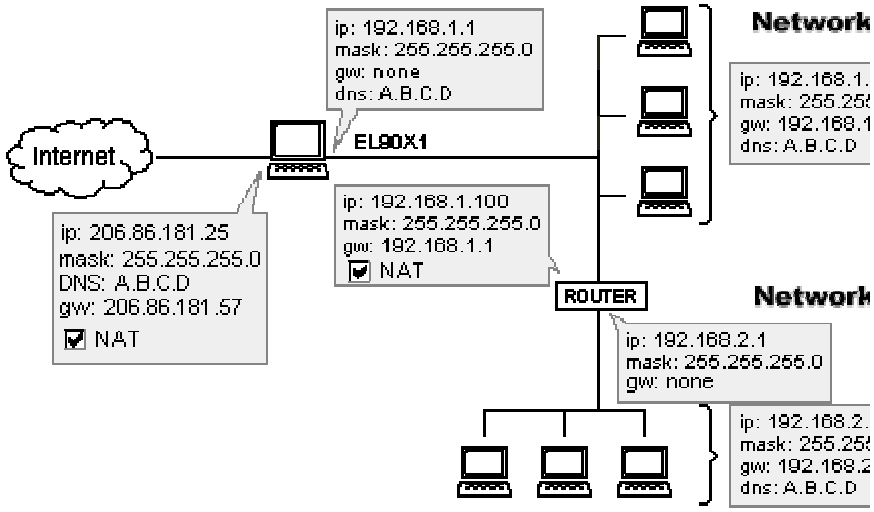
Inställningar för nätverk 2 (sekundärt nätverk)

Alla inställningar är vanliga inställningar där nätverk 2 kommer att vara det självständiga nätverket. Standardgateway på alla nätverk 2-datorer ställs till routerns IP-adress för nätverk 2 (192.168.2.1 i vårt exempel).

NAT mellan nätverk 1 och nätverk 2

Du kan använda WinRoute med NAT ställt "PÅ" för att ansluta det primära och det sekundära nätverket. Det sekundära nätverket kommer att se ut som en enstak dator så du kommer att dra nytta av lättare administration och högre säkerhet för det sekundära nätverket. Du bör ställa in avancerade NAT-inställningar ordentligt eftersom du inte skulle tycka om att behöva modifiera trafiken mellan dessa två nätverk.

Figure 2: Connecting cascaded segments to the Internet



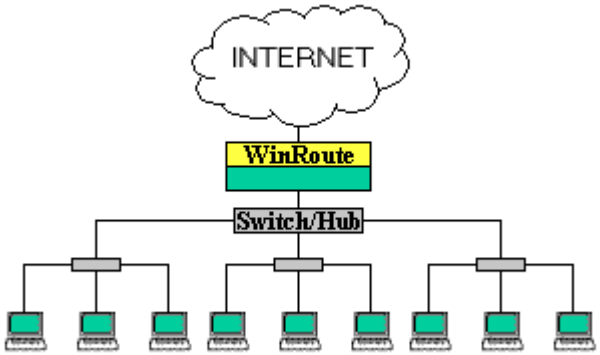
Avancerade NAT-inställningar på den WinRoute-dator som delar nätverk 1 och nätverk 2

Grundat på destinationens IP-adress kommer du eller kommer du inte att utföra NAT. I vårt exempel, om paketens destination ligger på nätverk 192.168.1.0 så kommer paketen inte att NATas. Detta kommer att tillåta kommunikation mellan dessa två nätverk som om det inte funnes någon NAT.

För nätverksinställningarna följ de regler som beskrivs i resten av denna manual.

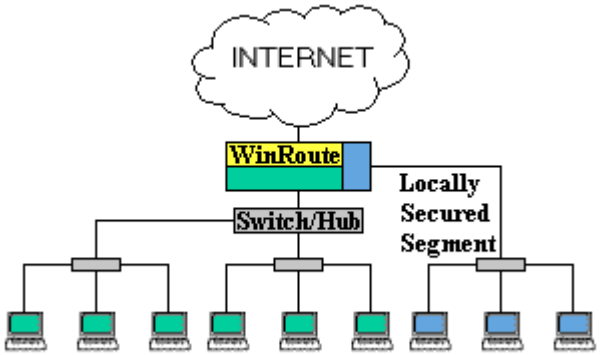
Ethernet-adapters med flera portar

Av de 170 000 eller fler nätverk som i dagsläget litar på WinRoute Pro som sin router/brandväggslösning inbegriper den vanligaste konfigurationen två kort för nätverksgränssnitt (NIC), en till Internet och den andra till ett lokalt nätverk (LAN). Denna grundkonfiguration filtrerar paket som går till och från Internet; emellertid kan den inte filtrera paket som går mellan lokala segment eftersom den trafiken inte passerar genom WinRoute. Ett exempel på denna konfiguration illustreras nedan i figur 1.



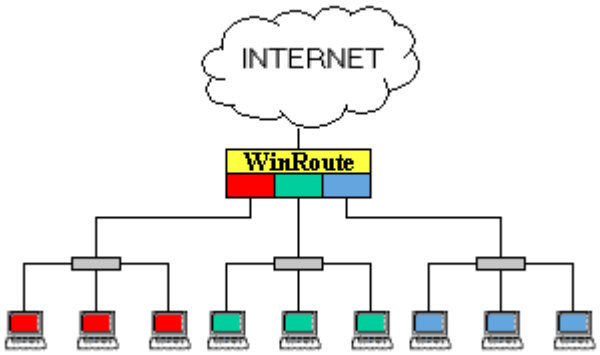
Figur 1. Den vanligaste konfigurationen av WinRoute Pro.

I en del fall kommer ett tredje NIC att läggas till WinRoute-maskinen vilket tillåter ett separat, säkrat segment. I ett sådant scenario filtreras paket som går ut och in i det säkrade segmentet, både från Internet och från andra lokal segment, genom WinRoute och ger en extra säkerhetsnivå.



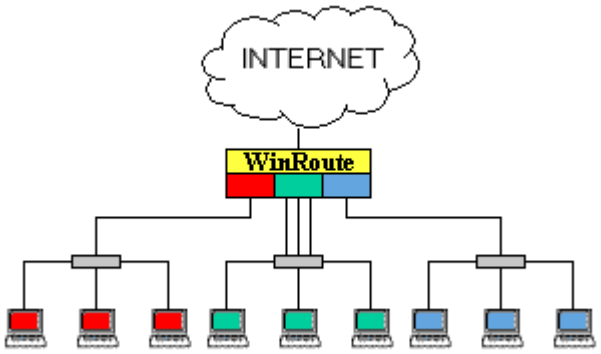
Figur 2. Ett separat segment till LAN kan läggas till genom att använda ett tredje NIC.

För större nätverk som kan ha flera separata segment med sina egna unika säkerhetspolicies, uppstår det problemet att antalet av sådana separata segment begränsas till antalet portar på WinRoute-maskinen. På grund av detta krävs extra hårdvara för lämpliga ytterligare routing/omkopplings- och säkerhetspolicies. Med den senaste introduktionen av Ethernet med många portar för NIC får WinRoute en möjlighet att bli nätverktrafikens enda kontrollant. Eftersom kort för flera portar kan ge WinRoute-maskinen mer än 24 portar beroende på antalet kortplatser på moderkortet, WinRoute-maskinen kan alltså vara, router, omkopplare, domänkontrollant etc. På så vis kan styrningen av nätverket centraliseras och kontrolleras från en enda punkt. Figur 3 illustrerar hur WinRoute Pro använder ett Ethernet-NIC med flera portar för att kontrollera tre separata nätverk.



Figur 3. WinRoute Pro utrustat med Ethernet-NIC med många portar.

Förutom ökad säkerhet och centraliserad ledning som fås genom Ethernet-NIC med flera portar, finns det ytterligare fördelar som belastningsbalans och haveriskydd. Lägg märke till tilldelningen av tre portar till det mellersta segmentet i Figur 4.



Figur 4. Mittsegmentet tilldelas tre portar för portsamling.

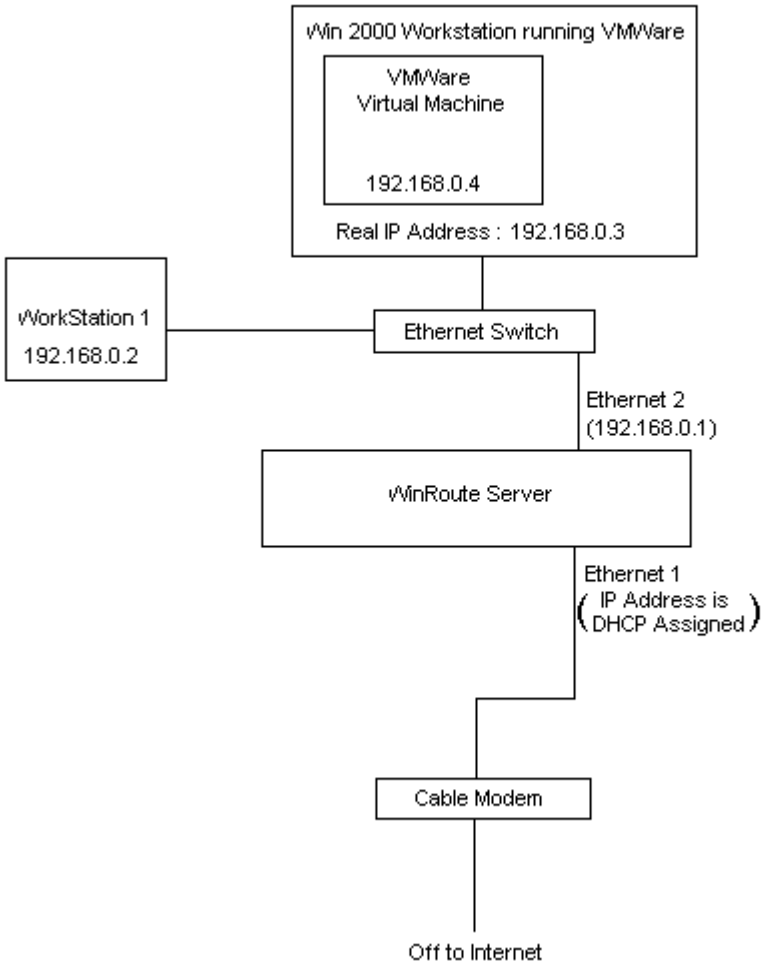
Belastningsbalans kan åstadkommas genom samlade portar. På bilden ovan till exempel har det mellersta nätverkssegmentet fått sig tilldelat tre portar. Om detta segment använder en omkopplare för att ansluta till WinRoute-maskinen kan var och en av de tre maskinerna hämta data vid 100 Mbps. De andra två segmenten kan endast hämta ett sammanlagt antal av 100Mbps eftersom endast en port från det segmentet är förbunden med WinRoute-maskinen. En bonusfunktionalitet av portsamling är skyddet mot porthaveri. Om en linje avbryts kommer trafiken att omroutas genom nästa tillgängliga port.

Användning av NICmed flera portar tillsammans med WinRoute kan ge ett verksamt, men mycket effektivt, multirouting-system till ett mycket bekvämare pris, allt under ett enda administrativt paraply. WinRoute har nyligen med framgång testats med **D-Link 4 port DFE 570 TX** och **Adaptec 2 port Duralan ANA-62022**. Inga andra kort har testats.

Det bör noteras att denna typ av nätverksdesign kräver olika undernät för varje nätverkssegment som är förbundet till WinRoute-maskinen.

VMWare

VMWare är en applikation som kan tävla med den PC som den är installerad på ända ner till nivån för hårdvara. För nätverket ses denna virtuella dator som en fullständigt separat enhet. Eftersom den virtuella datorn har sina egna nätverksegenskaper , kommer WinRoute att räkna den virtuella maskinen som ytterligare en dator.



KAPITEL 4

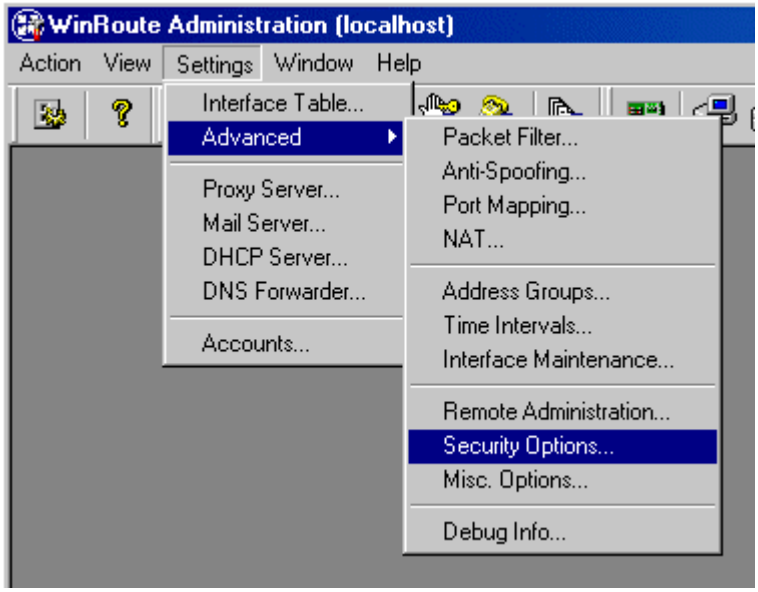
BRANDVÄGGSKONFIGURATION

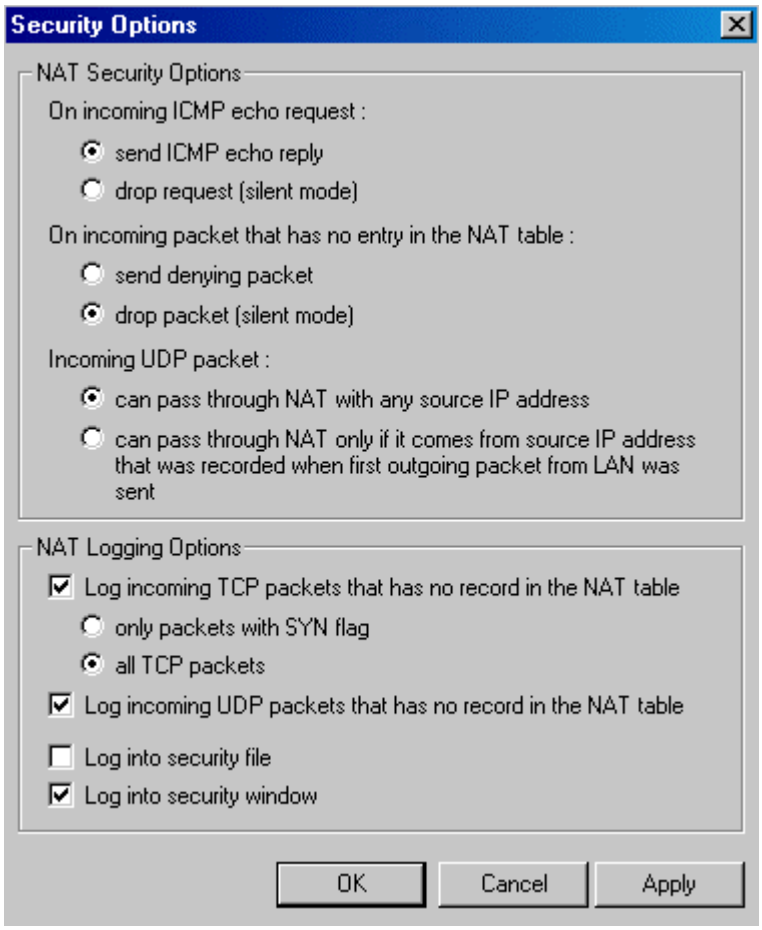
I detta kapitel

Hitta rätt porttilldelning

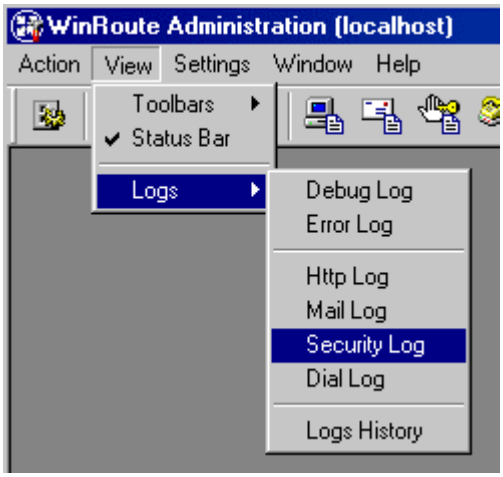
➢ ***Om du har modell 19 eller högre>***

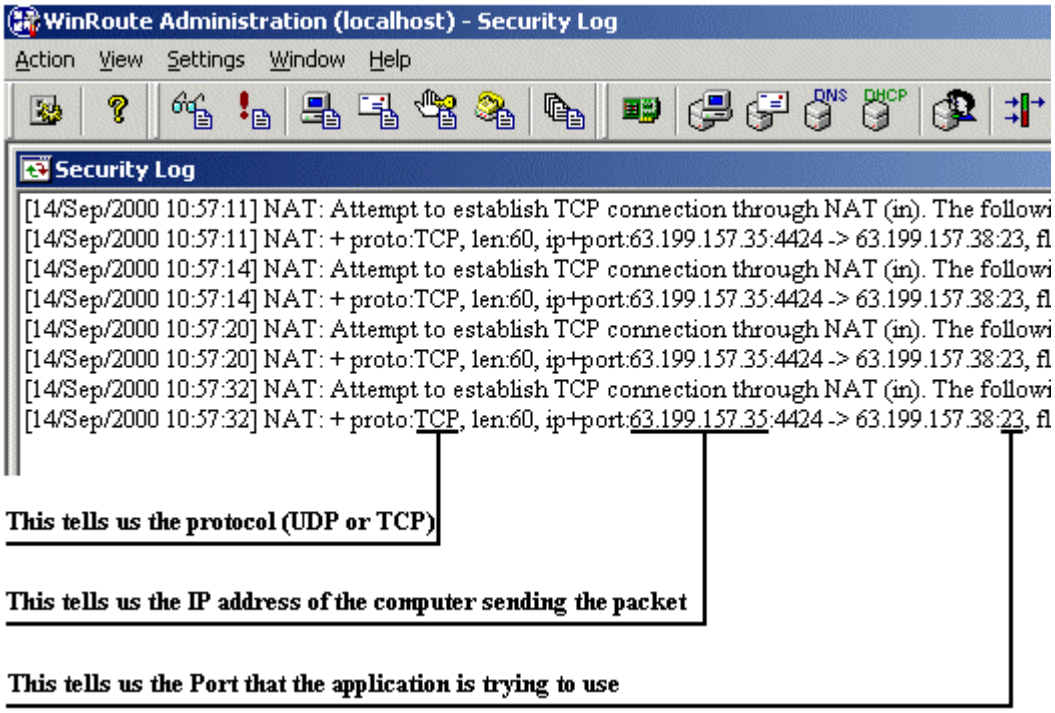
I administrationsfönstret väljer du Inställningar-> Avancerat-> Säkerhetsalternativ




Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Längst ner i fönstert för säkerhetsalternativ finns det några loggningsalternativ. Aktivera loggningen av TCP- och UDP-paket som inte är kända av NAT-tabellen till säkerhetsfönstret. Detta kommer att logga endast paket som initierats från utsian av WinRoute. WinRoute kommer att släppa dessa paket såvida inte portmappning utförs. Eftersom detta är ett begränsat villkor för loggning kommer vi endast att se ett urval av paket så det blir lättare att hitta det paket vi letar efter. Nästa steg är att öppna säkerhetsloggen från Visa-> loggmeny.





I detta fall skickar en dator vid 63.199.157.35 ut ett paket från port 4424 till en dator vid 63.199.157.38 och port 23. Port 23 är standardporten för Telnet. Om du hade haft en telnetserver som kördes på någon privat adress som 192.168.1.3 skulle den lyssna på port 23. Därför skulle du mappa TCP-paket på port 23 till 192.168.1.3.

Meddelande- och telefonitjänster

Det finns för närvarande flera Instant messaging-tjänster som stöder filöverföring för chat såväl som dator til dator eller dator till telefon. WinRoute Pro har testats framgångsrikt med följande konfigurationer för **AOLs instant messenger**, **Yahoo instant messenger**, **MSN Messenger** och **ICQ**.

AIM kräver inte några specifika inställningar. Använd standardanslutningens inställningar och försäkra dig om att du inte specificerar att du använder en proxyserver.

Yahoo IM-användare måste ändra inloggningspreferenserna -> anslutning till "Ingen nätverksdetektering". Alla Yahoo IM-tjänster bör fungera ordentligt bakom NAT med denna inställning.

MSN Messenger fungerar bäst om du använder HTTP-proxy. Aktivera WinRoutes proxy på standardporten 3128 (samtidigt med Network Address Translation). Dator till dator-chat fungerar för närvarande inte bakom WinRoute; däremot fungerar dator till telefon.

ICQ fungerar i de flesta fall med standardinställningarna för den **senaste** versionen. Om det uppstår komplikationer när du använder filöverföring rekommenderar vi att du använder den HTTPS-proxy som åtefinns i Preferenser -> anslutningar -> server och brandvägg. Aktivera WinRoutes proxy på standardporten 3128 (samtidigt med Network Address Translation).

Obs: Du ska inte behöva mappa några portar för några som helst av dess applikationer.

H.323 - NetMeeting 3.0

WinRoute inbegriper stöd av H.323-protokoll. Det betyder att alla applikationer med voice-over-IP kan kommunicera genom WinRoute. Sådana applikationer är Microsoft NetMeeting, CuSeeMee, Internettelefoni (du kan till exempel köra Siemens IP-telefoni genom WinRoute) och andra.

Om kommunikationen initieras från ett ställe bakom WinRoute

I ett sådant fall krävs inga inställningar. Winroute kommer att stödja praktiskt taget obegränsat med samtidiga anslutningar.

Om kommunikationen upprätta från Internet till datorn bakom WinRoute

I ett sådant fall är det nödvändigt att skapa portmappning, med andra ord att tala om för Winroute vart det ska routa inkommande H.323-paket. Du måste sätta upp följande portmappning:

Protokoll:	TCP
Avlyssnings-IP:	ospecificerat för den IP-adress som används för H.323-kommunikation i fall av multihome-system
Avlyssningsport:	1720
Destinations-IP:	LANs IP-adress för H.323-applikationen
Destinationsport:	1720

H.323-protokollet körs inte på port 1720 enbart - WinRoute kommer att lägga till de andra anslutningarna automatiskt. På grund av H.323-protokollets begränsning kan endast en arbetsstation åt gången använda sig av sådan kommunikation.

IRC - Internet Relay Chat

Det är inga speciella inställningar som krävs för att köra IRC-klienten. Till och med DCC (Direct Chat/Send(Receive)-filer) kommer att fungera automatiskt om du använder standardport 6667 på ditt IRC.

För att köra IRC-servern bakom NAT var vänlig mappa följande portar:

Protokoll: TCP

Avlyssnings-IP: ospecificerat eller den IP du vill använda för IRC-servern

Avlysnningsport: 6667

Destinations-IP: IP-adress för datorn med din IRC-server

Destinationsport: 6667

Om du använder något annat än standardporten kommer det att göra att DCC inte fungerar.

CITRIX Metaframe

WinRoute stöder fullständigt **CITRIX Metaframe**-protokollet. För att få tillgång till en CITRIX Metaframe-server som körs innanför WinRoutes nätverk från Internet måste du utföra följande portmappning:

För CITRIX Metaframe:

Protokoll: TCP

Avlyssnings-IP: ospecificerat eller allmän IP-adress som du vill att servern ska använda

Avlyssningsport: 1494

Destinations-IP: privatklass IP-adress för servern innanför nätverket

Destinationsport: 1494

Du kan skapa mappade portar och ha tillgång till flera servrar samtidigt. För att göra detta kommer du att på klientdatorn behöva förinställa vilken port de ska använda för tillgång till servern. Detta kan specificeras i klientens .ini fil - när du skapar anslutningsikonen.

MS Terminal Server

WinRoute stöder fullständigt **MS Terminal Server** -protokoll. För att från Internet få tillgång till en MS Terminal-server som körs innanför WinRoutes nätverk kommer du att behöva utföra följande portmappning:

För MS Terminal-server:

Protokoll: TCP

Avlyssnings-IP: ospecificerat eller allmän IP-adress som du vill att servern ska använda

Avlyssningsport: 3389

Destinations-IP: privatklass IP-adress för servern innanför nätverket

Destinationsport: 3389

Du kan skapa flera mappade portar och få tillgång till fler servrar samtidigt. För att göra detta kommer du att på klientdatorn behöva förinställa vilken port de ska använda för att få tillgång till servern. Detta kan specificeras i klientens .ini fil - när du skapr anslutningsikonen.

Internettelefoni - BuddyPhone

WinRoute är branschens första mjukvara för router/firewall som för upp Internet-telefonin på riktig affärsnivå. BuddyPhone gör att du kan placera om ett samtal via Internet från ett nätverk till ett annat.

Stödet för BuddyPhone fungerar bäst med ICQ. Registrera denna kostnadsfria mjukvara för instant messenger och du kommer att kunna njuta av "one-touch-button"-operationer när du ringer dina vänner.

Alla användare som är aktiva i din ICQ-buddy list kommer att finnas med i din BuddyPhone telefonkatalog och att placera ett samtal är lika lätt som att välja en sådan användare i listan.

Inga inställningar krävs så länge du använder BuddyPhone och ICQ tillsammans.

Att använda BuddyPhone utan ICQ

WinRoute kan leda de samtal som kommer från Internet till rätt mottagre i det lokala nätverket baserat på porten.

Använd portarna 710 och uppåt för att tilldela de lokala användarna deras egna portar.

Exempel:

Du har tre användare i ditt LAN som använder BuddyPhone.

Användarens namn	Användarens interna IP-adress	Port tilldelad användaren
John	192.168.1.2	710

Quido	192.168.1.3	711
Bob	192.168.1.4	712

Sedan ska du ställa in portmappningen:

Avlyssningsport	Destinations-IP	Destinationsport
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

Placeringen av telefonsamtal till användaren kommer att vara lika lätt som att mata in company.com:port# i BuddyPhones dialog för direktuppringning. Till exempel sales.gamerouter.com:711.

- ***Obs! Det är inte fel i vår dokumentation! Destinationsporten är verkligen 700. Det är det portnumer som BuddyPhone använder för att arbeta. WinRoute kommer att ge routing baserat på avlyssningsport.***

CU-YouSeeMe

Följande portmappning är nödvändig för att ta emot **CU-SeeMe**-samtal genom NAT:

Protokoll: UDP

Avlyssnings-IP: <ospecificerat>

Avlyssningsport: 7648

Destinations-IP: IP-adressen för den arbetsstation som kör CU-SeeMe-klienten

Destinationsport: 7648

Protokoll: UDP

Avlyssnings-IP: <ospecificerat>

Avlyssningsport: 7649

Destinations-IP: IP-adressen för den arbetsstation som kör CU-SeeMe-klienten

Destinationsport: 7649

Begränsningar:

- För närvarande är det inte möjligt att köra mer än en CU-SeeMe-klient på det lokala områdesnätet
- Det är inte möjligt att ansluta till en "reflektor" som skyddas av ett lösenord.

Fjärrtillgång - PC Anywhere

I denna avdelning

PC Anywhere

WinRoute innefattar bästa möjliga support för Symantecs PC AnyWhere för alla mjukvarurouters på marknaden. PC AnyWhere gör att användaren kan få tillgång till och styra datorer innanför nätverket . För att göra detta måste du tillämpa följande scenario:

1. Styrd dator kommer att köra PC Anywheres värd.
2. Fjärrdator kommer att köra PC Anywhere Remote
3. Portmappningen på WinRoutes dator kommer att konfiguereras på följande sätt:

   Protokoll: TCP/UDP

   Avlyssnings-IP: ospecificerat

   Avlyssningsport (område): 5631-5632

   Destinations-IP: IP-adressen för PC Anywhere värden innanför ditt nätverk (t.ex.192.168.1.12)

   Destinationsport: 5631-5632

Säkerhetsproblem

För att öka säkerheten och för att undvika att öppna ditt nätverk för världen utanför tillåter WinRoute användarna att välja en specifik IP-adress från vilken tillgången är tillåten genom vissa portar. Denna konfiguration gör att endast vissa datorer eller nätverk får tillgång till ditt system från Internet.

För att installera datorer som är tillåtna att få tillgång till ditt nätverk måste du först definiera en adressgrupp (även om du går in i bara en enda dator). För att konfigurera detta gå till menyn Inställningar=>Avancerat=>Adressgrupper.

Att ändra tillgången mellan olika datorer

Du kan sätta upp adminsitratörsrättigheter i WinRoute för att möjliggöra anslutning direkt till WinRoute-värden. När du ändå är i värddatorn kan du ändra destinations-IP i portmappning och direkt tillgång till den dator du väljer. Häpnadsväckande!

PC Anywhere gateway

Att köra pcAnywhere i gateway-modus på WinRoutes brandvägg kommer att tillåta fjärrklienten att hämta tillbaka en lista över tillgängliga pcAnywhere-värdar som körs bakom brandväggen. Med hjälp av denna lista kan du styra vilken som helst av pcAnywhere-värdarna bakom WinRoutes brandvägg.

Dessa steg utgår från att du använder pcAnywhere 9.0 och inte filtrerar några inkommande/utgående paket vid WinRoutes brandvägg

- Hanterade datorer bakom WinRoutes brandvägg kommer att köra PC Anywhere Host med användning av TCP/IP
- Fjärrdator kommer att köra PC Anywhere Remote med användning av TCP/IP
- pcAnywhere har installerats på WinRoutes brandvägg med användning av gateway-modus. När du konfigurerar gateway-apparaten ska både den utgående och den ingående apparaten ställas in på TCP/IP

- På WinRoutes brandvägg måste pcAnywhere konfigureras för att lysna på det interna NIC (t.ex.192.168.1.1). Anvisningar om hur man konfigurerar pcAnywhere för att lyssna på en specifik IP-adress/NIC kan hittas på Symantecs webbplats
- Lägg till den/de specifika IP-adressen/erna för de datorer som ska hanteras i Nätverksalternativ för pcAnywhere. För att scanna hela undernätet använd 255 som sista oktett (192.168.1.255).
- Konfigurera portmappningen i WinRoute på detta sätt:

  Protokoll: TCP/UDP

  Avlyssnings-IP: externt NIC (206.86.181.25)

  Avlyssningsport: OMRÅDE (5631-5632)

  Destinations-IP: internt NIC (192.168.1.1)

  Destinationsport: 5631-5632

Spelavdelning

I denna avdelning

Om att köra spel bakom NAT

Att spela spel

Många spel stöder idag en multianvändaromgivning. Användare kan tävla med varandra över Internet och LAN eller de kan också gå med i en av de spelservrar som finns på Internet. Användare kan också ha en egen spelserver och låta vänner, familj eller fullständiga främlingar njuta av den spänning det är att spela spel tillsammans.

Det finns många spel som inte kräver några inställningar alls i WinRoute. Innan man försöker konfigurera WinRoute för ett specifikt spel rekommenderar vi dig att först köra spelets demo-version. I olikhet med proxyservrar stöder WinRoutes grundläggande konstruktion många spel direkt "från hyllan."

Vissa spel kräver att en viss port konfigureras i WinRoute för att de ska fungera och kunna köras. Portar används för ytterligare identifiering av den spelare som sitter vid spelservern (i allmänhet).

Om spelet har en specifik port associerad till sig är detta inte något problem för WinRoute! Konfigurera bara WinRoutes portmappning att vidarebefordra paket som kommer till ditt nätverk till spelarens dator bakom brandväggen.

Vilka portar som används varierar från spel till spel. Var vänlig se den dokumentation som kommer med varje spel eller ring spelförsäljarens tekniska support för ytterligare information. Denna manual innehåller endast ett antal exempel på inställningar för de mest populära spelen.

Aasheron's call

Asheron's call är ett populärt spel på Microsoft Gaming Zone. För att spela detta spel från datorn bakom GameRouter måste du utföra följande portmappningsinställningar:

1. Gå till menyn *Inställningar->Avancerat->Portmappning*
2. Utför följande inställningar:

Namn:	S1	S2	S3	S4	S5
Portnummer:	2300-2400	9000-9013	6667	28800 - 29000	
Destinations-IP:	IP för datorn med spelet	IP för datorn med spelet	IP för datorn med spelet	IP för datorn med spelet	IP f med
Protokoll:	TCP/UDP	UDP	TCP	TCP	

Battle.net (Blizzard)

Följande portmappning måste ställas in för att du ska kunna spela spel på battle.net. Endast en spelare kan spela vid samma tillfälle.

Protokoll: TCP/UDP

Avlyssnings-IP: ospecificerat

Avlyssningsport 6112

Destinations-IP: IP- -adressen för spelarens dator (t.ex.192.168.1.6)

Destinationsport: 6112

Half-Life

Half-Life

Protokoll: TCP/UDP

Avlyssnings-IP: ospecificerat

Avlyssningsport: 27015

Destinations-IP: IP-adressen för spelarens dator (t.ex. 192.168.1.6)

Destinationsport: 27015

MSN Gaming zone

Följande konfiguration måste testas noggrant med MechWarior3 på **MSN Gaming Zone**. Endast en maskin åt gången kan få tillgång till MSN.

1. G till menyn *Inställningar->Portmappning*
2. Lägg till ny portmappning

   Protokoll: TCP

   Avlyssnings-IP: "ospecificerat"

   Avlyssningsport: område 2300 till 2400

   Destinations-IP: den lokala IP-adressen för den maskin som du vill ansluta till MSN

   Destinationsport: område 2300 to 2400
3. Lägg till ytterligare en portmappning

   Protokoll: UDP

   Avlyssnings-IP: "ospecificerat"

   Avlyssningsport: område 28800 till 28912

Destinations-IP: den lokala IP-adressen för den maskin som du vill ansluta till MSN

Destinationsport: område 28800 till 28912

Quake

Quake 3

Quake 2/3-klienter

Inga speciela inställningar är nödvändiga

Quake 2/3-server

För masterservern:

Protokoll: UDP

Avlyssnings-IP: ospecificerat

Avlyssningsport: enkel 8002

Destinations-IP: x.x.x.x

Destinationsport: 8002

För klienter som ansluter till Quake3 Arena-server:

Protokoll: UDP

Avlyssnings-IP: ospecificerat

Avlyssningsport: enkel 27960

Destinations-IP: x.x.x.x

Destinationsport: 27960

StarCraft

Att spela StarCraft

WinRoute Pro innehåller unik support för alla StarCraft-spelare (Blizzard Entertainment). Flera spelare på nätverket som är anslutet till Internet genom WinRoute Pro kan ha kul med att spela spelet mot sina virtuella "fiender" på Internet.

För närvarande fungerar full automatisk support endast i det fall att alla spelarna går in i spelet från ett och samma nätverk på datorer bakom WinRoute Pro och inte på värddatorn.

För fler uppgifter gå till www.tinysoftware.com

Extra mappningar för några vanliga spel/apps

Nödvändiga portar för olika applikationer

Age of Empires II - 2 portmappning nödvändig

Protokoll: TCP

Källans IP: ospecificerat

Källans port: 47624

Destinations-IP: IP-adress för den maskin som körs på applikationen

Destinationsport: 47624

Protokoll: TCP/UDP

Källans IP: ospecificerat

Källans port: område 2300 - 2400

Destinations-IP: IP-adress för den maskin som kör applikationen

Destinationsport: område 2300 - 2400

Delta Force

Protokoll: TCP

Källans IP: ospecificerat

Källans port: område 3568 - 3569

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: område 3568 - 3569

Dial Pad

Protokoll: UDP

Källans IP: ospecificerat

Källans port: område 51200 - 51201

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: område 51200 - 51201

Gamespy

Registrering

Protokoll: UDP

Källans IP: ospecificerat

Källans port: 25635

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 25665

För spelen själva

Protokoll: UDP

Källans IP: ospecificerat

Källans port: område 25000 - 30000

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: område 25000 - 30000

Kali - 3 portmappningar nödvändiga

Protokoll: UDP

Källans IP: ospecificerat

Källans port: 2213

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 2213

Protokoll: UDP

Källans IP: ospecificerat

Källans port: 6666

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 6666

Protokoll: UDP

Källans IP: ospecificerat

Källans port: 57

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 57

Mplayer

Protokoll: TCP/UDP

Källans IP: ospecificerat

Källans port: 8000 - 9000

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 8000 - 9000

PCanywhere versionerna 2.0 - 7.51 - 2 portmappningar nödvändiga

Protokoll: TCP

Källans IP: ospecificerat

Källans port: 65301

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 65301

Protokoll: UDP

Källans IP: opecificerat

Källans port: 22

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 22

Quicktime - 2 portmappningar nödvändiga

Protokoll: TCP

Källans IP: ospecificerat

Källans port: 554

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: 554

Protokoll: UDP

Källans IP: ospecificerat

Källans port: område 6970 - 6999

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport: område 6970 - 6999

RTSP

Protokoll: UDP

Källans IP: ospecificerat

Källans port: område 6970 - 7170

Destinations-IP: IP_adressen för den maskin som kör applikationen

Destinationsport område 6970 - 7170

VNC

Protokoll: TCP

Källans IP: ospecificerat

Källans port: 59xx (beroende på displaynummer)

Destinations-IP: IP-adressn för den maskin som kör applikationen

Destinationsport 59xx

Protokoll: TCP

Källans IP: ospecificerat

Källans port: 58xx

Destinations-IP: IP-adressen för den maskin som kör applikationen

Destinationsport 58xx

LISTA ÖVER TERMER

A

ARP

Address Resolution Protocol associerar en IP-adress till en hårdvaruadress genom begära ytterligare information, kallad MAC-adress, från den sändande maskinen. WinRoute använder ARP endast för loggningsändamål för att öka säkerheten.

B

BOOTP

Bootstrap-protokoll som helt enkelt refererar till de datorer inom ett lokalt områdesnätverk som har utformats för att acceptera en IP-adress dynamiskt från en DHCP-server.

Brandvägg (firewall)

En filtreringsmodul lokaliserad på en gateway-maskin som examinerar all inkommande och utgående trafik för att avgöra om den kan routas till sin destination. WinRoute ger en omfattande brandvägg via NATs funktionalitet, tilldelningen av regler för specificerade IP-adresser och förmågan att registrera viss information går en väg så att den kan auktoriseras på vägen tillbaka.

C

Cache

Refererar till en plats där data lagras tillfälligt. WinRoute använder cachelagring för tillfällig lagring av webbsidor för att att upprätthålla bandbredden.

D

DHCP

Dynamic Host Configuration Protocol är ett protokoll för att organisera och förenkla adminstrationen av IP-adresser för lokala maskiner. I många fall (som med WinRoute) har en DNS-server byggts in i DHCP-servern för ytterligare förenkling. Genom att specificera IP-adressen för en specifik nätverksanordning, vanligen den anordning som är förbunden med Internet, kommer DHCP att använda de DNS-värden som är associerade med den anordningen.

DNS

Domain Name System är ett namngivningsschema för IP-adressering. Så är till exempel www.tinysoftware.com ett domännamn och har en associerad IP-adress. En DNS-server matchar domännamnen med en IP-adress. Vi använder domännamnssystemet eftersom det är lättare att komma ihåg ett domännamn än en räcka med nummer.

E

ETRN

ETRN är ett kommando som används av SMTP-servrar för att förhandla om längre tid, efter att ha etablerat en anslutning bör SMTP-server göra en förfrågan om SMTP-post.

ETRN-kommandot används alltid där en SMTP-server inte är "online" 24 timmar om dygnet och e-post till en sådan SMTP-server måste lagras på en tillfällig plats på en annan SMTP-server.

F

Flaggor (flags)

Flaggor är den utvidgade informationsdelen av ett paket. De innehåller extra information om det paket som används av routers. Här är listan över flaggor som visas av WinRoute:

SYNC - Synchronize (synkronisera) - det grundläggande paketet från en TCP-anslutning

ACK - Acknowledge (erkänn) - erkännande av datautbytet

RST - Reset (återställ) - begäran om återupprättane av anslutningen

URG - Urgent (brådskande) - brådskande paket

PSH - Push (påskynda) - begäran om omedelbar leverans av paketet till de högre skikten

FIN - Finalize (avsluta) - avsluta anslutningen

FTP

File Transfer Protocol (filöverföringsprotokoll) är ett applikationsprotokoll som används för att överföra, uppdatera, flytta, döpa om eller kopiera data över hela Internet.

G

Gateway

Ingångspunkten från ett nätverk till ett annat. En gateway är ansvarig för att rätt fördelning av data kommer in i och går ut från ett lokalt områdesnätverk. WinRoute måste installeras på gateway-maskinen, även kallad värddatorn.

I

ICMP

Internet Control Message Protocol använder datagram för att rapportera fel i överföringen mellan värddator och gateway.

IP-adress

IP-adressen är det unika 32-bitsnummer som identifierar datorn i ett IP-nätverk. En unik IP-adress tilldelas varje dator på Internet. Varje paket som passerar över Internet innehåller information om från vilken adress det skickats (källans IP-adress) och till vilken adress den bör levereras (destinationens IP-adress).

IPSEC

Internet Protocol Security tillåter i korthet att virtuellt privat nätarbete använder avsändarens autentisering och kryptering. WinRoute stöder Novel- och Cisco-varianterna av IPSEC.

L

LAN

Ett lokalt områdesnätverk (Local Area Network, LAN) är en grupp av till varandra anslutna datorer som kan dela resurser mellan sig.

M

MAC-adress

Media Access Control-adress är mer specifikt än en IP-adress och kan inte ändras eftersom den är specifik för varje nätverks hårdvaruapparat.

MX-arkiv

MX-arkien (MX records) innehåller information om andra e-postservrar på Internet. Genom att använda MX-arkiven kan du gå förbi din ISP e-postserver och leverera e-post direkt till destinationens e-postserver.

Fördel av detta har du i det fall din ISPs e-postserver *inte är tillförlitlig*. Å andra sidan kan det faktum att du försöker leverera e-post *direkt till destinationen* påverka den tid e-postleveransen tar. I det fall *destinationens e-postserver* inte kan nås kommer e-postbrevet att förbli *icke skickat* i kön av utgående e-postbrev på din WinRoute e-postserver.

N

NAT

Med NAT - Network Address Translator - kan du ansluta till Internet med hjälp av en enda IP-adress och datorerna inom nätverket kommer att använda Internet som om de var anslutna direkt till det (med vissa begränsningar).

Anslutningen av ett helt nätverk som använder en enda registrerad IP-adress möjliggörs eftersom NAT-modulen skriver om källans adress i de paket som skickas från datorer i det det lokala områdesnätverket till adressen för den dator som WinRoute körs på.

NAT skiljer sig avsevärt från flertalet proxyservrar med gateways på applikationsnivå. Dessa kommer i princip aldrig att kunna stödja så många protokoll som NAT gör.

Nätverksgränssnitt

Nätverksgränssnittet (network interface) är den anordning som ansluter datorn till andra datorer med hjälp av ett kommunikationsmedium. Ett nätverksgränsnitt kan vara ett Ethernet-kort, modem, ISDN-kort etc. Datorn skickar och tar emot paket med hjälp av nätverksgränssnittet.

Nätverksmask

Nätverksmask (network mask) används för att gruppera IP-adresser tillsammans. En grupp av adresser tilldelas varje nätverkssegment. Masken 255.255.255.0 grupperar till exempel ihop 254 IP-adresser. Om vi exempelvis har ett undernätverk 194.196.16.0 med masken 255.255.255.0, är de adresser vi kan tilldela datorerna på undernätverket från 194.196.16.1 till och med 194.196.16.254.

P

Paket

Ett paket är en grundenhet för kommunikationsdata som används vid överföring av data från en dator till en annan. Varje paket innehåller en viss mängd data. Den maximala längden av ett paket beror på kommunikationsmediet. Som exempel är den maximala längden på Ethernet-nätverk 1500 bytes. I varje lager kan vi dela paketets innehåll i två delar: rubrikdelen och datadelen. Rubriken innehåller kontrollinformation för det särskilda lagret, datadelen innehåller data som hör till det övre lagret. Mer detaljerad information om paketets struktur kan hittas i avdelningen om paketfiltrering.

POP3

POP3-protokoll används mest av e-postklientens mjukvara för att hämta e-post från postlådor vid POP3-kompatibla e-postservrar. WinRoute har också denna förmåga, dvs. det kan automatiskt hämta e-post vid vilken POP3-kompatibel e-postserver som helst och distribuera den vidare till postlådor för lokala mottagare.

POP3-protokoll är ett **TCP**-protokoll som arbetar på **port 110**. Om du vill ha tillgång till denna e-postserver för protokoll som körs på eller bakom WinRoute-datorn (för att hämta din e-post FRÅN Internet) måste du utföra **portmappning** för TCP-protokoll, port 110 skickas till **privatklass** IP-adress för den dator som kör e-postservern.

Port

En port är ett 16-bitsnummer (det tillåtna området är 1 till och med 65535) som används av transportlagrets protokoll - TCP och UDP-protokoll. Portar används för att adressera applikationer (tjänster) som körs på en dator. Om det bara fanns en enda nätverksapplikation som kördes på datorn skulle det inte behövas några portnummer och IP-adressen skule vara fullt tillräcklig för adressering.

Emellertid kan man ju köra flera applikationer på en särskild dator och vi behöver kunna differentiera dem. Detta är vad portnumren används till. På det sättet kan man också se ett portnummer som en adress till en applikation inom datorn.

Portmappning

Portmappning (eller Port Address Translation - PAT) är den process där paket som kommer till gränssnittet kontrolleras för det portnummer och den IP-adress de vill komma till. Baserat på de portmnummer och IP-adresser som hittas vidarebefordras dessa paket till den fördefinierade privatklass IP-adressen på det lokala nätverket.

Postlådor (mailboxes) i WinRoute

Postådorna (mailboxes) finns i en separat katalog där WinRoute installerats. Vanligen i c:/Program files/WinRoute/Mail.

Inga postlådor skapas efter installationen även om nya användare skapas. Postådorna skapas rent fysiskt EFTER det att det första e-postbrevet kommit in till en användare.

PPTP

PPTP - Point To Point Tunnelling Protocol - är ett VPN- protokoll som avänds av Microsofts operativsystem för att skapa krypterad anslutning mellan två datorer.

Protokoll

Definierar regler för dataöverföring.

Proxy

Proxy är en annan metod för att dela på tillgång till Internet. Proxy opererar med data på en högre protokollsnivå med följd att delat Internet med proxyservrar aldrig var helt tillförlitligt och dessutom krävde en speciell applikationsgateway för varje nätverksprotokoll.

R

RAS

Remote Access Service hänför sig till förmågan att ringa in till en annan dator eller annat nätverk från distans. I sammanhang med WinRoute, refererar RAS helt enkelt till uppringningsanslutning.

Routingtabell

Routingtabeller är den uppsättning regler som genereras av Microsofts operativsystem baserat på de inställningar du utför vid installationen av TCP/IP-protokollet. Routingtabellen används av WinRoute som den uppsättning regler enligt vilken paket ska routas. För att se routingtabellen gå till MS-DOS-promptens fönster och skriv in kommandot `route print`.

S

SMTP

SMTP (Simple Mail Transfer Protocol) används för direkt kommunikation mellan e-postservrar (så som e-postservern i WinRoute och e-postservern för din ISP) och för att skicka ut e-post från e-postklientens mjukvara. SMTP är ett "envägs"-protokoll - dvs. e-post kan skickas eller tas emot av e-postservern men den kan inte hämta e-post vid någon annan e-postserver som använder detta protokoll.

SMTP-protokollet är ett TCP-protokoll som arbetar på **port 25**. Om du vill få tillgång til detta protokoll med den e-postserver som körs bakom eller på WinRoute-datorn (för att tillåta en annan e-postserver att skicka e-post till dig eller för att använda denna e-postserver för din utgående e-post om befinner sig på ditt LAN) så måste du utföra **portmappning** för TCP-protokoll, port 25 skickas till **privatklass** IP-adress för den dator som kör e-postserver.

T

TCP/IP

TCP/IP är en summa av nätverksprotokoll som används för kommunikation mellan datorer. Alla protokoll är paketbaserade, dvs. alla data som skickas igenom delas i sina små delar och skickas över nätverket. TCP/IP-protokollen är: IP, TCP, UDP, ICMP, och andra som baseras på IP.

U

UDP

UDP (User Datagram Protocol) använder en speciell typ av paket som kallas datagram. Datagram kräver inte något svar, de fungerar bara en väg. Datagram används vanligen för strömmande media eftersom en tilfällig pakteförlust inte kommer att påverka överföringens slutprodukt.

V

VPN

Virtual Private Network inbegriper multipla lokala områdesnätverk med förmågan att dela på resurser över Internet genom att skapa en direkttunnel som utför kryptering och dekryptering i båda ändarna. WinRoute stöder virtuell privat networking via PPTP.

INDEX

A

I

K

L

M

N

O

P

Q

R

S

T

U

V

W