Microsoft Products Related Softwares

RRAS analyser

In the last 5 years I have been involved in remote Access projects. The last one was very special because we had to give RAS functionalities to sales forces in 15 different countries in the world via a Windows CE PDA.
They were using the internet to create a VPN connection to their companies and then synchronize data.
Today it is on production. Most of the projects were using VPN servers from CISCO or Checkpoint.

Because I am working also with Microsoft products I had to evaluate Microsoft VPN server (in fact Windows 2000 itself - RRAS service).

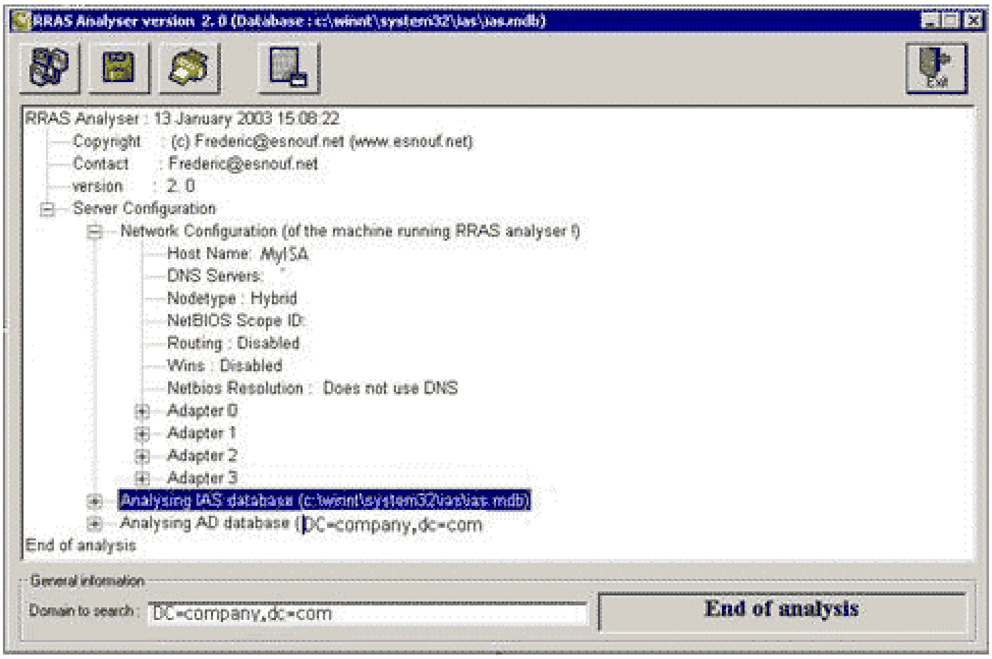
The big problem I detected was the user interface, and it was a major problem to sell the solution and also to support it. Imagine that this VPN server will connect 25 countries in the world and enable the user to synchronize their email. You don't really want to create one single rule that says 'everyone can access to everything', do you ?

With the RRAS service you can create profiles such as 'if you are member of AD group 'messaging sync France', you can talk to 192.1.1.5 on port TCP 25 and 110. Once this rule is created you have to create 24 others, like 'if you are member of AD group 'messaging sync <country>', you can talk to 192.1.<country>.5 on port TCP 25 and 110.

Now everything works fine, but how can you have a clear and quick overview of your current configuration. The answer is to take a long shit of paper, a good pencil, check rule by rule, ... which will make in this case 25 x 5 screens to read.

It is not a really easy way to do it, and to be honest most of my customers did not feel comfortable with it, because it is closely linked to the company security. At that time it was impossible to sell that VPN solution.

So I designed 'RRAS analyzer'. This program will 'DUMP' in just a few seconds all the important information you need to get a clear idea about 'who has access to what' via your VPN server. This program will read the RRAS database but will also check the AD to see who is member of whatever group, who has RAS enabled.


RRAS Analyser version 2. 0 (Database : c:\winnt\system32\ias\ias.mdb)
Exit

```
RRAS Analyser : 13 January 2003 15:08:22
    Copyright   : (c) Frederic@esnouf.net (www.esnouf.net)
    Contact     : Frederic@esnouf.net
    version     : 2. 0
  ⊟ Server Configuration
      ⊟ Network Configuration (of the machine running RRAS analyser !)
            Host Name: MyISA
            DNS Servers:  *
            Nodetype : Hybrid
            NetBIOS Scope ID:
            Routing : Disabled
            Wins : Disabled
            Netbios Resolution :  Does not use DNS
          ⊞ Adapter 0
          ⊞ Adapter 1
          ⊞ Adapter 2
          ⊞ Adapter 3
      ⊞ Analysing IAS database (c:\winnt\system32\ias\ias.mdb)
      ⊞ Analysing AD database (DC=company,dc=com
End of analysis
```

General information
Domain to search : DC=company,dc=com
End of analysis

I had the opportunity to use it but also to share it with some other consultants and this tool has been very useful to sell the product but also to support it.

```
Current machine is DOTNET1

********************************************************
          Network configuration
********************************************************


Host Name:  dotnet1
DNS Servers:  127.0.0.1
DNS Servers:  192.192.1.6
Node type: Hybrid
NetBIOS Scope ID:
IP Routing not enabled
WINS Proxy Enabled
NetBIOS Resolution Does not use DNS
*************
Adapter name: Ethernet adapter {132B304F-1C90-474D-976C-3121EC17E90A}
AdapterDescription: Intel(R) PRO/100+ Management Adapter with Alert On LAN*
Physical Address: 00-D0-B7-2A-49-26
DHCP disabled
IP Address: 192.192.1.1
Subnet Mask: 255.255.255.0

Default Gateway: 192.192.1.1
DHCP Server: 255.255.255.255
Primary WINS Server: 192.192.1.6
Secondary WINS Server: 0.0.0.
Lease Obtained: jeudi, janv 1 00:00:00 197
Lease Expires :  jeudi, janv 1 00:00:00 197


********************************************************
          Analysing IAS database
********************************************************

PROFILE : POLICY - Exchange roaming users
  PROPERTY : msNPAction
     Value : POLICY - Exchange roaming users
  PROPERTY : msNPConstraint
      Type = GROUP MEMBERSHIP
           SID : S-1-5-21-583907252-436374069-842925246-1114
         Group : CN=RAS - Exchange server,OU=RAS
GROUPS,OU=DELEGATION,DC=ad,DC=acme,DC=com
              Member : CN=USER1,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
  PROPERTY : msNPSequence (Sequence order in the MMC - RAS snapin)
     Value : 4


PROFILE : POLICY - Exchange roaming users
  PROPERTY : msNPAuthenticationType2
     Value : 4
       Encryption= Microsoft encrypted (MS-CHAP-V2) activated
  PROPERTY : msNPAuthenticationType2
     Value : 10
       Encryption= Unknown value
  PROPERTY : msRADIUSFramedProtocol
     Value : 1
        PPP
  PROPERTY : msRADIUSServiceType
     Value : 2
        Framed
  PROPERTY : msRASFilter
     Nb of filters :  1
       FILTER Number  1
        Inbound traffic (0100FFFF)
        Deny traffic except those listed below
        Criteria number  1
          Source address : 0.0.0. 0
          Source mask    : 0.0.0. 0
          Dest address   : 192.192.1. 25
          Dest mask      : 255.255.255. 255
                    =>  1 machines with this mask
          Protocol       : Any
          Port(s)        : No rule (means all ports)
  New PROPERTY : msRASMPPEEncryptionPolicy
     Value : 1 (check RFCs 2865 and 2866)
  PROPERTY : msRASMPPEEncryptionType
     Value : 0
```

```
PROFILE : POLICY - Paris Servers
  PROPERTY : msNPAction
      Value : POLICY - Paris Servers
  PROPERTY : msNPConstraint
       Type = GROUP MEMBERSHIP
              SID : S-1-5-21-583907252-436374069-842925246-1115
            Group : CN=RAS - All servers in Paris,OU=RAS
GROUPS,OU=DELEGATION,DC=ad,DC=acme,DC=com
                    Member : CN=user3,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
                    Member : CN=user2,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
                    Member : CN=USER1,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
  PROPERTY : msNPSequence (Sequence order in the MMC - RAS snapin)
      Value : 3

PROFILE : POLICY - Paris Servers
  PROPERTY : msNPAuthenticationType2
      Value : 4
        Encryption= Microsoft encrypted (MS-CHAP-V2) activated
  PROPERTY : msNPAuthenticationType2
      Value : 3
        Encryption= Microsoft encrypted (MS-CHAP) activated
  PROPERTY : msNPAuthenticationType2
      Value : 10
        Encryption= Unknown value
  PROPERTY : msNPAuthenticationType2
      Value : 9
        Encryption= Unknown value
  PROPERTY : msRADIUSFramedProtocol
      Value : 1
          PPP
  PROPERTY : msRADIUSServiceType
      Value : 2
          Framed
  PROPERTY : msRASFilter
      Nb of filters :  1
        FILTER Number  1
          Inbound traffic (0100FFFF)
          Deny traffic except those listed below
          Criteria number  1
             Source address : 0.0.0. 0
             Source mask    : 0.0.0. 0
             Dest address   : 192.192.1. 0
             Dest mask      : 255.255.255. 0
                           =>  255 machines with this mask
             Protocol       : Any
             Port(s)        : No rule (means all ports)

PROFILE : POLICY - London servers
  PROPERTY : msNPAction
      Value : POLICY - London servers
  PROPERTY : msNPConstraint
       Type = GROUP MEMBERSHIP
              SID : S-1-5-21-583907252-436374069-842925246-1116
            Group : CN=RAS - All servers in London  (192.192.2.x),OU=RAS
GROUPS,OU=DELEGATION,DC=ad,DC=acme,DC=com
                    Member : CN=user3,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
                    Member : CN=user2,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
  PROPERTY : msNPSequence (Sequence order in the MMC - RAS snapin)
      Value : 2

PROFILE : POLICY - London servers
  PROPERTY : msNPAuthenticationType2
      Value : 4
        Encryption= Microsoft encrypted (MS-CHAP-V2) activated
  PROPERTY : msNPAuthenticationType2
      Value : 3
        Encryption= Microsoft encrypted (MS-CHAP) activated
  PROPERTY : msNPAuthenticationType2
      Value : 10
        Encryption= Unknown value
  PROPERTY : msNPAuthenticationType2
      Value : 9
        Encryption= Unknown value
  PROPERTY : msRADIUSFramedProtocol
      Value : 1
          PPP
  PROPERTY : msRADIUSServiceType
      Value : 2
          Framed
  PROPERTY : msRASFilter
      Nb of filters :  1
        FILTER Number  1
          Inbound traffic (0100FFFF)
          Permit traffic except those listed below
          Criteria number  1
             Source address : 0.0.0. 0
             Source mask    : 0.0.0. 0
             Dest address   : 192.192.2. 0
             Dest mask      : 255.255.255. 0
                         =>  255 machines with this mask
             Protocol       : Any
             Port(s)        : No rule (means all ports)


PROFILE : POLICY - dsl home user 1
  PROPERTY : msNPAction
      Value : POLICY - dsl home user 1
  PROPERTY : msNPConstraint
       Type = GROUP MEMBERSHIP
               SID : S-1-5-21-583907252-436374069-842925246-1117
             Group : CN=RAS - Mr A - DSL home user,OU=RAS
GROUPS,OU=DELEGATION,DC=ad,DC=acme,DC=com
                     Member : CN=user3,OU=USERS,OU=DELEGATION,DC=ad,DC=acme,DC=com
  PROPERTY : msNPSequence (Sequence order in the MMC - RAS snapin)
      Value : 1


PROFILE : POLICY - dsl home user 1
  PROPERTY : msNPAuthenticationType2
      Value : 4
        Encryption= Microsoft encrypted (MS-CHAP-V2) activated
  PROPERTY : msNPAuthenticationType2
      Value : 10
        Encryption= Unknown value
  New PROPERTY : msNPTimeOfDay
      Value : 0 08:00-19:00 (check RFCs 2865 and 2866)
  New PROPERTY : msNPTimeOfDay
      Value : 1 08:00-19:00 (check RFCs 2865 and 2866)
  New PROPERTY : msNPTimeOfDay
      Value : 2 08:00-19:00 (check RFCs 2865 and 2866)
  New PROPERTY : msNPTimeOfDay
      Value : 3 08:00-19:00 (check RFCs 2865 and 2866)
  New PROPERTY : msNPTimeOfDay
      Value : 4 08:00-19:00 (check RFCs 2865 and 2866)
  PROPERTY : msRADIUSFramedProtocol
      Value : 1
          PPP
  PROPERTY : msRADIUSServiceType
      Value : 2
          Framed
  New PROPERTY : msRASMPPEEncryptionPolicy
      Value : 1 (check RFCs 2865 and 2866)
  PROPERTY : msRASMPPEEncryptionType
      Value : 8



*************************************************************
     Users with 'ALLOWED ACCESS' property in Active directory
*************************************************************

Analysing DC=ad,DC=acme,DC=com domain.

 3 users detected with this property set.


CN : USER1
     Allowed to dialin
         No callback number set. Up to the user


CN : user2
     Allowed to dialin
         Callback number is set :  123456789


CN : user3
```

Allowed to dialin

No callback number set. Up to the user

Esnouf.net is in no way affiliated with Microsoft Corp.