



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.



A paper by Jason R. DePriest
Memphis, TN 38103

This tutorial will guide you through “locking down” your PowerVPN server. When you have finished, access will be restricted so that end-users see only what they need to see and most violation attempts will be logged.

This tutorial assumes the following:

- You have already installed PowerVPN server on a stand-alone Windows NT 4.0 Server. The server should have Microsoft Windows NT 4.0 Service Pack 5 or Service Pack 6a installed, as well.
- You have already configured both your outside and inside interfaces on the PowerVPN server.
- The outside interface of the PowerVPN server is inside your firewalled DMZ.
- The firewall has already been properly configured to only allow the appropriate access.
- You have already created at least a subset of the network entities on the PowerVPN server you will be using to create your access lists and rules.

© SANS Institute 2000 - 2005. All rights reserved.

First, We need to allow only those systems that require access to these services and block all other traffic. This will stop any unauthorized malicious systems from parking on a port and attempting well-known exploits or password guessing. PowerVPN has a built-in “implicit deny” rule. This means that anything not actively permitted is automatically denied. This means most of the access rules we will be creating will grant certain access to certain groups. If you have an administrator group, you can create a rule that resembles Figure 1., Figure 2., and Figure 3.

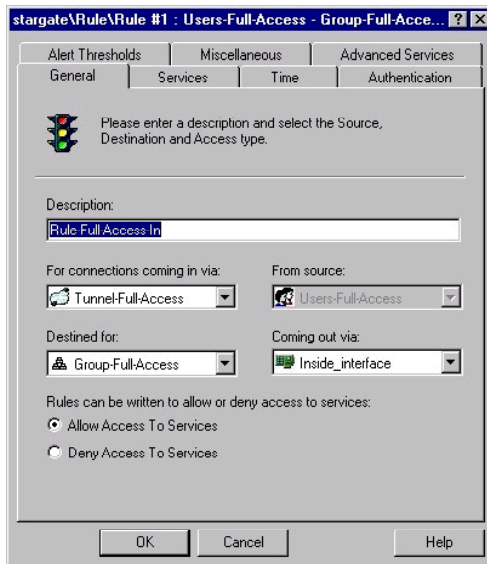


Figure 1.

Here we establish who this rule applies to: anyone coming in via the Full-Access Tunnel attempting to access any of the systems in Full-Access Group.

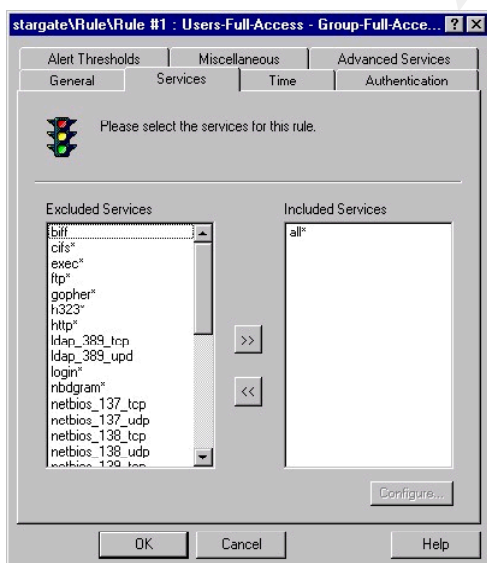


Figure 2.

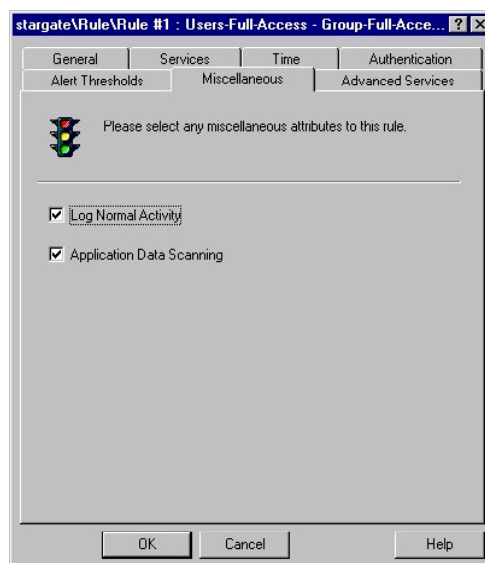


Figure 3.

Be sure to “Log Normal Activity” so you will know who uses this Full-Access tunnel and when. Errors and failed access attempts are logged even if this feature is not checked.

Application Data Scanning enables PowerVPN to examine incoming packets at the data level. If this is not checked, PowerVPN acts as a simple packet filter; this results in less security but better performance.

Spoofed Addresses

What is a spoofed address?

When someone from outside of your network is trying to trick your equipment into thinking he is inside your network by using a fake or hijacked IP address that fits your internal addressing scheme, he is trying to “spoof” an address.

The best way to block address spoofing is to check which interface the traffic is trying to enter. Internal traffic should not be entering the outside interface; it should only enter via the inside interface.

We need to create a rule to block any traffic coming in via the outside interface that claims to be from an inside address.

To further enhance this rule, you can expand it to block all “private” addresses coming into the outside interface. Private addresses include the following 10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0/12.

To set this rule using PowerVPN, you need to access the PowerVPN management console and go to the following section:

Console Root → Axent Technologies → Raptor Management Console → <name of server> → Access Controls → Rules.

From there select *New → Rule*.

The rule you create should resemble Figure 4. and Figure 5.

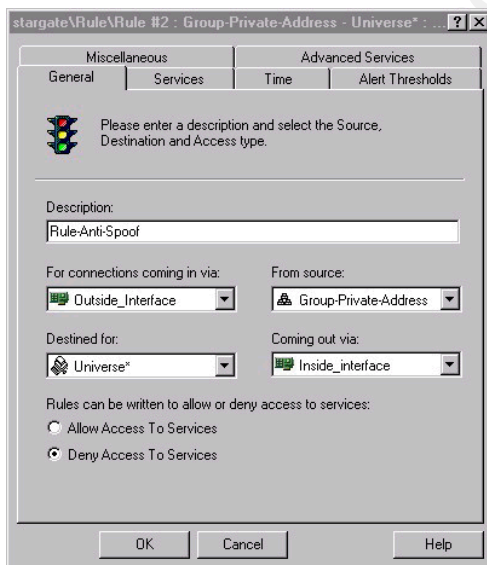


Figure 4.

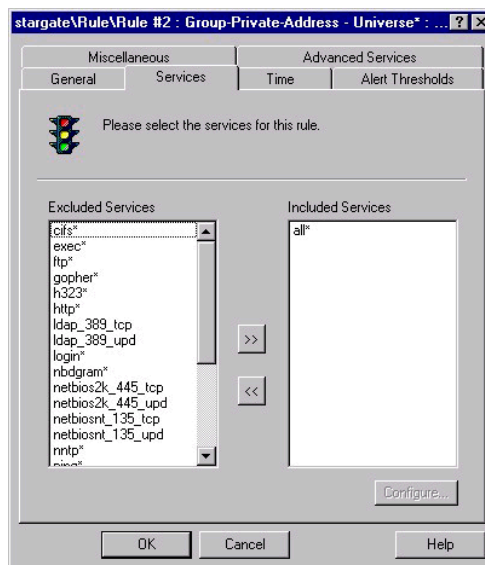


Figure 5.

This applies when “Group-Private-Address” includes all three private subnets and “Universe*” is all addresses.

What else do I have to worry about?

Many of the rules we need to set up can be combined into a single rule or a small group of catch-all rules that block certain ports and allow only certain users to bypass them.

To see what services, protocols, and ports are already defined within PowerVPN, you will need to go to the following section:

Console Root → Axent Technologies → Raptor Management Console → <name of server> → Base Components → Protocols.

You should see something similar to Figure 6.

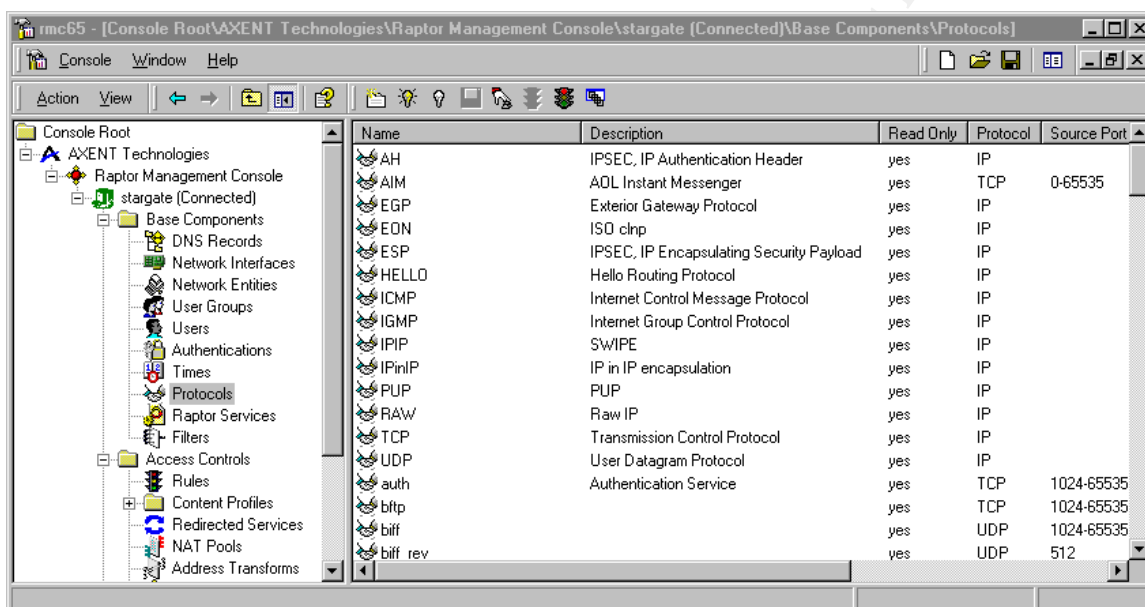


Figure 6.

The following section will describe what we intend to control and why we need to control it.

Login Services

What login services need to be controlled?

- telnet tcp port 23
- SSH tcp port 22
- FTP tcp port 21
- NetBIOS tcp port 139
- RMC tcp port 418
- SRL (telnet) tcp port 423
- exec tcp port 512
- login tcp port 513
- shell tcp port 514

Both RMC (Remote Management Console) and SRL (Secure Remote Login) are Raptor Firewall and PowerVPN specific. The others are all standard ports that might be listening for some sort of authentication.

Access must be restricted and/or monitored to these ports or you risk system compromise.

RPC (Remote Procedure Call)

RPC listens on tcp port 111 and UDP port 111 along with portmap.

You can see <http://www.cert.org/advisories/CA-97.26.statd.html> for a specific advisory relating to a buffer overflow in an RPC server, statd. This overflow can be exploited remotely and locally and can allow a user to gain root privileges. As old as this exploit may seem, keep in mind that the hacker community is constantly hammering on potentially powerful services to exploit.

An improperly configured portmapper could grant everyone access to your system.

NFS (Network File System)

NFS listens on tcp port 2049 and up port 2049.

The following bullet-points are directly from the NFS-How-To

(<http://howto.tucows.com/otherhowto/other-formats/html/NFS-HOWTO-html.tar.gz>):

- It makes sharing of files over a network possible.
- It works mostly well enough.
- It opens a can of security risks that are well understood by crackers, and easily exploited to get access (read, write and delete) to all your files.

From this alone, you can see that this feature must be controlled and monitored. But what does this mean?

The client-side of NFS, by default, will trust the NFS server implicitly. This allows a compromise at the server level to easily propagate to the client level or vice-versa.

lockd - the NFS file locking service

The lockd service listens on tcp port 4045 and up port 4045.

A simple DoS against lockd can be read about in further detail here:

http://www.securiteam.com/unixfocus/Linux_rpc_lockd_vulnerable_to_remote_DoS.html.

NetBIOS

Windows systems use several ports for NetBIOS communications (tcp and up ports 135 - 139). NetBIOS is extremely important to almost all aspects of Windows networking. Name resolution, file/print sharing, user and domain management, and netlogon are just a few of the services handled by Windows using NetBIOS. For this reason we need to keep strict and specific controls over who is permitted to use it. If you are running a Windows 2000 system, you also need to include tcp port 445 and up port 445.

Do I really need to give examples of how this can be exploited?

Using the preinstalled Windows NT tools *nbtstat* and *net [view]* you can find out who is logged on to a system and what shares exist on that system. This is small time, using a tool like *enum* (Jordan Ritter @ <http://demerol.darkridge.com/~jpr5/>) or *winfingerprint* (Kirby Kuehl @ <http://www.technotronic.com/winfingerprint/>), you can easily enumerate NetBIOS shares, user names, group names, certain registry settings, decipher a server's role (PDC, BDC, member server, etc), and other scary things.

In short, this is a glaring hole and needs to be monitored and restricted.

X Windows

This is not a problem in the Microsoft world. But if you have *nix boxes running on the inside of your organization and someone coming in through the VPN can access them, then this is something you must restrict.

Unix and Linux boxes listen on tcp port 6000 through tcp port 6255 for X Windows sessions.

Naming Services

The implications of this are obvious: someone could come in through the VPN and perform a zone transfer to potentially retrieve a map of your internal addresses.

DNS zone transfers should be restricted to the specific secondary systems that are installed strictly for this purpose. You must restrict tcp port 53.

We will have to take into consideration that both client queries and secondary DNS server queries will access upd port 53 and adjust the rule(s) accordingly.

For LDAP, similar risks apply and you will need to restrict tcp port 389 and upd port 389.

Mail

Mail must be monitored and controlled to keep people from using your systems to spoof email addresses (easily accomplished by telnetting to an unprotected, listening SMTP port).

Depending on what mail services you have configured, you may also need to block POP and IMAP.

SMTP typically runs on tcp port 25. No typical VPN clients should need access to this. Only your external mail relay systems would need access to this service.

For my particular corporate environment, we are not using POP or IMAP for mail. You may or may not need to block or restrict these services. POP2 listens on tcp port 109 and POP3 listens on tcp port 110; IMAP listens on tcp port 143.

Web

If you have an intranet site, then you will need to place some permissions on HTTP access. It would be wise to put controls in place even if you do not have an intranet site; you never know who might be running a web server at their desk... think of FrontPage 97 and 98's Personal Web Server which had to be installed for FrontPage to work properly.

The typical HTTP port is tcp port 80, with 8000, 8080, and 8888 being common alternatives. SSL (Secure Socket Layer) is evidenced by an HTTPS prefix instead of HTTP; it uses tcp port 443.

ICMP

You may want to allow only your administrative group to utilize ping and/or tracert. There should be no reason for the average user to need the information these programs can provide. Therefore, you should restrict incoming echo requests and outgoing echo replies. Echo uses tcp port 7 and upd port 7.

You should also restrict the particular messages that ICMP can send. You could put controls on icmp_echo_request (msg. 8), icmp_echo_reply (msg. 0), icmp_time_exceeded (msg. 11), and icmp_dest_unreachable (msg. 3).

If an unauthorized user was able to do a ping sweep of your internal network, it would be trivial for that person to construct a map of what your layout is.

Miscellaneous

PowerVPN has some other services should be monitored and restricted.

A list of these follows:

- | | |
|----------------------|-----------------------------|
| • discard | tcp port 9 and upd port 9 |
| • systat | tcp port 11 |
| • daytime | tcp port 13 and upd port 13 |
| • netstat | tcp port 15 |
| • chargen | tcp port 19 and upd port 19 |
| • tftp (Trivial FTP) | upd port 69 |

- finger tcp port 79
- nntp (USENET News) tcp port 119
- ntp upd port 123
- bgp (border gateway protocol) tcp port 179
- snmp (simple network management protocol) tcp port 161 and upd port 161
- snmptrap tcp port 162 and upd port 162
- syslog upd port 514
- LPD (printer) tcp port 515
- socks tcp port 1080

That completes the listing of what we need to control, restrict, and monitor. This will be much easier than it may seem. We will take advantage of PowerVPN's implicit deny rule: anything that is not specifically allowed is denied.

Next we will compile this list down to a few rules and implement them on our PowerVPN server.

Applying the rules

To use PowerVPN the way it was intended, you will need to create User Groups for the different permission sets you will be implementing.

We have already looked at a group called *Users-Full-Access*. This is what I used for my administrative group.

Typical User

I also have a group called *Users-Email-Intranet-Only*, which is just what it sounds like: a basic group with access to only the barest of essentials.

To set up their permissions, go to *Console Root* → *Axent Technologies* → *Raptor Management Console* → *<name of server>* → *Access Controls* → *Rules*.

From there select *New* → *Rule*.

Look at the next four screenshots to see what access is afforded them.

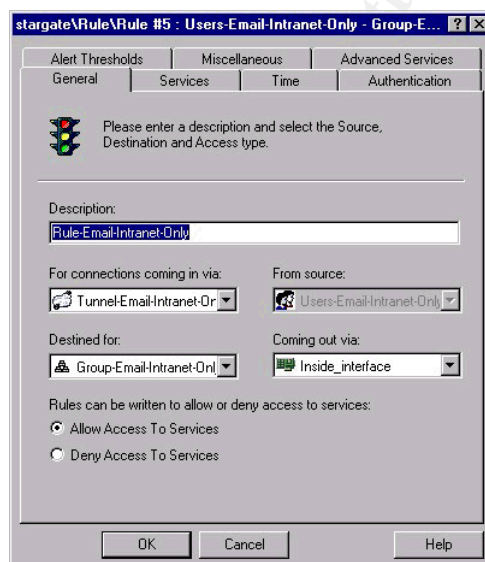


Figure 7.

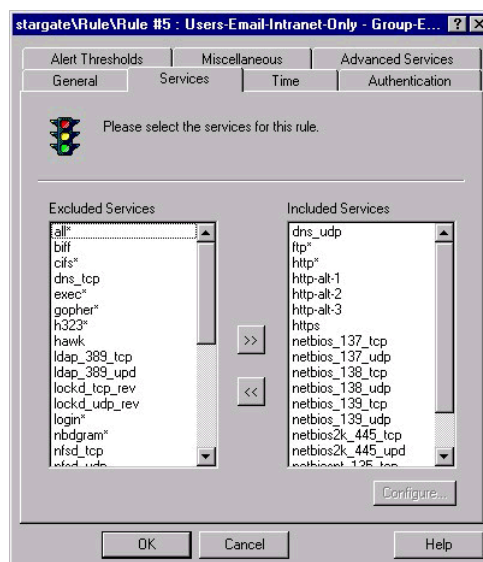


Figure 8.

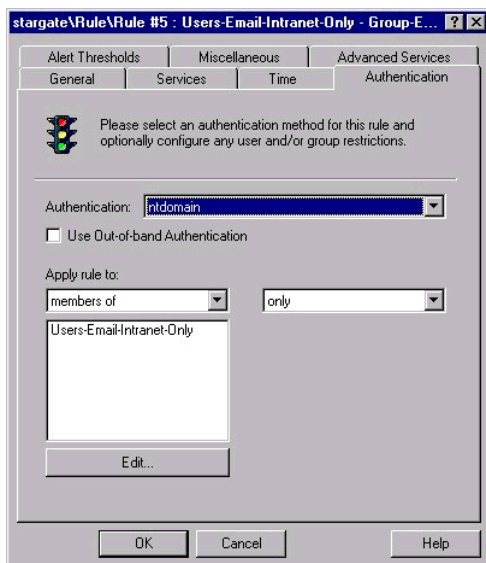


Figure 9.

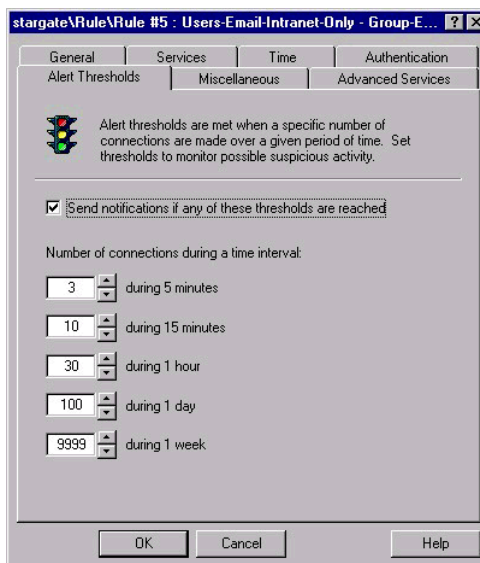


Figure 10.

Figure 7. shows that this rule will apply to anyone coming in through the Tunnel associated with the *Users-Email-Intranet-Only* group. Figure 8. shows that they will have access to all http, email, FTP, and NetBIOS related functions.

Figure 9. shows that we will require NT domain authentication for those that this rule applies to. It also shows that we want this rule to apply only to members of the *Users-Email-Intranet-Only* group. This is important because an individual user can be a member of more than one group.

Figure 10. shows how to set up your alerts. Since typical users are the most likely to be compromised, it is very important to log these types of events.

DNS Zone Transfer

If you have a server-to-server VPN tunnel established and need to propagate your DNS information to a DNS server at the other end of the tunnel, the following screenshots show a rule that could accomplish this.

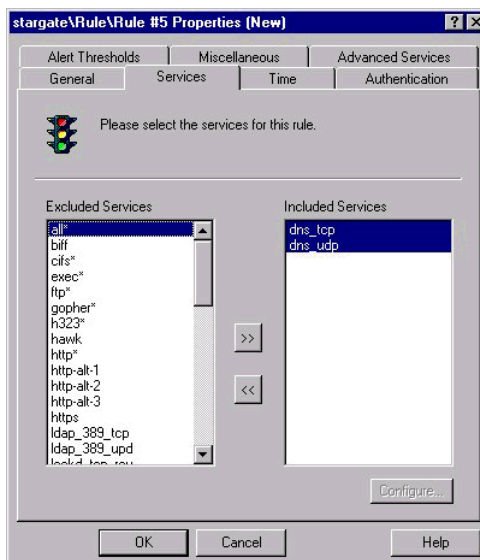
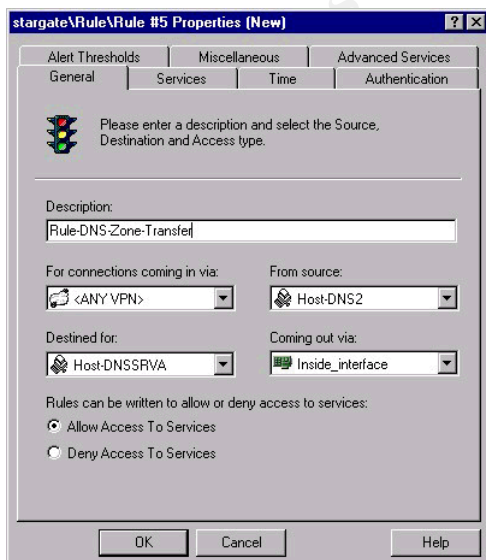


Figure 11.

Figure 12.

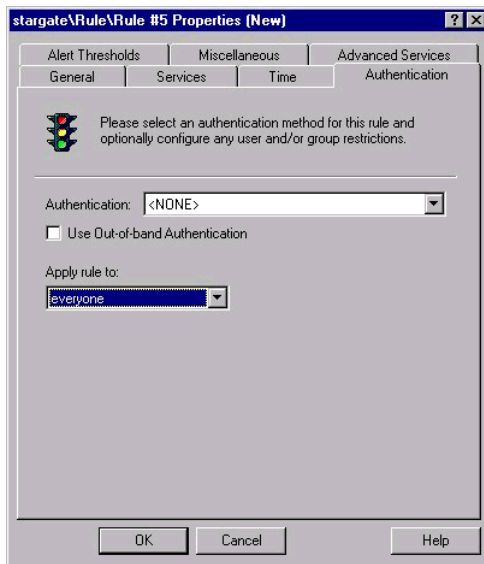


Figure 13.

Figure 11. and Figure 12. show that some external DNS server Host-DNS2 is allowed to contact your internal DNS server, Host-DNSSRVA for a zone transfer or for an address query. To minimize user intervention, there is nothing special configured on the “Authentication” tab. The only item being allowed in by this rule is a specific system.

Email Relay

If you have external mail relay systems that are at the other end of a server to server VPN tunnel, then you need to make sure you allow the servers to talk to each other.

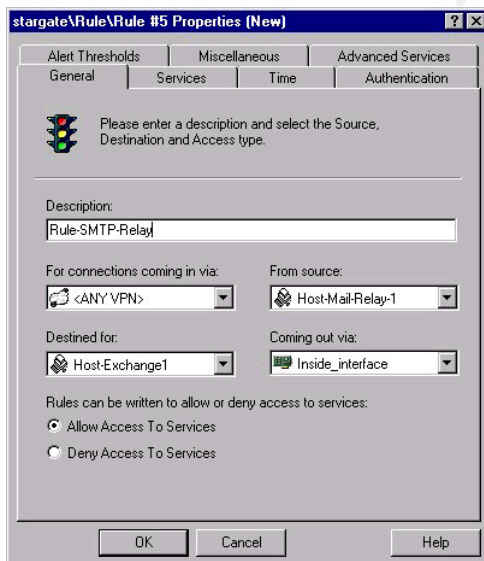


Figure 14.

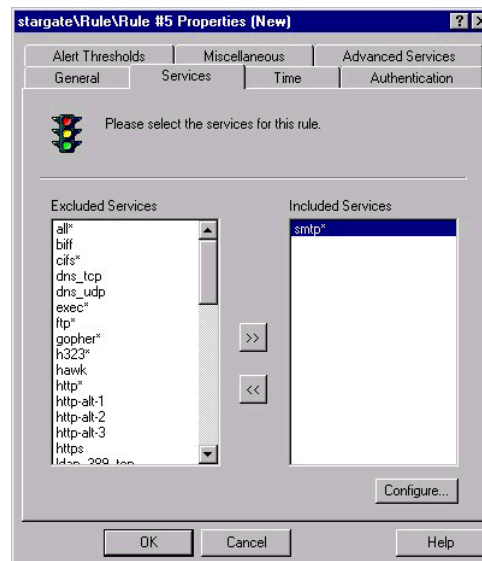


Figure 15.

As you can see, this is very similar to the DNS rule above. This time we are only allowing smtp traffic through from the designated server.

I've shown you how to set up full access for admins and highly restricted access for typical users. Of course, you can always create rules based on one particular user or create a new group when certain people need access to something that is restricted.

Example 1:

One of the vice-presidents of the company must have access to a particular server in a particular department to access a shared directory there. She must also be able to send and receive email, browse the Intranet, and establish mainframe connectivity via SNA. The server with the shared directory on it is running Windows NT Server 4.0; it is a member server of the company domain and does not handle any domain user authentication. The same server is also running Microsoft SNA Server 4.0.

This one is complicated, but not as complicated as you might think.

The best approach is to create a new Group of systems and subnets that she needs to access. You do this under *Console Root* → *Axent Technologies* → *Raptor Management Console* → *<name of server>* → *Access Controls* → *Network Entities*.

From there select *New* → *Group*.

See Figure 16. and Figure 17. for what this might look like.

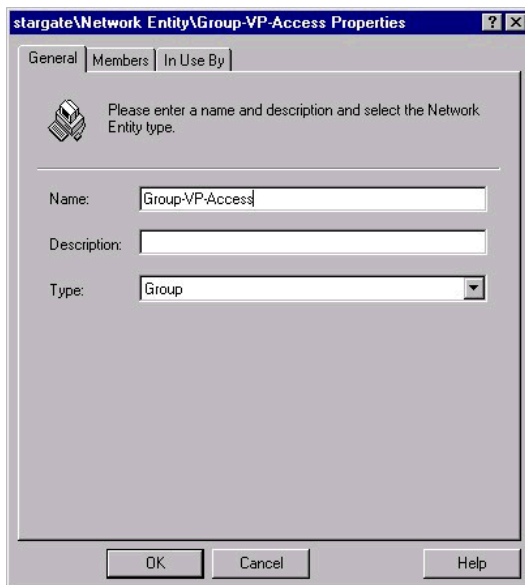


Figure 16.

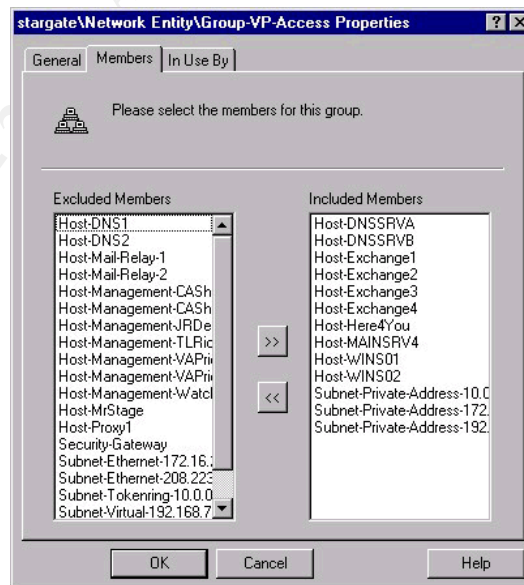


Figure 17.

Now that we have a group, we need to develop a new tunnel that uses this group as an endpoint. See Figure 18.

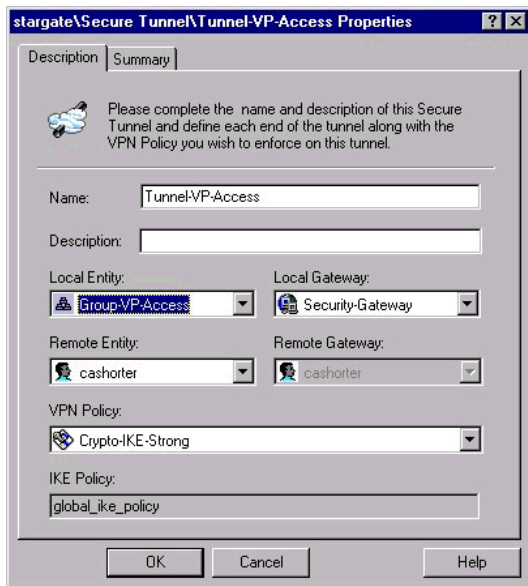


Figure 18.

As you can see, this tunnel applies only to the user “cashorter”, who is our VP in question, and only if she is destined for a system that is in the *Group-VP-Access* group.

Now we can finally build a rule to allow in the services that she needs.

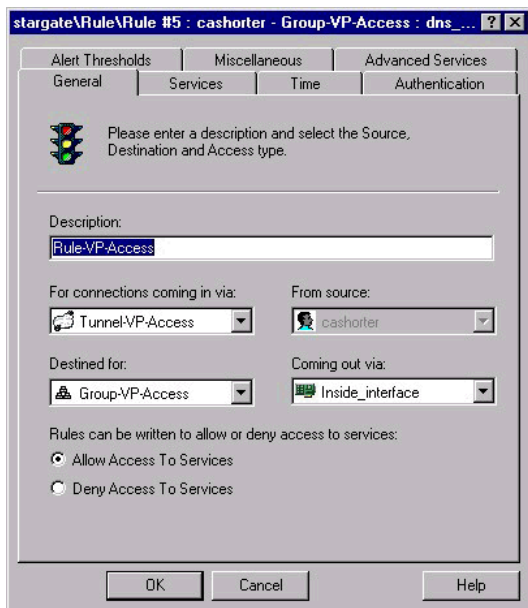


Figure 19.

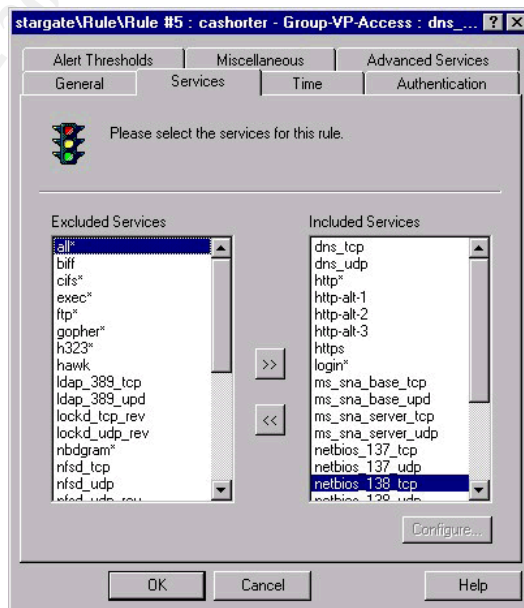


Figure 20.

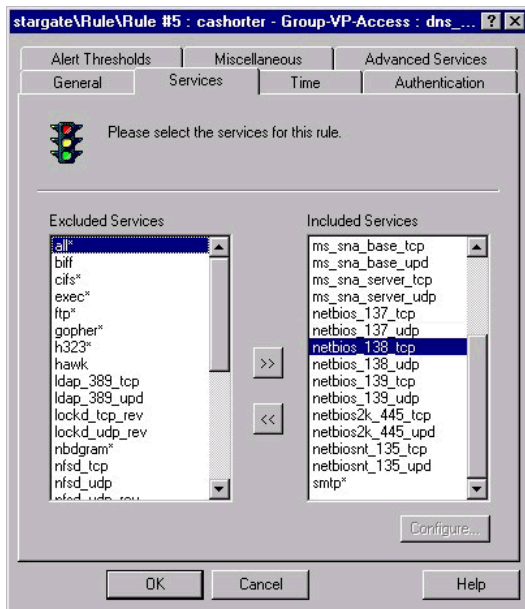


Figure 21.

You can see the stack of services that need to be included in Figure 20. and Figure 21. There was a further complication because PowerVPN did not have the settings for Microsoft SNA in with its services.

I had to manually add tcp/upd ports 1477 and 1478 respectively.

The implicit deny built in to PowerVPN will take care of the rest.

Now just save and reconfigure and you are in business.

See? That wasn't difficult at all.

Example 2:

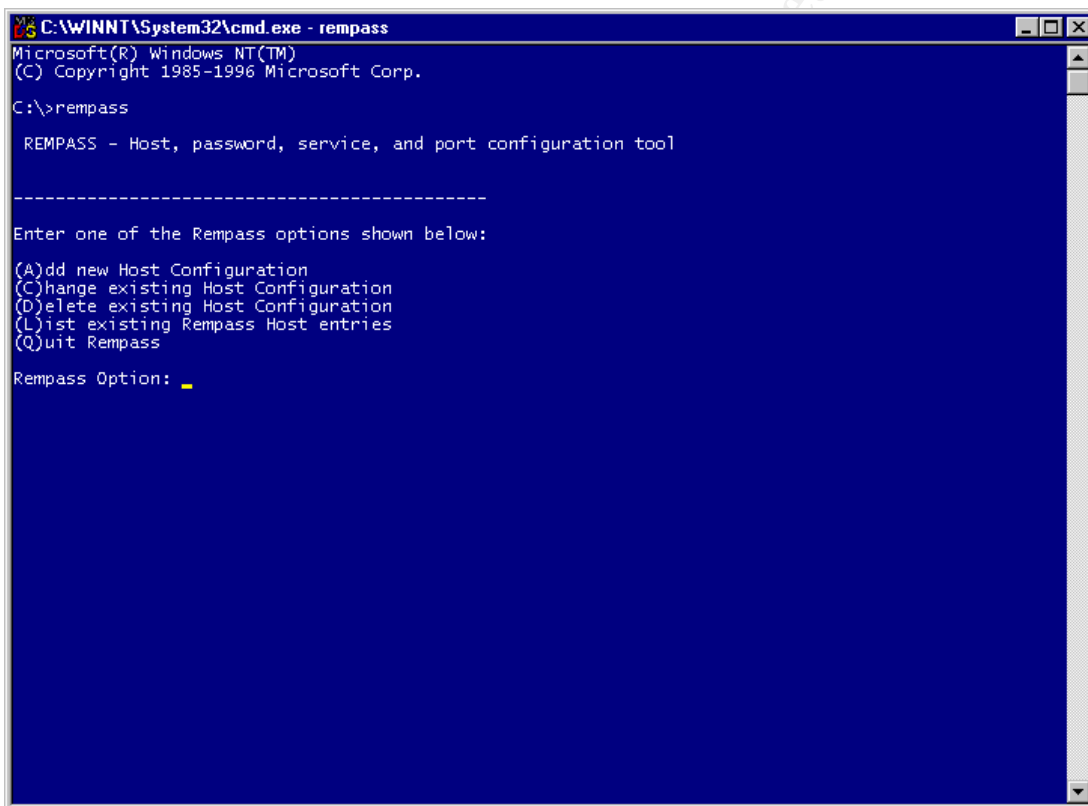
I promise this example is much easier.

A new employee, James, is hired to be your backup administrator to the VPN. He will need to be able to remotely access the PowerVPN server and perform various functions to lighten your load.

First, you need to make sure that James' system has a static IP address. This is how the PowerVPN server keeps track of who had administrative access to the system. Let's assume that James gets the IP address 10.23.7.5 assigned to him as a static IP address.

Before you go creating rules for his system, you need to visit the server itself and run the application that will acknowledge that he is, indeed, an administrator.

See the next four screenshots to get an example of setting someone up to remotely access the system via the RMC.



```
C:\WINNT\System32\cmd.exe - rempass
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>rempass

REMPASS - Host, password, service, and port configuration tool

-----
Enter one of the Rempass options shown below:
(A)dd new Host Configuration
(C)hange existing Host Configuration
(D)elete existing Host Configuration
(L)ist existing Rempass Host entries
(Q)uit Rempass

Rempass Option: _
```

Figure 16.

First we run the program "rempass" from the command line on the PowerVPN server. Figure 16. shows the main menu of rempass. We are going to select option (A) to add a new host configuration and then enter 10.23.7.5 when it asks for the IP address.

```
C:\WINNT\System32\cmd.exe - rempass
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>rempass

REMPASS - Host, password, service, and port configuration tool

-----

Enter one of the Rempass options shown below:

(A)dd new Host Configuration
(C)hange existing Host Configuration
(D)elete existing Host Configuration
(L)ist existing Rempass Host entries
(Q)uit Rempass

Rempass Option: a
Host name or IP address: 10.23.7.5
-----

Service List:

(1) Firewall Management Console
    -Configure firewall to accept remote management connections

(2) Logfile Retrieval
    -Configure firewall to allow remote client to access firewall logfiles

(3) Log Event Submission
    -Configure firewall to accept log output from remote client

(4) Content Scanning
    -Configure firewall to use remote content scanner

(5) Intrusion detection
    -Configure firewall to accept intrusion notification

Please Choose a Service ('m' for main menu): _
```

Figure 17.

As you can see, this gives us several options. Option (1) is the one we are interested in.

© SANS Institute 2000-2005


```
C:\WINNT\System32\cmd.exe - rempass
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.
C:\>rempass

REMPASS - Host, password, service, and port configuration tool

-----
Enter one of the Rempass options shown below:
(A)dd new Host Configuration
(C)hange existing Host Configuration
(D)elete existing Host Configuration
(L)ist existing Rempass Host entries
(Q)uit Rempass

Rempass Option: a
Host name or IP address: 10.23.7.5
-----
Service List:

(1) Firewall Management Console
    -Configure firewall to accept remote management connections

(2) Logfile Retrieval
    -Configure firewall to allow remote client to access firewall logfiles

(3) Log Event Submission
    -Configure firewall to accept log output from remote client

(4) Content Scanning
    -Configure firewall to use remote content scanner

(5) Intrusion detection
    -Configure firewall to accept intrusion notification

Please Choose a Service ('m' for main menu): 1

Enter up to 64 characters for
10.23.7.5's passphrase:
```

Figure 18.

Pressing (1) gives you the prompt to enter and verify the password for the host you already entered.


```
C:\WINNT\System32\cmd.exe - rempass
(L)ist existing Rempass Host entries
(Q)uit Rempass

Rempass Option: a
Host name or IP address: 10.23.7.5
-----
Service List:

(1) Firewall Management Console
    -Configure firewall to accept remote management connections

(2) Logfile Retrieval
    -Configure firewall to allow remote client to access firewall logfiles

(3) Log Event Submission
    -Configure firewall to accept log output from remote client

(4) Content Scanning
    -Configure firewall to use remote content scanner

(5) Intrusion detection
    -Configure firewall to accept intrusion notification

Please Choose a Service ('m' for main menu): 1

Enter up to 64 characters for
10.23.7.5's passphrase:

Verify new password:
Rempass 10.23.7.5 (10.23.7.5) password added.
-----

Enter one of the Rempass options shown below:
(A)dd new Host Configuration
(C)hange existing Host Configuration
(D)elete existing Host Configuration
(L)ist existing Rempass Host entries
(Q)uit Rempass

Rempass Option:
```

Figure 19.

Select (Q)uit and you are done.

The RMC does not run through a tunnel. It is designed to connect to the inside interface of the PowerVPN box from within the internal network.

Raptor Firewall with PowerVPN has a Secure Remote Login feature that is not supported under Windows NT Server (only supported under Solaris). If this feature were supported, you would need to create a rule to allow the secure telnet sessions to connect.

I hope this has shown you the basics of PowerVPN.

The Remote Management Console is extremely intuitive. This is still true even in the instances where it takes many steps to complete simple tasks.

If you would like further information on related subjects, you can check the next page for a listing of the resources I used in compiling this paper.

References

The following references and resources were used:

Internet Resources-

Writing Snort Rules - Martin Roesch - <http://www.snort.org/>

Building Your Firewall Rulebase - Lance Spitzner -

<http://www.enteract.com/~lspitz/rules.html>

Hard Copy Resources-

Raptor Firewall & PowerVPN 6.5 Configuration Guide for NT - Axent Technologies -

Published by Axent Technologies

Implementing IPSec - Elizabeth Kaufman and Andrew Newman - Published by Wiley Computer Publishing

Network Intrusion Detection, An Analyst's Handbook - Stephen Northcutt - Published by New Riders

Software Resources-

Snort Lightweight Intrusion Detection System for Win32 - Free - Written by Martin Roesch @

<http://www.snort.org>, ported to Win32 by Mike Davis @

<http://www.datanerds.net/~mike/snort.html>

nmap for Windows NT - Free - Written by Fyodor @ <http://www.insecure.org/nmap>, ported to Windows NT by eEye Digital Security @

<http://www.eeye.com/html/Databases/Software/nmapnt.html>.

The PowerVPN and Raptor Firewall management console help files - comes with PowerVPN - see <http://www.axent.com> for more product information.

windump - Free - ported to Windows from the Unix tcpdump by Loris Degioanni, Piero Viano, and Fulvio Risso @ <http://netgroup-serv.polito.it/windump>.

tcpdump for Windows - comes with the RaptorMobile piece of the PowerVPN solution - developed by Axent Technologies @ <http://www.axent.com>.

Some other Internet resources were briefly referenced and used. They are noted throughout this paper where needed.

Tips

These are tidbits of advice that might come in handy.

- Don't forget to "Save and Reconfigure" when you make any changes.
- Check the log files!
- PowerVPN has an implicit deny rule. Anything that you do not give someone specific access to will be denied.
- Use descriptive names for the elements you create. When seen in one of the drop-down boxes of another element, the name is the only clue you will have as to what it is (i.e. *Group-Typical-User* is better than *Group1*)
- Make sure you have a written security policy before you start setting everything up. Your Firewall and VPN solution *enforces* your security policy, it doesn't define it.

FAQ

These are common questions end-users might ask you and some sample answers.

Why do we need something like that?

It can save you money and save the company money.

It can save you money if you already have an ISP. You would be responsible only for the charges from AOL, MSN, BellSouth.net, or whomever you are already using. If you are using a high-speed access provider like Time Warner's Road Runner cable modem or BellSouth's Fast ADSL, then a second phone line would no longer be needed just for a modem.

It can save the company money by removing the need for modem pools and the accompanying phone lines.

I like calling directly into a modem in my department, how is a VPN any better?

There are several reasons.

First, with a VPN, there is a centralized management point. There is only one system that remote people would be able to come in and out of the bank through. There would be no need for each department to have its own three or four modems sitting in a server room. With centralized management, there is less guesswork involved in finding someone who can resolve any issue or problem.

Next, it is much more secure. Someone using a war-dialer program can scan a group of phone numbers, find all the modems, and start hacking away. In addition, if the servers that the modem(s) are connected to aren't properly secured, then the modems become even more of a vulnerability. All connections to the VPN will pass through the firewall twice before entering the internal network; it is also much easier to assign the type of resources and specific machines available to each user at the VPN-level.

This sounds complicated. Will it require a lot more work on my part? The way I connect now is second nature; how hard will it be for me to learn some new method?

Unfortunately, using the RaptorMobile software will require you to learn some new procedures. The good news is that once the software has been installed and configured, it is relatively simple to connect to your tunnel(s).

I can use your existing NT domain account to authenticate you; that way you will be using a login ID and password that you are already familiar with and use on a daily basis.

Is there anything else that this VPN would be good for?

As a matter of fact, yes.

Currently, if a new acquisition wants to connect to the company network, some sort of dedicated line must be installed (56k, 64k, 128k, T-1, T-3, etc.) to connect them. They need access in order to get Exchange email, the Intranet, and mainframe sessions. A dedicated line carries a hefty install charge and a monthly fee.

Enter, the VPN. If a new acquisition already has an ISDN line or a T-1 in place for Internet access, they can leverage the same connection for access to the our network.

Depending on the size of the organization, they would need to have an IPSec compliant server on site to communicate with the PowerVPN server at our location.

© SANS Institute 2000 - 2005, Author retains full rights.