



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.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Branch Office connectivity: Private Frame to VPN's, makes dollars and sense.

David O. Boyden

May 04, 2003

GSEC V1.4B

Abstract

Virtual Private Network technology has been around for many years. The use of VPN's (Virtual Private Network) is ideal for communicating between business partners and for providing employees home access to their company resources. Confidential information can be encrypted and sent real time between networks and hosts over the Internet. Most companies already have Internet access and firewalls or other equipment that can support VPN's. With the standardization of VPN protocols and algorithms such as 3DES and IKE it makes it relatively easy for companies to communicate with each other even across multi-vendor platforms.

Over the past few years the stability of VPN technology has increased, so have Internet access methods. With the widespread adaptation of DSL (Digital Subscriber Line) the technology has become very stable. DSL is also very inexpensive, especially considering the amount of bandwidth available and the low costs associated with it. The scope of this discussion is not to dig into DSL technology itself but to demonstrate how this technology can be leveraged using VPN Dynamic's V6 firewall appliances and Checkpoint firewalls to replace Frame Relay or dial-up in certain instances while balancing the security risks, costs, management aspects and exposing the return on investment possibilities.

Can VPN technology over DSL work for me?

Whether or not you can move from frame relay to VPN's over DSL depends on many factors. Is DSL or Cable Internet access available in the area you would like to implement it? If so, what speeds are available and will the available speed be enough to support the small office using encryption? Is the DSL provider a reputable company, one that will hopefully stay in business? The DSL service must be stable so as not to diminish the quality of service the company expects and maybe used to.

You should also analyze all traffic patterns and host access requirements to determine how your existing bandwidth is used to support the remote location. What traffic must traverse the Internet to access hosts within your private network and therefore be encrypted? It is very important to have a complete understanding of the traffic access requirements. Some companies may have simple requirements and only require encrypted access to IP ports on a handful of hosts.

Other configurations can be much more complicated, for example, is your company running a directory such as Microsoft Active Directory? This must be accounted for and worked into the overall design to accommodate replication over the VPN.

Does your company have some sort of web content security (Web filter) system implemented? Many of the web content systems work like a data sniffer and monitor the data packets for web destinations and compare the locations to a database. The content filter then interrupts the user's web session if their destination has been flagged inappropriate. For this "sniffer" based technology to work the content filter must be on the same network segment the user accesses the internet through. By essentially moving the Internet access from traversing the private frame relay to now directly accessing the Internet at the remote location, the central web content filtering model no longer works. These are just some of the challenges in store.

Assessing the need, why should I switch?

One of the first questions you may ask yourself is why? Why should I move from a private, seemingly secure, frame relay network to using the Internet and VPN's? Many companies, including ours, use private frame relay to communicate between branch offices in a hub and spoke configuration. These companies may have many small remote offices that communicate over frame relay back to a central location. All internet communications from these remote offices traverse over frame to the central location then to the Internet. While this is a secure and effective configuration it is also expensive. Our small remote sites are running over 128k circuits, which is not a lot of bandwidth.

One of the main reasons to make the move from Frame to VPN is the cost savings and more effective bandwidth usage depending on your requirements and environment.

VPN's can save you money and more efficiently utilize your bandwidth.

One of our first locations we considered for conversion from frame relay to DSL was a small dispatching location. We have 7 computers and users that run a dispatching application that monitors service calls and allows the dispatch of personnel. This location in addition to the user P.C's had a file server and router to access resources at our central location. With the current hub and spoke frame relay configuration all traffic, including Internet web traffic, had to cross the 128k line back to our central office.

After analyzing the business application requirements for this remote location it was determined that by moving this location to VPN/DSL the only traffic that must traverse the Internet and therefore the VPN was database access to a few database servers, http/https access to the Intranet server and email access to a central email server.

If we were to move this location from Frame Relay to DSL we could split the traffic and have the general web traffic go straight to the Internet via the DSL provider and encrypt all other traffic that must communicate with resources back at the central office. This would make internet access faster at the remote site and reduce traffic on our main internet pipe at our central location.

The cost per month for the existing 128k frame relay was \$800.00. This was especially high due to the sites location and frame relay provider. After researching DSL access for this location we were able to get a 384k/1.5 Meg line for less than \$100.00 per month.

We decided to take a look at all of our small (25-user or less) branch locations and do an analysis on DSL availability and return on investment. We found 25-30 locations that were good DSL/VPN candidates. We also determined if we were able to move to VPN's and DSL at these locations we could save approximately \$18,000.00 per month.

Evaluating the risk, security and availability

In our hub and spoke configuration over 80 remote locations connect back to a central location and access the Internet via a central network and firewall cluster. While there are many security aspects to consider, currently the Internet access point is a single entry at the central office.

By moving remote offices from private Frame Relay to DSL VPN access, we just added another access point into our company network for each location moved. This means we must secure this remote office to ensure we have not created a backdoor or weak link into our private network that could be exploited. The remote VPN appliance must be configured to block all incoming traffic except legitimate encrypted traffic to and from the central office. The firewall appliance must only allow company approved outbound TCP/IP traffic to the Internet and only select encrypted traffic to the central office. Central traffic logging must also be enabled. In addition to the firewall security, the desktop computers must all have company approved anti-virus software that has been configured to auto-update its virus signature and program files. The workstations must also have the desktop locked down using Windows group policies to enforce a common desktop. This will help keep the users from adding programs to the system which is against company policy and may compromise security.

Availability and redundancy should also be considered. With Frame Relay our branch offices were spread across six T1 circuits using a few different Telco carriers. In this configuration we did not have a single point of failure. By moving branches to VPN access and all VPN's terminating to a single Internet firewall cluster and segment, we have major single point of failure.

If the main Internet access point at the central office were to go down so would all VPN's from the remote branches. This being said, I highly recommend implementing cluster technology and VPN redundancy on the central VPN termination point.

Firewall infrastructure and requirements.

Our central VPN access point is comprised of Checkpoint NG FP3 firewalls running on Checkpoint Secureplatform which is a pre-hardened Linux platform. (www.checkpoint.com) The central Checkpoint management server is running on Redhat Linux 7.2. The VPN appliance that will be used at the remote location is a VPN Dynamics V6 (www.vpndynamics.com) which runs Checkpoint Smalloffice NG FP3 firewall. By running Smalloffice NG we can centrally maintain the security policy and have all traffic logs at the remote location write to our central management server. The central logs in turn can be monitored and reports generated if needed.

After evaluating our needs for both small remote offices and remote dispatching locations we ended up with two remote configuration models. For our small 5-10 user dispatching locations that do not have local file servers we went with the VPN Dynamics V4 (www.vpndynamics.com). The V4 is essentially a Sofaware (www.sofaware.com) VPN appliance. These small dispatching locations are comprised of workstations and no other hosts. The workstations needed encrypted access to database servers, http Intranet servers and http based email. They also needed Internet http access.

Due to our limited budget for the remote dispatching locations, the configuration options with the V4, the remote office access requirements and the relatively low cost of the V4 made it a suitable appliance for this type of remote location.

For our larger offices with 25-30 users which currently have a Windows 2000 server for network authentication and running active directory we needed an appliance that would allow more management and security policy granularity. These sites also require web content filtering. For these reasons the VPN Dynamics V6 was chosen. The plan is to replace the remote branch router and frame relay with the V6. The Windows 2000 server would stay, and the VPN would be configured to allow Active directory replication, DNS and other necessary traffic to flow to and from the central office location. In addition, for web content filtering, Surfcontrol (www.surfcontrol.com) would be installed on the remote Windows 2000 server to enforce our web content policy.

IPSec Configuration

The VPN's between the remote office locations and the central office network will be established with IPSec using IKE (Internet Key Exchange) for key exchanges. AES-256 (Advanced Encryption Standard) will be used for encryption. Most reports state AES is around three times faster than 3DES.

IKE exchanges consist of two phases. Phase 1 uses Diffie-Hellman, group 2 (1024 bit) for the shared secret exchange. During phase 1 an SA (Security Association) is created which consists of the negotiated encryption method, authentication method and keys.

During Phase 2 the SA generated in Phase 1 will be used to encrypt the IPSec data. The encryption will be AES 256 and the data integrity or authentication algorithm will be SHA1.

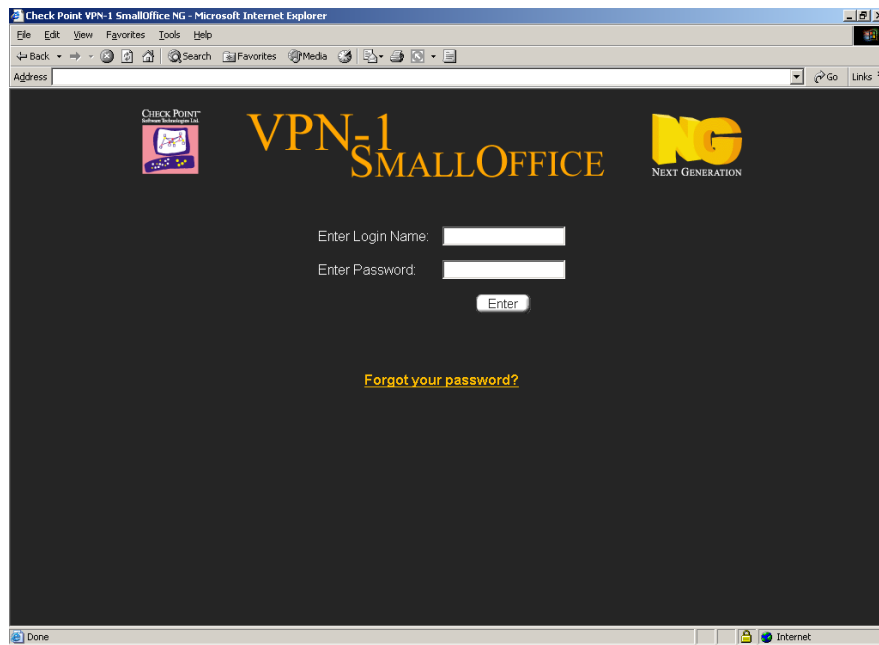
V6 Initial configuration (Branch office appliance).

The V6 is a hardware appliance running Linux and Checkpoint small Office with three 10/100 Mb Ethernet ports. The ports are labeled “DMZ”, “Office” and “Internet”. The “Internet” port connects to the DSL or cable modem Ethernet port. The “Office” port connects to hubs or switches that will be protected behind the firewall. The “DMZ” port can be used to attach a web server or other host that should be isolated on its own segment. The unit can be purchased pre-licensed for 5, 10, 25 or 50 IP addresses to protect behind the appliance. The V6 also has a local console port that allows you to login to the Linux operating system. Windows HyperTerminal can be used to connect using 115000: N: 8:1 with flow control set to none. From the terminal you can verify configuration, start and stop the firewall and run various Linux OS and firewall commands.



http://www.vpndynamics.com/vpn/images/products/v6/001_rear.jpg

The appliance is initially configured via a web browser. Plug a P.C into the “Office” port using the provided crossover cable. Configure a static address on the P.C of 192.168.1.101 with 255.255.255.0 as a subnet mask. The default gateway is not necessary at this point. The management interface is initially accessed by connecting to <https://192.168.1.1> from a web browser. Once connected to the management address you may be prompted to accept the certificate, accept the certificate and you will be presented with the following logon page.



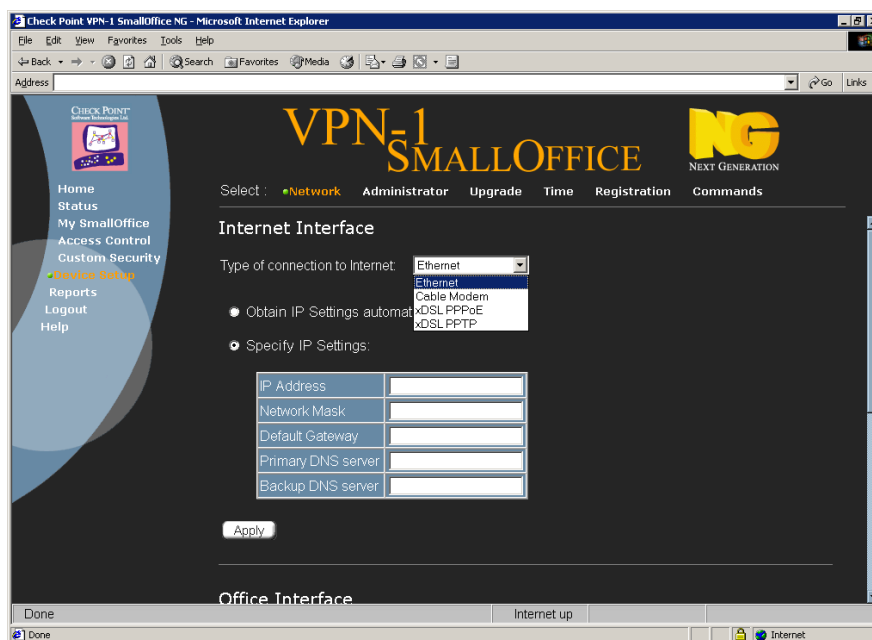
The default user account is “admin” with “admin” as the password. Logon using these credentials, and you will be presented with an option to change the username and password. Change the account and password at this time.

Configuring the V6 Interfaces

The “Internet” interface on the V6 appliance must be configured to establish internet connectivity. Our remote office DSL is using a static IP address. The available options for the Internet port IP configuration are Ethernet (static IP), Cable Modem (DHCP), DSL PPPOE, or PPTP.

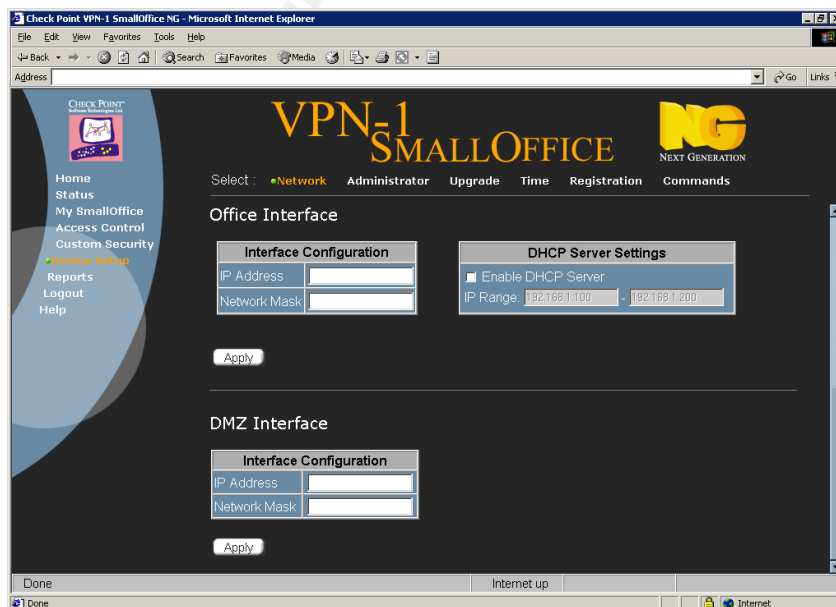
The first step is to configure the “Internet” port for Ethernet and enter in the IP address, Network mask, default gateway and DNS servers. This information should be provided by your DSL provider. Once the interface is configured select “apply”. Below is a screen shot of the “Internet” interface configuration screen.

© SANS Institute
Unauthorized
Distribution



The next step is to configure the “Office” port subnet address. The “office” port is the inside interface you will have your hosts connected to. The “office” port is configured by default to use a RFC 1918 address (192.168.x.x). This address will be changed to a unique RFC 1918 address (172.16.x.x) to eliminate IP and routing conflicts with other private subnets located behind the central office firewall. You can assign the subnet of your choice.

Under the “Office” interface section enter in the IP address and subnet you want assigned to the interface and select “apply”. If you want to use DHCP you can also enable DHCP and define a range of IP addresses you want assigned.



All destined internet traffic from the hosts connected via the “office” port will be network translated behind the outside IP address of the wan port and communicate directly to the Internet. The “DMZ” port will not be configured since we will not be using it for our branch office.

Establishing connectivity with the central office firewall.

Once the V6 has been configured for Internet connectivity and the LAN subnet has been configured with its unique subnet, the V6 needs to be configured to communicate with the central office firewalls. All firewall rules will be defined centrally using Checkpoint management and pushed to the V6 appliance over a secure connection across the Internet.

The V6 is configured by default to run in “stand-alone” mode. We need to change the configuration from stand-alone to “Join VPN” which basically sets up the appliance to be centrally configured and managed under the Checkpoint NG smartcenter using the Checkpoint SmartDashboard GUI management tool. Login in to the V6 appliances using a web browser connecting to the new IP address assigned to the “Office” interface. Use the new administrator account and password that you defined earlier in the configuration process. From the main menu select the “My Smaloffice” menu option on the left side of the screen. The following screen should appear.



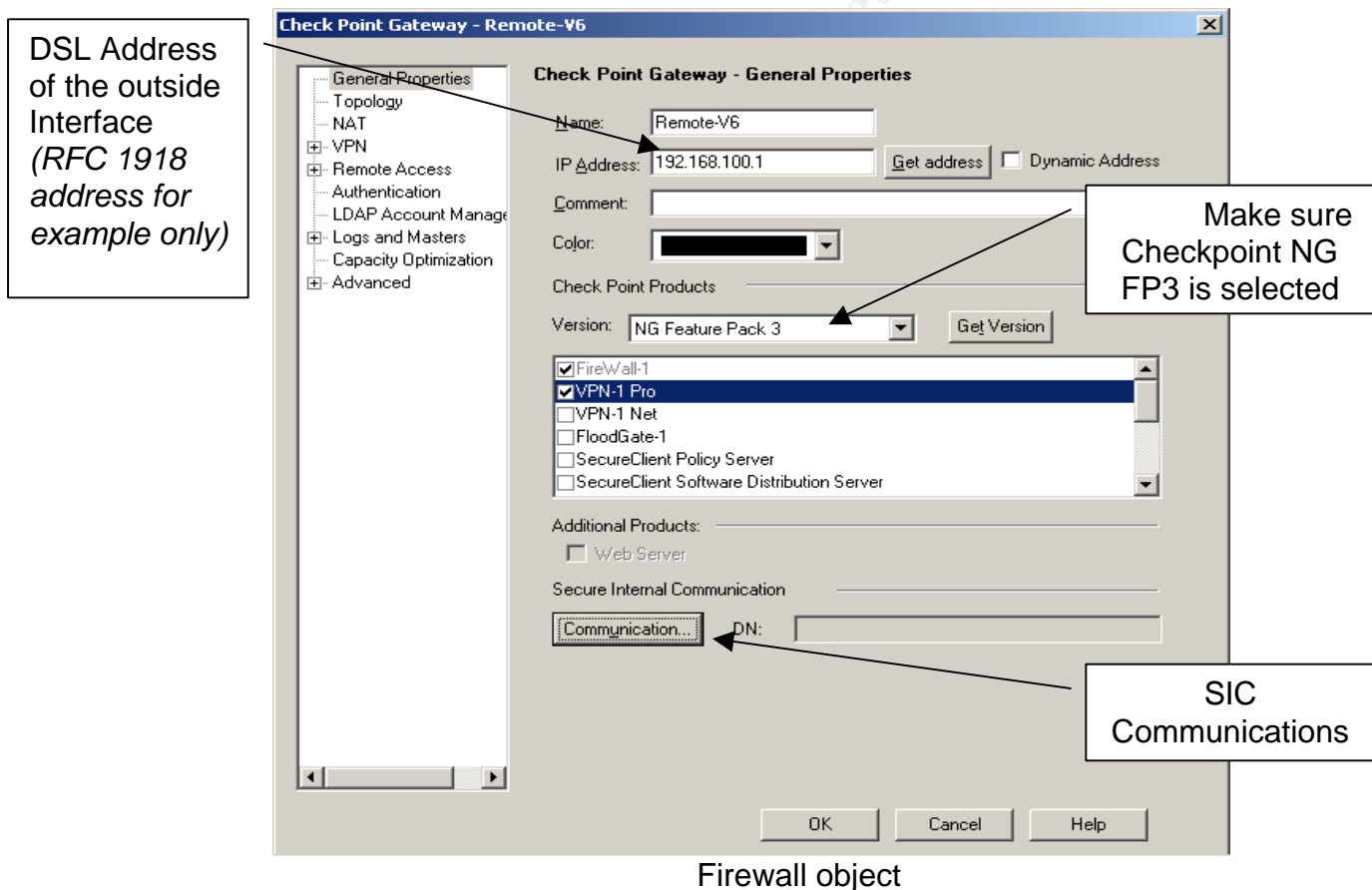
Change the “Control Mode” from Stand Alone to “Join VPN” You will now need to enter an “Activation Key” into the field provided under the Smartcenter Server configuration section shown above.

I recommend the activation key being alpha numeric, upper and lower case and at least 10 characters in length. The activation key is the shared secret

used to initially establish the secure communication back to the central firewall. The activation key equates to the “SIC” or Secure Internal Communications, which is the communication process that must also be configured on the firewall object that will be created on the main firewall system to represent the V6 firewall appliance. “SIC” is used to provide a secure communication channel for managing the Checkpoint Smaloffice firewall which includes managing the rule base, central logging, and other communication processes necessary between the V6 Smaloffice appliance and the central management firewall system.

Checkpoint NG FP3 Configuration

Once the activation key has been set on the V6, a firewall object must be created in the central office security policy to represent the remote V6 appliance. Using the Checkpoint SmartDashboard configuration utility, create a firewall object. The outside (DSL) address of the V6 must be the primary IP of the firewall object being created.



Communication [X]

The Activation Key that you specify must also be used in the module configuration.

Activation Key:

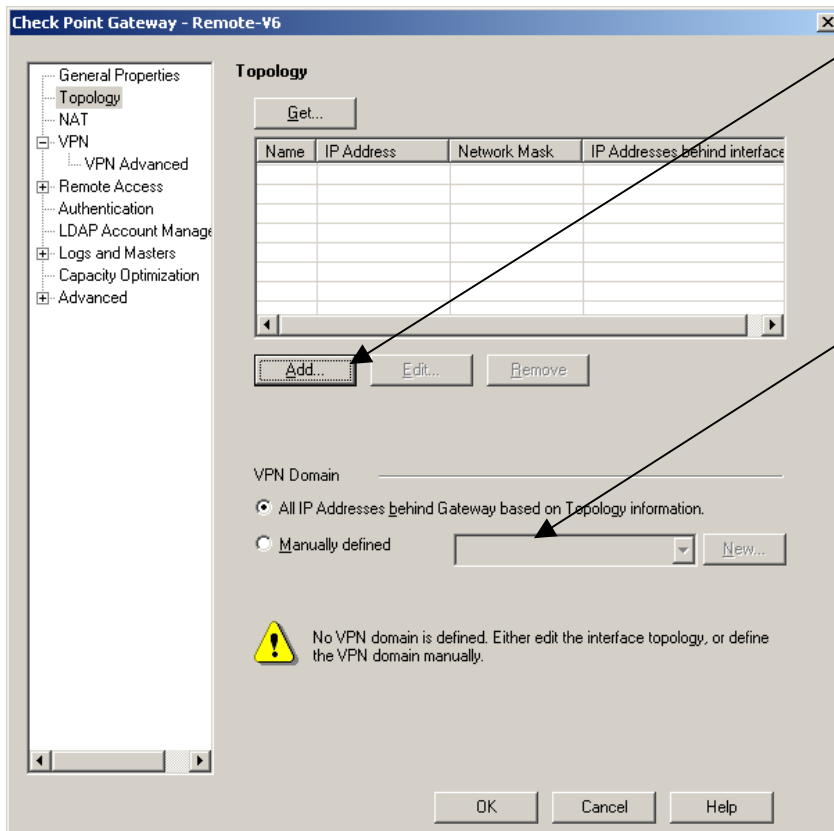
Confirm Activation Key:

Trust state:

Enter in the same activation key used when configuring the V6 firewall. Select "Initialize". At this point a secure communication link should be established with the remote V6 unit and the Checkpoint management server.

The "Sic" communication needs to be set on the newly created firewall. Select the "Communication" button on the "General Properties" screen.

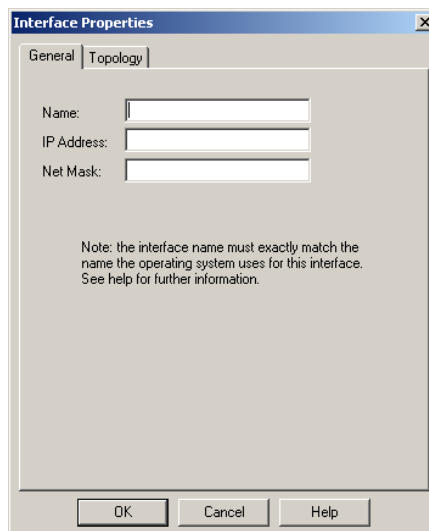
© SANS Institute 2003, All rights reserved.



Use this button to manually add the interfaces that were configured on the V6.

This is the VPN encryption domain. This dictates which networks behind the firewall may be encrypted or decrypted. Networks must be part of the encryption domain and explicitly defined in the rule base to participate in the VPN.

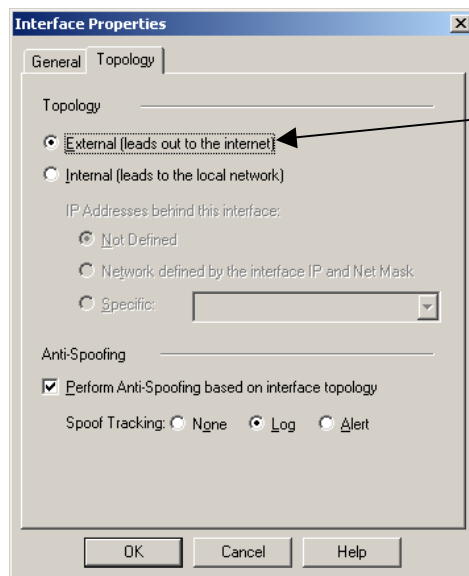
All interfaces of the V6 should be added to the object under the “Topology” section. Since the SIC trust has been established you can select the “Get” button to retrieve the interface information automatically. Otherwise define the Internet (Outside) and Office (Internal) network manually by selecting “add” and entering in a name, the IP address and interface.



(Screen shot of interface configuration window)

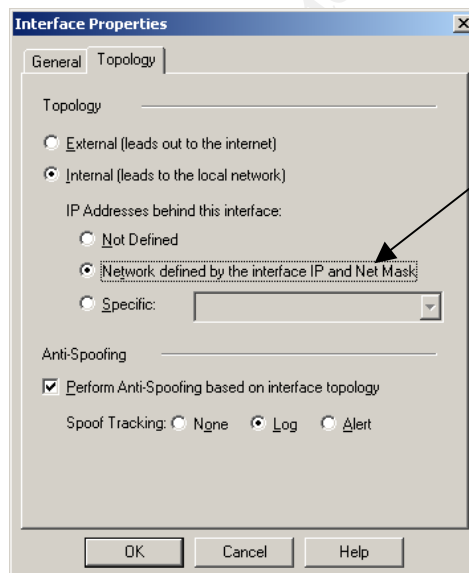
Anti-Spoofing

Anti spoofing should also be defined for each interface. By enabling anti-spoofing packets are examined to ensure the packet is valid for that interface. This prevents packets coming through an interface with a spoofed address of a trusted network. To enable anti-spoofing select the "Topology" tab on the interfaces properties screen. The external facing interface (Internet) should be configured as "External" select the "log" option under spoof tracking.



This is the external interface facing the Internet. All packets are allowed through this interface as long as they don't have a source address belonging to a network defined behind one of the other interfaces.

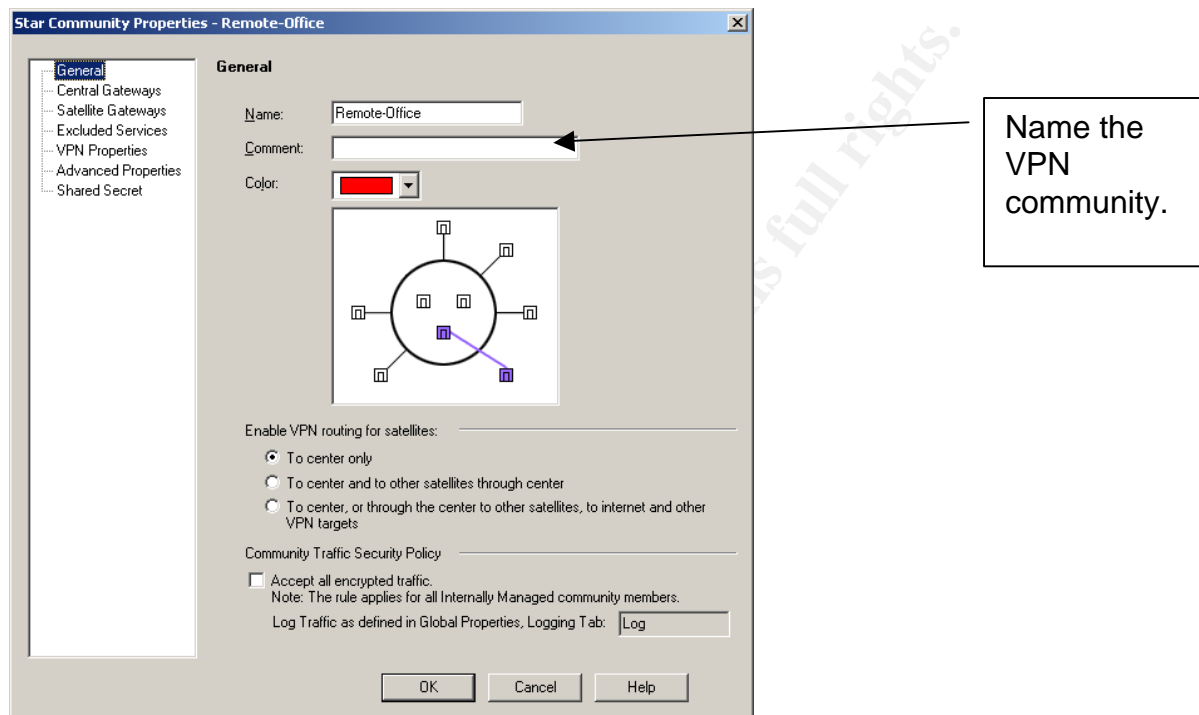
The internal network interface should also have anti-spoofing enabled as illustrated below.



This will only allow packets with a source address that is part of the defined network defined by the interface configuration.

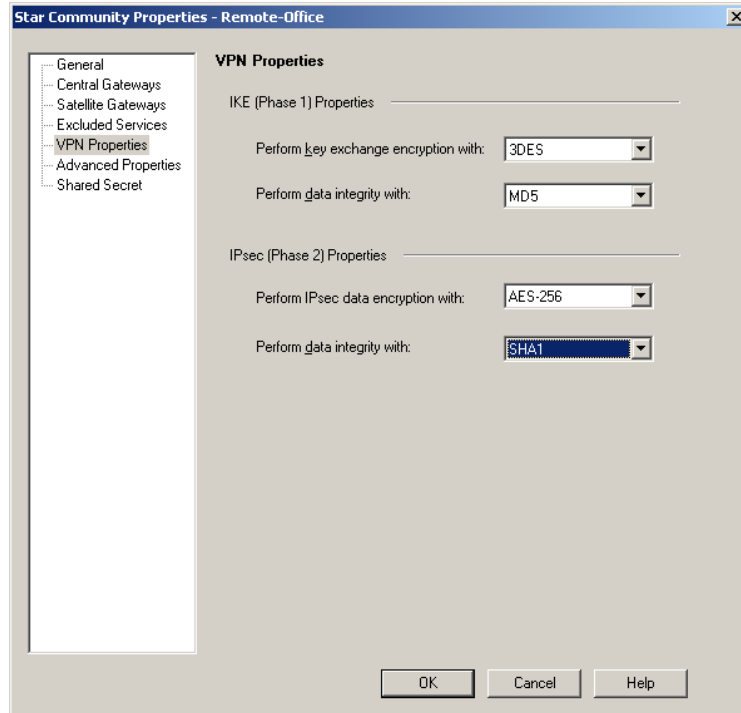
Configuring encryption and creating the rule base.

Now that “SIC” has been successfully initialized and the remote V6 firewall object has been configured, a VPN community needs to be created. The “VPN Community” will define the encryption configuration for the remote V6 firewall and the firewall at the central office. Under the “VPN Communities” tab within the SmartDashboard tool create a new VPN community.



The above setting will work well for our branch to central office VPN. Under the “Central” gateway tab add the central office firewall that will be participating in the VPN with the remote office. The remote V6 firewall will be added under the “Satellite” gateway tab.

Configure the encryption configuration under the “VPN Properties” tab.

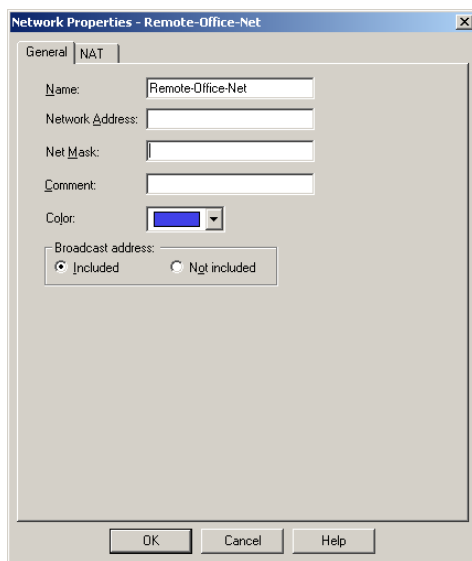


This is where the encryption algorithms are defined for the community. Since both the Central firewall and the remote are part of the above community the encryption setting configured will apply to both firewalls.

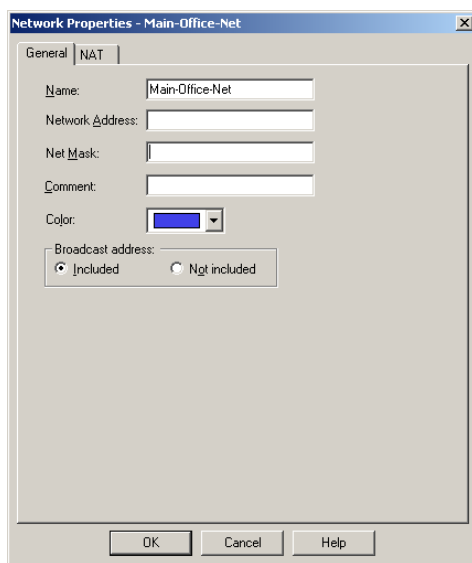
Configuring the security policy

The V6 is now ready for a security policy to be installed. The security policy is essentially the rule set that defines what communication is allowed through the firewall. Security policies are created using the Checkpoint SmartDashboard which is a client interface to the Checkpoint Management server. The policies are created using the GUI and saved on the central office management server. Once a policy has been defined it is “pushed” or downloaded to the remote firewalls. In our case the policy will be installed on our central office firewall and the remote office V6 firewall appliance. The Checkpoint management server is used for many purposes including centrally housing the security policies and receiving the logs from the remote firewalls.

Our next step is to create two network objects. One will represent the network behind the remote V6 firewall. The other object will represent a network behind the central office firewall. These network objects will be used in the security policy rule base to define the encryption rules between the central and remote networks.



Create one object that represents the remote network as shown above.
Create a second object that represents the central office network.



Now we will create a few rules using the SmartDashboard client tool. One rule will be used to decrypt all traffic from the remote office network to the central office network via the remote-office VPN community we created earlier in the processes. The second rule will encrypt all traffic from the central office network to the remote office network. In addition to the encryption rules we will have a third rule that allows HTTP and HTTPS only from the remote network to the Internet. The last rule is the clean up rule which drops all other traffic and logs the drops.

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
Remote-Office-Net	Main-Office-Net	Remote-Office	* Any	accept	Log	* Policy Targets
Main-Office-Net	Remote-Office-Net	Remote-Office	* Any	accept	Log	* Policy Targets
Remote-Office-Net	* Any	* Any Traffic	TCP http TCP https	accept	Log	* Policy Targets
* Any	* Any	* Any Traffic	* Any	drop	Log	* Policy Targets

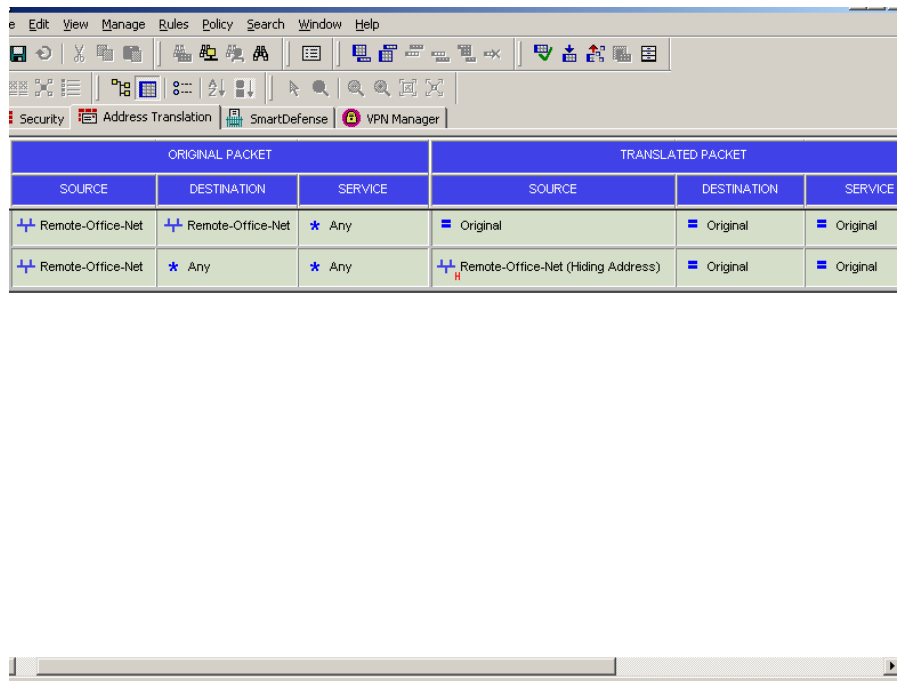
Simple rule based policy

The above policy will be pushed or downloaded to both the central office firewall and the remote V6 firewall. Notice the above rules list “any” for the services allowed over the VPN tunnel. All services will be allowed and encrypted. I recommend tightening this to allow only necessary services required for proper communication between servers, applications, management functions, etc. Basically all traffic necessary for proper communications. If you are unsure what services need to be open you can monitor the firewall logs while allowing all traffic. This is one way of determining which ports are being used. You can also determine this by connecting a network analyzer such as a sniffer to the local network being the firewalls and examining the traffic before it’s encrypted or after it’s decrypted.

Configuring Network translation

The remote office will also need http and https access directly to the Internet. So far we have most of the rules in place. We still need to add a network translation rule to hide the internal network (RFC 1918 IP addresses) behind the IP address of the outside interface of the V6 remote firewall. This will cause all internet bound traffic from our remote network to appear as if it’s coming from the single IP address of the outside “internet” interface address assigned by the ISP. With hide translation the firewall keeps track of the internal “real” translated addresses and source ports of each connection. The firewall modifies the original source port of outgoing connections and replaces the port with a dynamically created port number; this information is placed in a translation table. This process enables the firewall to keep track of its translated connections. The return packets are then matched up to the source port in the

firewalls translation table and the real source port and IP address is replaced and the packet is delivered to the host. This completes the Nat communication process between the internal host using hide mode translation and an Internet host. The following two rules define the Network Translation and cause the remote office Internet traffic to “hide” behind the external IP address of the V6.



ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
+ Remote-Office-Net	+ Remote-Office-Net	* Any	Original	Original	Original
+ Remote-Office-Net	* Any	* Any	+ Remote-Office-Net (Hiding Address)	Original	Original

Network Translation rules

Web Content Filtering

By moving the remote office from frame relay to VPN the remote office is now directly accessing the internet through the remote V6 firewall. This bypasses our content web content filter located at the central office. For this reason we elected to install Surfcontrol on the remote office Windows 2k server. Surfcontrol is configured to block and report surfing attempts to a number of categories. The windows 2k server sits on the same hub as the internal interface of the V6 firewall. Since Surfcontrol uses a “sniffer” type of technology it does not cause performance degradation. It simply watches the web traffic and compares the destinations to the subscription database. If a user attempts to access a site that is in one of the categories we elected to enable, the web session will be redirected to a web page that informs the user the site they attempted to access is restricted. All web access is logged to an access database. Reports are automatically generated and emailed to management.

Conclusion

With the proper VPN and firewall infrastructure you can leverage DSL technology to create a secure yet cost effective alternative to frame relay, dial-up or other private leased line technology. In my example Checkpoint software and VPN Dynamics appliances were used. This can also be accomplished with a number of different vendor platforms. With the proper planning and resources a secure and reliable VPN alternative to frame relay can be developed.

References

1. Cheng, P.-C. "An Architecture for the Internet Key Exchange Protocol". March 30, 2001
URL: <http://www.research.ibm.com/journal/sj/403/cheng.html>
2. Perlman, Radia Kaufman, Charlie "Key Exchange in IPsec: Analysis of IKE".
URL: http://snoopy.seas.smu.edu/ee8392_summer01/week7/perlman2.pdf
3. Phoneboy.com "How NAT works". 2002-Nov-12
URL: <http://phoneboy.com/fom-serve/cache/77.html>
4. VPN Dynamics V6 Datasheet.
URL: http://www.vpndynamics.com/vpn/pdf/v6_datasheet.pdf
5. Federal Information Processing Standard Publication 197
Nov 26, 2001. "Announcing the Advanced Encryption Standard (AES)"
URL: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
6. Check Point Software Technologies, "VPN-1/Firewall-1 NG FP3 Management I Student addition" 2002
7. Surfcontrol
"Web Filter Users Guide Version 4.2" 2002.
http://www.surfcontrol.com/general/guides/web/SCWF_UserGuide_v42.pdf
8. RFC 1918 "Address Allocation for Private Internets" February 1996
<http://www.ietf.org/rfc/rfc1918.txt>