GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

VPN Architecture and Design for

CompanyX

GSEC Practical v.1.4b Option 2

Ajay K. Sood

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

This document summarizes the rationale and strategy which was employed in the construction of a global Virtual Private Network (VPN) for CompanyX. CompanyX's requirements are stated, as well as the risk and business drivers behind this initiative. An abstract scenario and generic design is presented, and the final design as implemented is discussed. Part of this discussion is a detailed summary of the sequence of steps followed in order to bring this design into being.

A detailed look at the technology and components of this solution is provided, and a functional validation of this design in a lab environment is presented. This proof of concept was provided to the CompanyX project team for implementation. The final design is presented, and detailed sequence of implementation steps is outlined. Finally, an overview of the enhanced state of security is provided.

© SANS Institute 2003, Author retains full rights.

1 Synopsis

As with many contemporary enterprises, CompanyX is undergoing extensive growth. Conversely, this growth has precipitated an impetus for CompanyX to conduct business in the global economy, requiring international collaboration among CompanyX employees. From this requirement has sprung a global connection initiative.

Studies as to the methods of accomplishing this union were then undertaken, and several options, such as Internet Virtual Private Network, dedicated connectivity (frame relay connection, ATM, etc.), or clear text Internet routing were weighed for feasibility, cost, and organizational acceptance.

Conclusions from this study were fairly pedantic, in that the solution had to be cost effective, with no sacrifice or compromise in the domain of security. It was decided that whether or not shared or dedicated connectivity was in use, that encryption would be a key requirement. The fact that all sites were currently Internet connected figured strongly into the decision making process.

The decision to connect CompanyX's international offices via Internet Virtual Private Network (IVPN) was subsequently made. Security was identified as a key enabler for this project. The scope of this project was to ensure that CompanyX's global information was to be transmitted securely, or in a manner that was confidential, integral, and highly available. As well, the solution must be scaleable, in order to accommodate additional sites, or growth within sites, with minimal down and integration times.

The purpose of this document is to detail the design of this solution. The initial situation will be stated, the requirements summarized, and the solution presented. A progressive cutover process will then be presented, with some intermediate steps.

Section 2 describes pre-planning and analysis of the problem at hand, while Sections 3 and 4 describe the design and rollout steps undertaken for this project.

N.B. All trademarks used in this document are the property of their respective owners.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2 Situational Analysis (Pre-Implementation)

2.1 Existing Technology

CompanyX has typically imposed security controls in efforts to secure the organization's assets. Such measures include, but are not limited to the integration of Internet firewalls at the various points of entry throughout the enterprise. As well, CompanyX currently makes use of VPN endpoints in order to secure inter-office communication.

Principally, CompanyX uses Check Point FireWall-1 for its Internet firewall. This product is recognized as an industry leader in the security space, and runs on a Nokia firewall appliance, also a well-respected platform. This stateful firewall is capable of enforcing detailed security policies, as well as tracking traffic which passes through it. Conversely, this firewall can be centrally managed and audited, making it a powerful tool for security policy compliance. Large deployments of Check Point FireWall-1 can be conveniently managed through an enterprise-class graphical user interface (GUI) [2].

The VPN concentrators used by CompanyX are the Nokia CryptoCluster series of VPN devices. These devices enable high performance VPN connectivity between sites, and have a tremendous depth of VPN topology and routing functionality. Several keying, authentication, and encryption methods are supported. Over and above, the CryptoCluster can be configured in highly-available clusters, which can be leveraged to eliminate single points of failure, and increase aggregate throughput [3].

Otherwise, Nokia CryptoClusters only boast a limited logging and reporting mechanism, which must be complemented by an external logging engine in order to generate truly meaningful logs and reports. As well, the Nokia CryptoCluster cannot act as a stateful firewall gateway, and is limited to Network and Port Address Translation (NAPT) and layer 3 filtering, using access lists (ACLs). The CryptoCluster product is also managed through an intuitive GUI, capable of easily managing multiple devices.

2.2 List of Locations

CompanyX has listed the following locations as candidates for this VPN initiative:

- Markham
- Chicago
- California
- United Kingdom
- France
- Germany

These will be the sites considered in this document, although the presented solution can be scaled to accommodate additional sites.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.3 Current Issues

CompanyX has several security concerns with its current design, which is an unsophisticated fully-meshed VPN infrastructure. Currently, all traffic is permitted between sites, with no logging or traffic enforcement imposed on the VPN. As well, direct Internet access from Satellite sites is of prime concern, as it is currently unrestricted, and the end users benefit only from the protection that their VPN gateways offer, namely network address translation, with no stateful inspection.

The exposures are very real; protocol weaknesses, as well as a host of Internet based attacks are available to a potential exploiter, as their VPN gateways cannot be relied upon to perform many tasks, including the following:

- Attack detection and logging
- TCP Sequence checking
- UDP response timeouts
- SYN flood denial
- Protocol anomaly detection
- Intrusion protection (also known as intrusion detection)
- Port scan protection

Additionally, the regulation of traffic between sites is a concern. A risk analysis has yielded that the greatest risks are associated with the hub sites, since this is where most, if not all of the intellectual property of CompanyX resides. It has been identified as a risk that unregulated internal traffic across the mesh must be curtailed. An abstraction of CompanyX's network is in Figure 2.3.1. Note that each numbered site is Internet connected, where only sites 5 and 6 have true stateful (Check Point) gateways, and all other sites have direct Internet access, as well as an unregulated VPN connection to all other sites.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

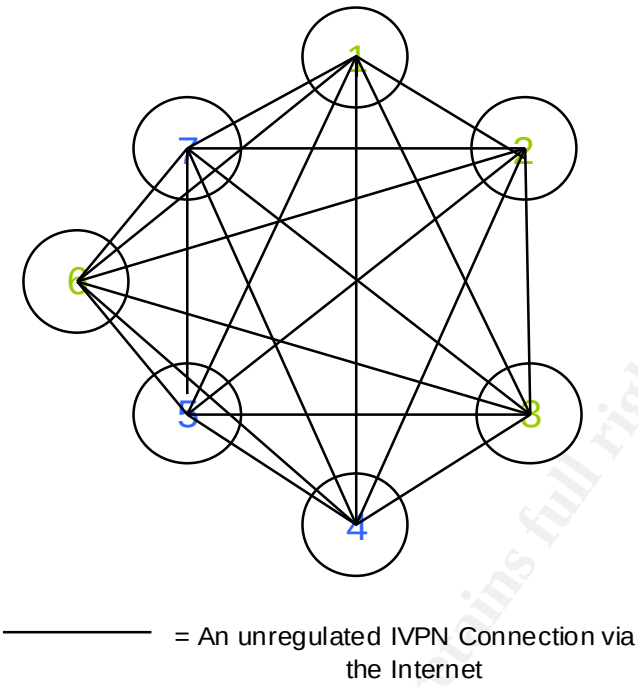


Figure 2.3.1 – Current situation at CompanyX

Therefore, the security exposures from any site truly become the security vulnerabilities of all other sites, and in particular, the hub sites (5 and 6), where company confidential and secret assets are stored.

© SANS Institute 2003, Author retains full rights.

3 Requirements and Rollout Planning

3.1 VPN Requirements

The following sections serve to briefly detail the requirements of the IVPN infrastructure to be implemented for CompanyX.

3.1.1 Data Encryption (Confidentiality)

It has been specified that the data must be encrypted in transit, and protected against third party interception. Therefore, the CompanyX IVPN will use 3-DES (triple data encryption standard) algorithm for rendering data in transit unintelligible. As well, Diffie-Hellman key exchange algorithms will be used to protect IKE session keys (Group 5). Also, Perfect Forward Secrecy (PFS) will be used to eliminate the interdependency between present and future keys [4].

3.1.2 Data Integrity

Another key requirement is that the data be protected from modification. The data in transit will make use of hashed message authentication code (HMAC), to guard against message modification. The chosen hash method will be SHA-1 (Secure Hashing Algorithm – Level 1) [4].

3.1.3 Authentication

In order to properly identify the gateways to each other, strong certificate policies will be used to protect the traffic. Since CryptoClusters can be configured as Certificate authorities free of charge, one would be inclined to leverage this feature to generate a strong means of authentication, rather than using weak password authentication (shared secret [4].

3.1.4 Centralized Traffic Flow

CompanyX requires that all Internet traffic pass through what they have defined as their *hub sites,* where a complete Internet perimeter solution is in effect. Hub sites are hereby defined as sites which contain a true stateful firewall, as well as other perimeter defense elements, such as anti-virus filters, content screening filters, intrusion detection engines, and other security measures. Tributary sites, which will feed all internal and Internet-bound traffic through these hubs, will be defined as *spoke sites*.

The reason hub sites have been provisioned is to lessen the cost of the overall solution by eliminating the need to replicate CompanyX's perimeter defense system at every Internet connected site. By ensuring that all Internet-bound traffic is pushed through hub-site gateways, CompanyX can reap the benefit of stateful inspection, content-filtering, anti-virus, and other protection mechanisms throughout their organization. No traffic is to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

traverse spoke gateways unencrypted. This also presents the advantage of having a central point of Internet access logging [2].

Additionally, this requirement has been set forth in order to mitigate the deficiencies of the lower cost VPN-only devices at the spoke sites. These devices must be configured to drop all traffic, other than that required to set up VPN tunnels (IKE, AH or ESP, as well as administrative traffic). It is imperative that these devices also be configured to force all traffic through the VPN tunnel, irrespective of whether or not the traffic is Internet bound. The NAPT functionality should be disabled as well.

Disadvantages of this configuration are few, but notable. Throughput for Internet requests will be lower, as they will incur encryption overhead, as well as additional latency. Also, additional capacity will have to be provisioned at the hub sites, as they will be providing Internet services, as well as encryption services for many other sites. The key to successful implementation from a connectivity perspective is to ensure that Internet bandwidth is well provisioned, and that traffic is efficiently routed through the VPN.

3.1.5 Spoke Traffic

It has been determined that spoke traffic will have to be carefully handled. In the case of Internet-bound traffic, the spoke site will send its traffic through the VPN cloud to the nearest hub, where it will traverse the hub site's firewall to the Internet. The return traffic will then come back through the hub firewall and continue back through the VPN to the spoke site.

If traffic must pass between spokes, this traffic will be routed through the respective hub site(s). In the event that two spokes have different hubs, than this traffic will be routed through the nearest hub, to the destination hub, and on to the destination spoke. Return traffic will be handled similarly.

3.1.6 High-Availability and Redundancy

High availability should be considered as a must for the hub sites. The Nokia VPN devices as well as the firewalls should be configured in high-availability pairs or clusters as the case may be. This can be extended to all other sites, in order to eliminate the single points of failure, but is more is more critical at the hub sites, as an outage there would result in a catastrophic loss of a large portion of CompanyX's VPN traffic. The subsequent design and discussion can be extended to include this level of redundancy [1].

Additional measures can be taken in order to ensure the availability of the VPN such as using multiple redundant Internet connections, as well as routing protocols, to further armour the system from network failures.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2 VPN Abstraction

3.2.1 Identification and Classification of Sites

The requirements discussed in section 3.1 can thus be summarized with a brief topological discussion, particular to CompanyX's environment. The identification and classification of CompanyX's locations is summarized in Table 3.2.1:

Site Number	Site Name	Site Type	Site Hub	Firewall
1	France	Spoke	United Kingdom	None
2	Germany	Spoke	United Kingdom	None
3	Hong Kong	Spoke	United Kingdom	None
4	California	Spoke	Markham	None
5	Markham	Hub	N/A	Check Point
6	United Kingdom	Hub	N/A	Check Point
7	Chicago	Spoke	Markham	None

Table 3.2.1.1 – VPN Site Classifications

Note that the hub and satellite sites have been chosen for their respective geographical proximities. It is subsequently possible to divide CompanyX's locations into two groups based on the location of their hubs. Sites whose hubs are the Markham location shall be referred to as Markham spokes, and the sites using the United Kingdom (UK) site as their hub shall be referred to as UK spokes.

3.2.2 VPN Topology

The CompanyX VPN can effectively be expressed as two forced hub and spoke topologies, connected by a VPN between hubs. The traffic flow of the VPN design is illustrated in Figure 3.2.2.1. The numbered elements in the figure refer to those in Table 3.2.1.1:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

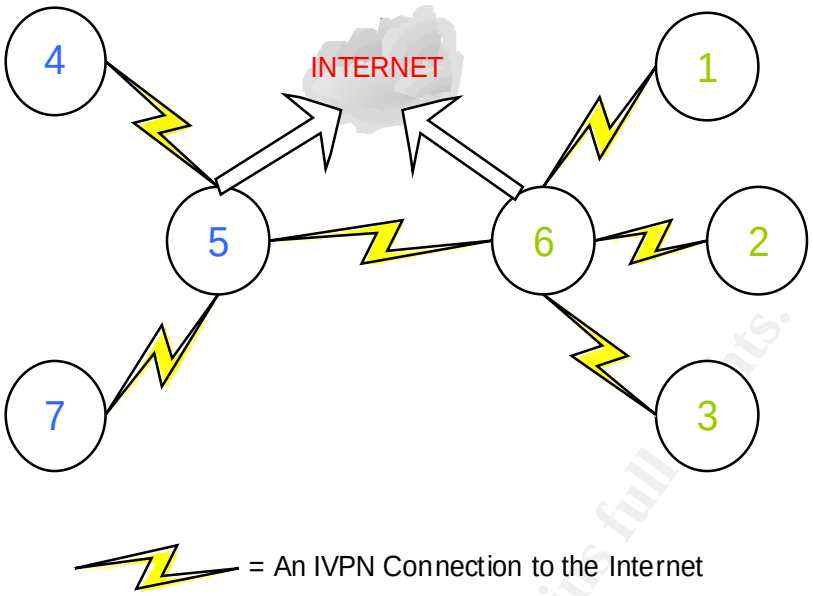


Figure 3.2.2.1 – Topology of CompanyX's VPN

Per Figure 3.2.2.1, traffic from Site 4 to Site 7 would pass through Site 5 (the nearest hub), and traffic from Site 7 to Site 1 would pass through Sites 5, 6, and 1 respectively. Internet Traffic from sites 4, 5, or 7 will traverse site 5, and Internet traffic from sites 1, 2, 3, or 6 will traverse Site 6.

© SANS Institute 2003, Author retains full rights.

3.3 Final VPN Network Design

From the discussions in Section 3.2, a basic Network Diagram can now be completed, including the major functional units such as the Nokia firewalls and CryptoClusters (Figure 3.3.1). It should be noted that the Markham VPN is represented in blue, while the UK VPN is in green. Both hub sites contain Check Point firewalls on Nokia IP440 platforms, which act as Internet gateways for their respective sites.

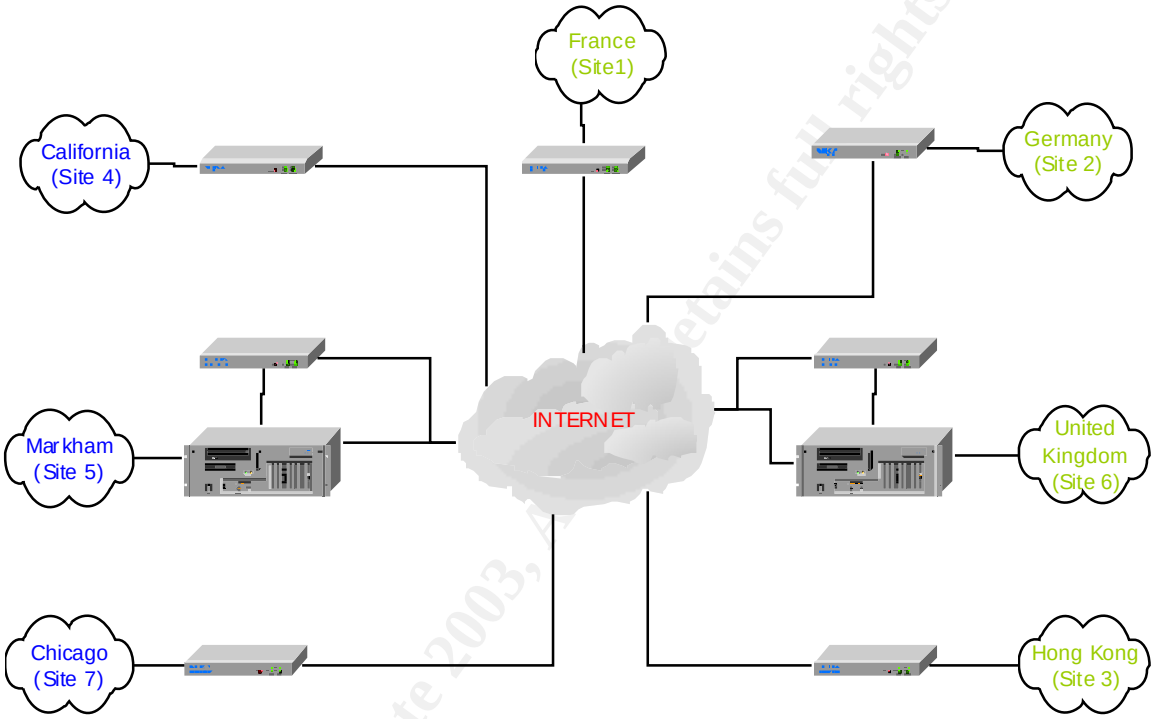


Figure 3.3.1 –VPN Network Diagram

As can be derived from Figure 3.2, all sites are actually Internet connected, but the traffic flow will be as in Figure 3.2.2.1.

Some attention should be drawn to the fact that the CryptoCluster VPN concentrators at the hub sites are connected to a separate network interface on their respective firewalls. This is to further protect the assets at the head site, as all ingress traffic will be inspected by the stateful gateway.

The default routes of the hub site CryptoClusters are set to be the internal interface of the firewall on the segregated VPN interface, and the firewall then sends the packets to the Internet provider's router. This design ensures that no traffic will pass to the Internet un-inspected. The hub site CryptoCluster devices contain static routes pointing directly to the provider's router for the protected networks to be encrypted. Although useful, stateful inspection was not deemed necessary for internal traffic [2].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The security policies of the firewalls should be configured to permit traffic from the VPN spoke sites associated to the hub. Naturally, network address translation should be enabled on the firewalls to ensure that the Internet-bound traffic will be routed properly across the Internet, and back through the firewall (and subsequently back through the VPN, should the case apply). The firewalls should also be configured to allow connections from the internal networks out to the rest of the VPN sites, as well as permit the inbound connections from the rest of the VPN sites.

Special care must be taken in the configuration of the head site perimeter, since this will be the central egress for the entire spoke group. Intrusion detection systems, and audit trails should be in place, as well as any other content screening technologies.

The method by which this can be achieved is summarized in a generic proof of concept in Section 4, which can be applied to this case with little difficulty. Section 4 presents a simplified model for implementing this topology, with greater detail.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4 Proof of Concept (During Implementation)

This section focuses on the steps required to configure the design from Section 3, and contains configuration-specific information with respect to implementing forced-tunnel architectures.

4.1 Hardware and Software Dependencies

The following configurations were all undertaken using the following hardware and software level [1]:

Check Point Firewall

Hardware:	Nokia IP650
Operating System Level:	IPSO 3.6 FCS4
Firewall Version:	Check Point FireWall-1/VPN-1 V. 5.0 (NG) Feature Pack 2
Firewall Policy Editor:	Feature Pack 2

* Check Point software available at www.checkpoint.com/techsupport/downloads
* Nokia software available at support.nokia.com

Nokia CryptoClusters

Hardware:	Nokia CC500 (Site 1, 2, 3, 4, 5) Nokia CC2500 (Site 6 and Router)
Boot Manager:	2.01
VPN Code Level:	Nokia VPN 4.1 (build 68)
VPN Policy Manager:	Version 4.1 (build 25)

* Nokia software available at support.nokia.com

Management PC

Operating System:	Microsoft Windows 2000, Service Pack 2

4.2 Proof of Concept

The infrastructure to be used to model the CompanyX VPN design is shown in Figure 4.2.1. This design consists of two VPN partitions, with two hub sites. Internet access will be provisioned through the Check Point Firewall only. Careful attention should be paid to the routing configuration of the hub site devices.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

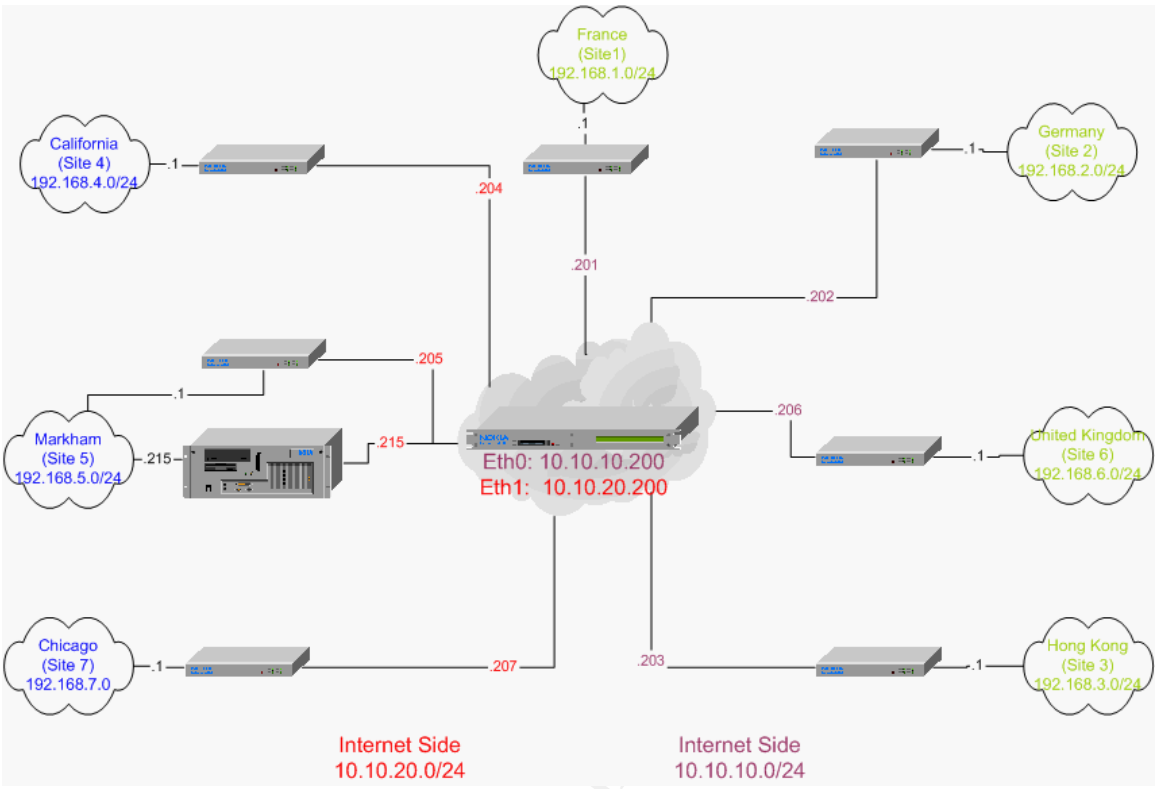


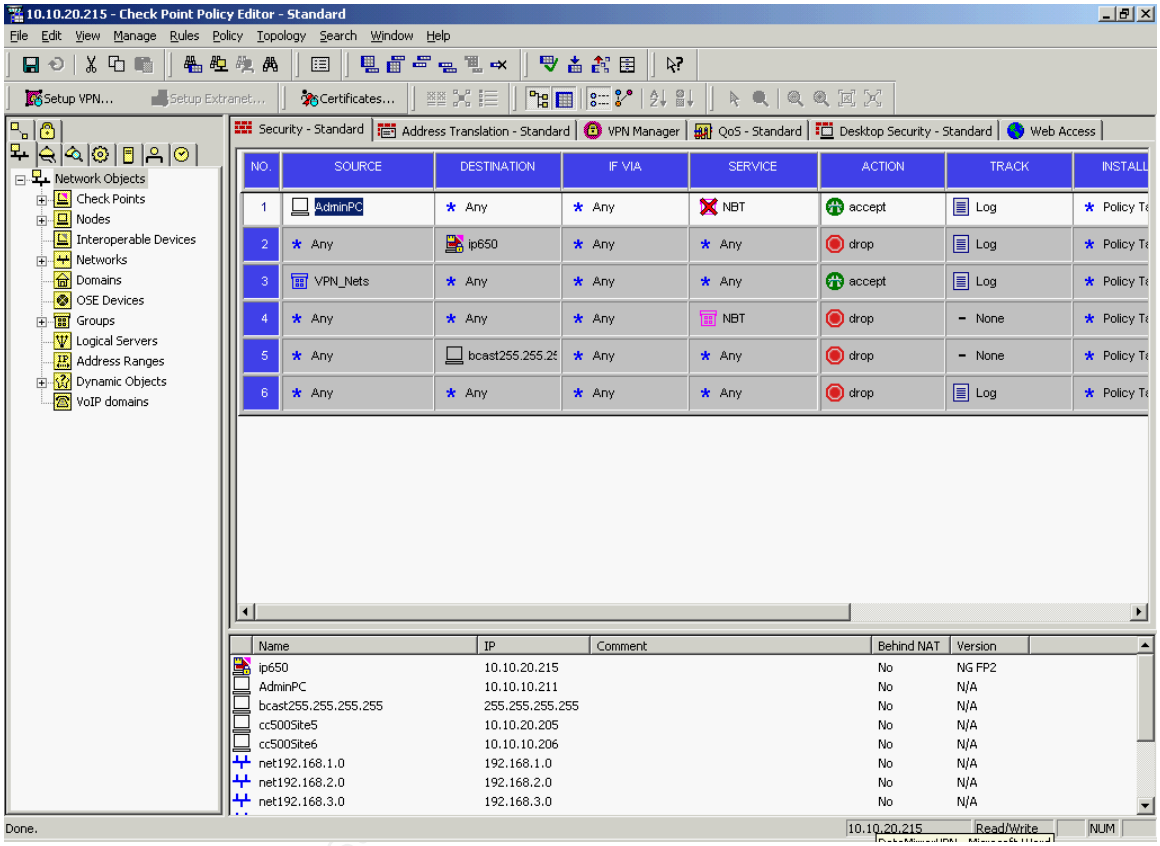
Figure 4.2.1 Proof of Concept Design

© SANS Institute 2003, Aut

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.3 Setting up the Check Point Firewall

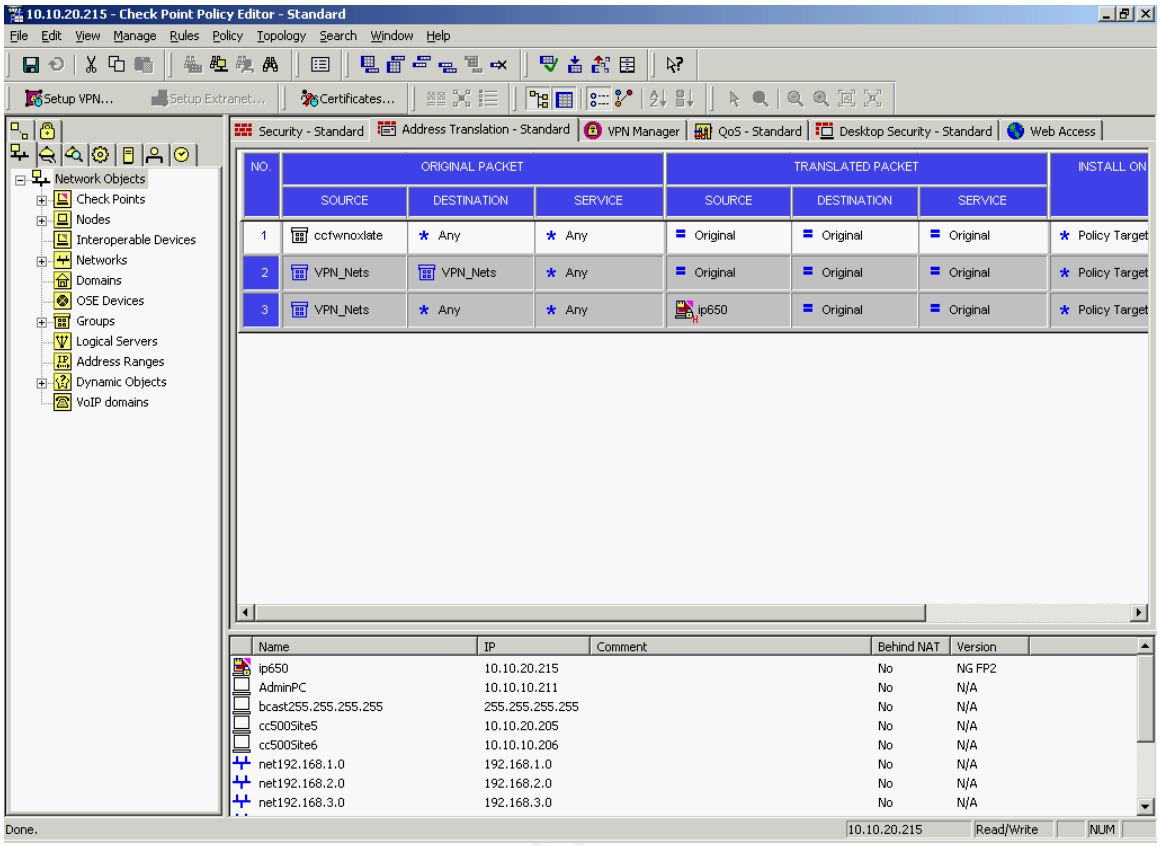
The Check Point firewall should be licensed, configured, and set up per the organization's security policy. No extraordinary parameters were set up on the Markham (Site 5) firewall, other than a few rules which permit administrative traffic to the firewall and VPN traffic to flow to and from the internal network, as well as to the Internet [1].



It should be noted that the 'VPN_Nets' group contains all of the networks contained in the CompanyX encryption domain. All of the other rules are fairly conventional [2].

Over and above security policy, standard NAT rules were configured to hide all Internet traffic behind the IP address of the firewall [1].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Also, static routes were put in place to ensure that VP traffic was routed correct from the Markham site. It is significant to note that most clients and routers use the firewall as the default route, which necessitates this step. Static routing is configured in the Nokia Network Voyager interface, and should contain the following routes in order to ensure that VPN traffic is properly routed to the Markham (Site 5) CryptoCluster, and not out the default gateway.

```
192.168.1.0/24      192.168.5.1          CU          eth-s1p3c0
192.168.2.0/24      192.168.5.1          CU          eth-s1p3c0
192.168.3.0/24      192.168.5.1          CU          eth-s1p3c0
192.168.4.0/24      192.168.5.1          CU          eth-s1p3c0
192.168.6.0/24      192.168.5.1          CU          eth-s1p3c0
192.168.7.0/24      192.168.5.1          CU          eth-s1p3c0
```

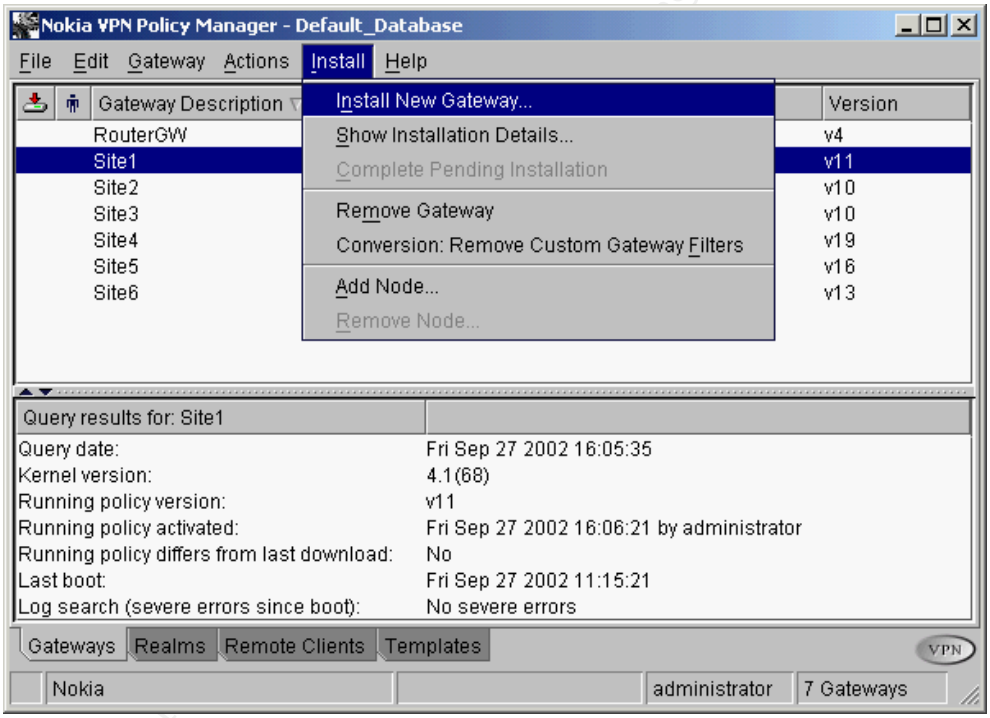
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.4 Setting up the Nokia CryptoClusters

Configuring the Nokia CryptoClusters is a simple process, which involves the use of the VPN Policy Manager. The following steps should be undertaken prior to attempting these configurations. Detailed instructions can be found in the product documentation [3]:

- Upgrade the boot manager on each device to 2.01 or later [3]
- Install Nokia VPN 4.1 (build 68) on each device
- Return the Nokia devices to factory defaults ('conf wiz')

- The first step would be to create all of the Nokia CryptoCluster Devices within the Policy Manager, and initialize the certificate authority (CA) on any device. In this case, the device for Site 1 will be used as the CA [3]:



Follow the steps in naming the device, and specify the necessary parameters:

- Choose 'Nokia CC500' or the appropriate device from the pull-down menu.
- Select 'Standalone' as the install type.

- Enter 'Site1' as the Gateway Description.
- Click 'Next'.

- Enter 192.168.1.1 as the inside address, with subnet mask 255.255.255.0.
- Enter 10.10.10.201 as the outside address, with subnet mask 255.255.255.0.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Enter a FQDN of Site1.<your company>.com.
- Set the default route to 10.10.10.200.
- Click 'Next'.

- Leave the VPN Partition set to 'Default VPN Partition' for now.

- Select 'New', next to 'Host Group Description'.
- Leave the default name 'Site1-Protected'.
- Click 'New'.

- Enter 192.168.1.0 as the IP address and 255.255.255.0 as the mask.
- Click OK twice.
- Click 'Next'.
- Leave 7 days as the expiry date unless you need more time (typically not required).
- Click 'Next'.

- You will see some pertinent identity information. Click 'Copy to Clipboard'.

- Open a HyperTerminal session on an initialized CryptoCluster.
- Press enter a few times until you get the 'Security Token' prompt.
- Paste the clipboard contents onto the terminal session. Type 'y' to accept the settings. The Nokia VPN device will enter the command prompt.
- Ensure that the Nokia device is then connected to the correct part of the lab or production network, with IP connectivity to the VPN Policy Manager.

- You are ready to connect to the device. Return to the VPN Policy Manager.

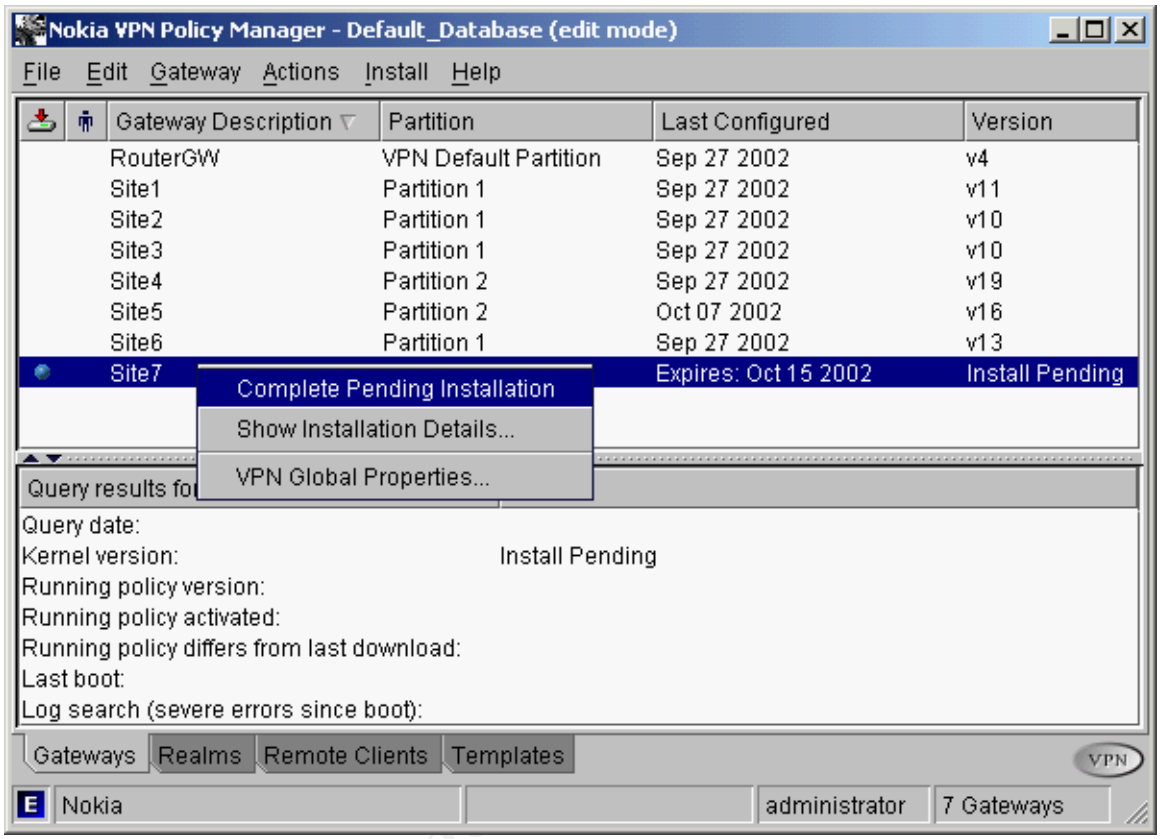
- INITIALIZE THE INTERNAL CA ONLY FOR THE SITE1 GATEWAY. For all other VPN devices, select to have a certificate assigned from the Site1 Gateway, and fill in the necessary fields.

- Configure the remaining gateways as follows:

Hostname	Internal IP (all /24)	External IP	Default Gateway	CA
Site1	192.168.1.1	10.10.10.201	10.10.10.200	Yes
Site2	192.168.2.1	10.10.10.202	10.10.10.200	No
Site3	192.168.3.1	10.10.10.203	10.10.10.200	No
Site4	192.168.4.1	10.10.20.204	10.10.20.200	No
Site5	192.168.5.1	192.168.5.215 (Firewall)	10.10.20.200	No
Site6	192.168.6.1	10.10.10.206	10.10.10.200	No
Site7	192.168.7.1	10.10.20.207	10.10.20.200	No
RouterGW	10.10.10.200	10.10.20.200	10.10.10.1	No

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

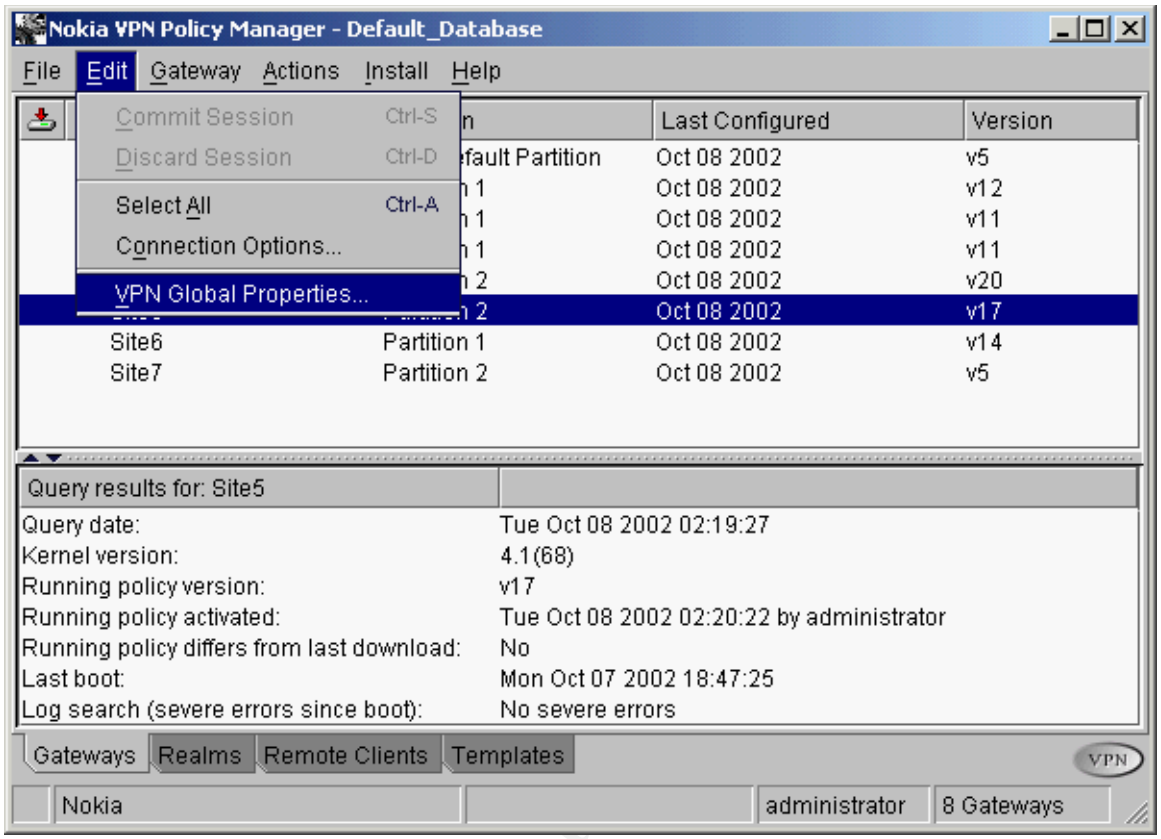
- Once you have completed this step, right click the newly created device and select 'Complete Pending Installation'. Upon successful completion, you will receive a prompt to save the device PIN – this is always recommended.



- At this point you should have all of the CryptoCluster gateways configured, and have connectivity to them from the management station.

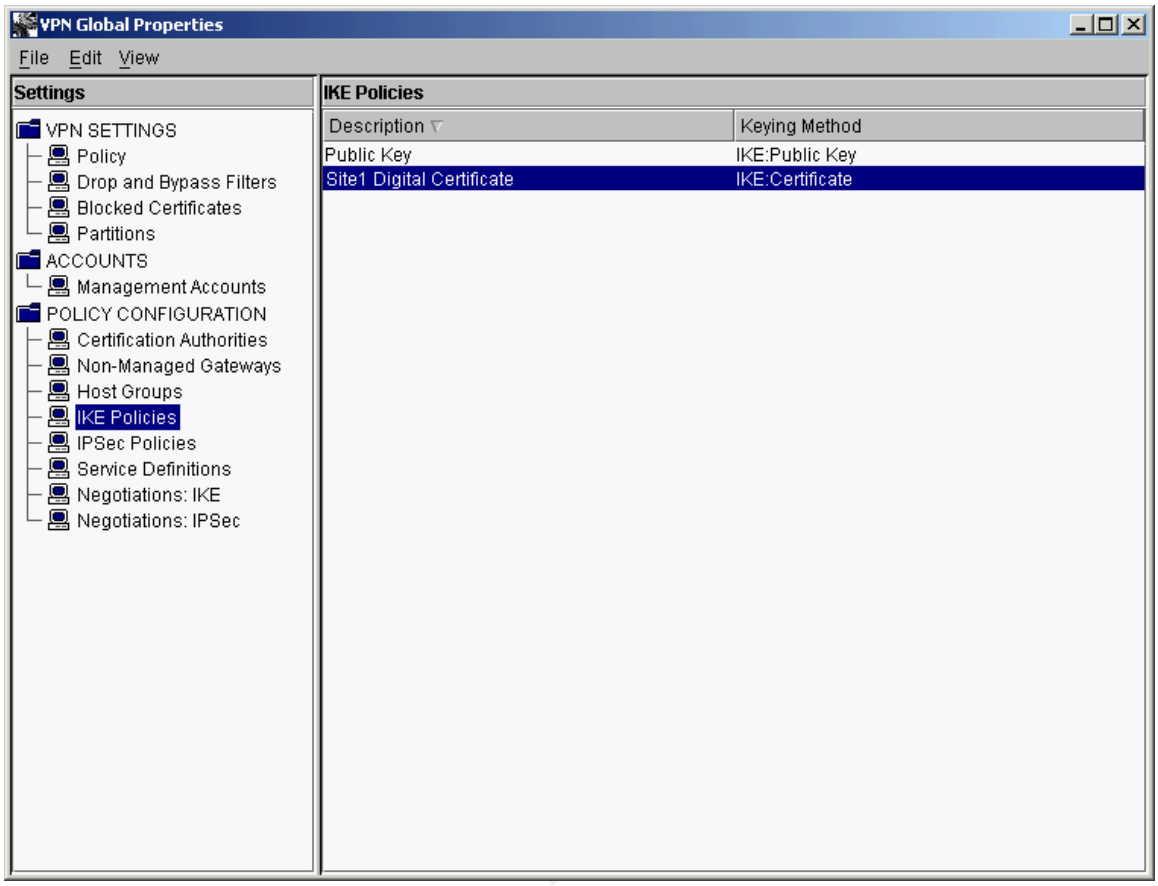
- Enter the Shared Properties Screen by selecting Edit-VPN Global Properties (or by clicking the 'VPN' medallion at the bottom right of the VPN Policy Manager Window.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



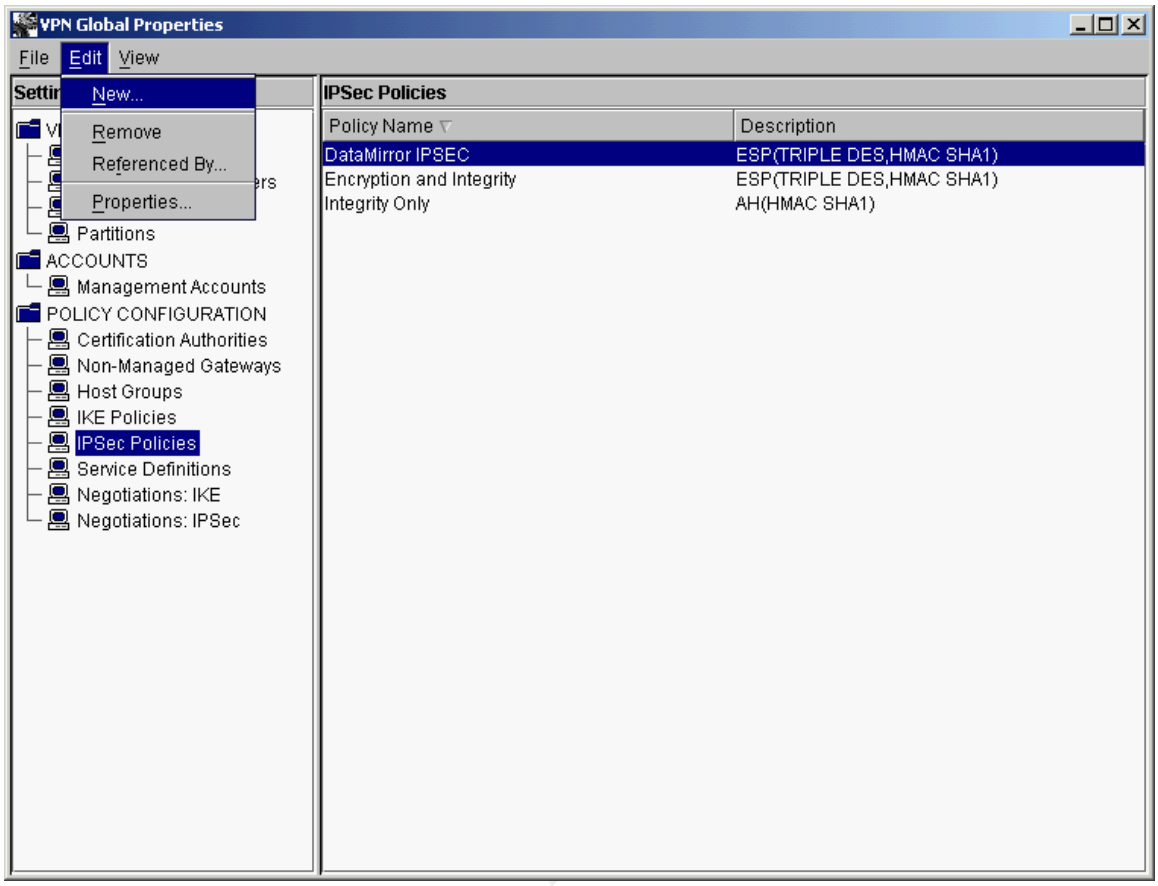
- The Global Properties Window will appear. Click the IKE Policies item. Note that a Site1 Digital Certificate Policy has been created for you. This is from when you initialized the CA on the Site1 gateway only. Double click this policy and explore the settings (Under advanced properties, you can set the Diffie-Hellman group to Group 5).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

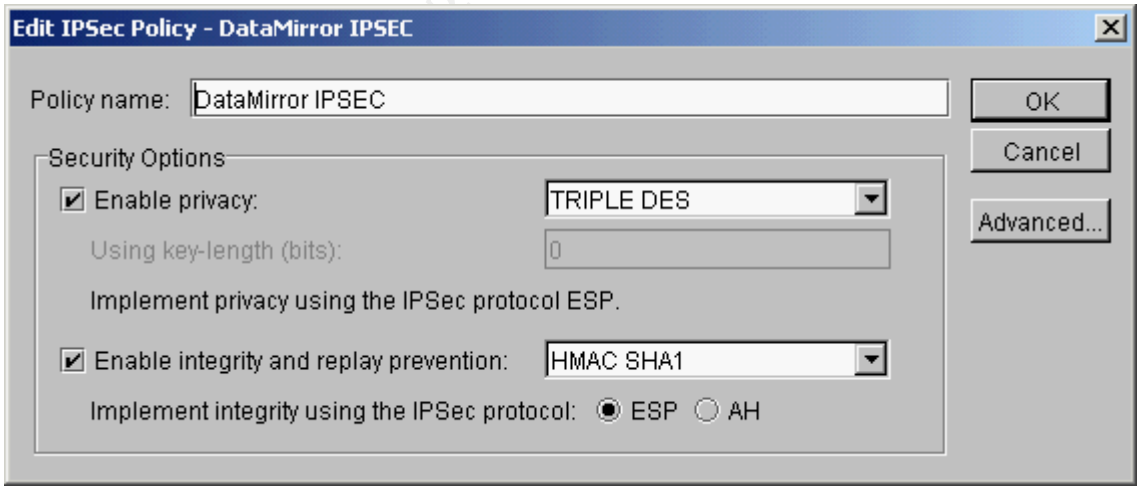


- Click the 'IPSEC Policies' item. Select Edit-New.

© SANS Institute 2003,

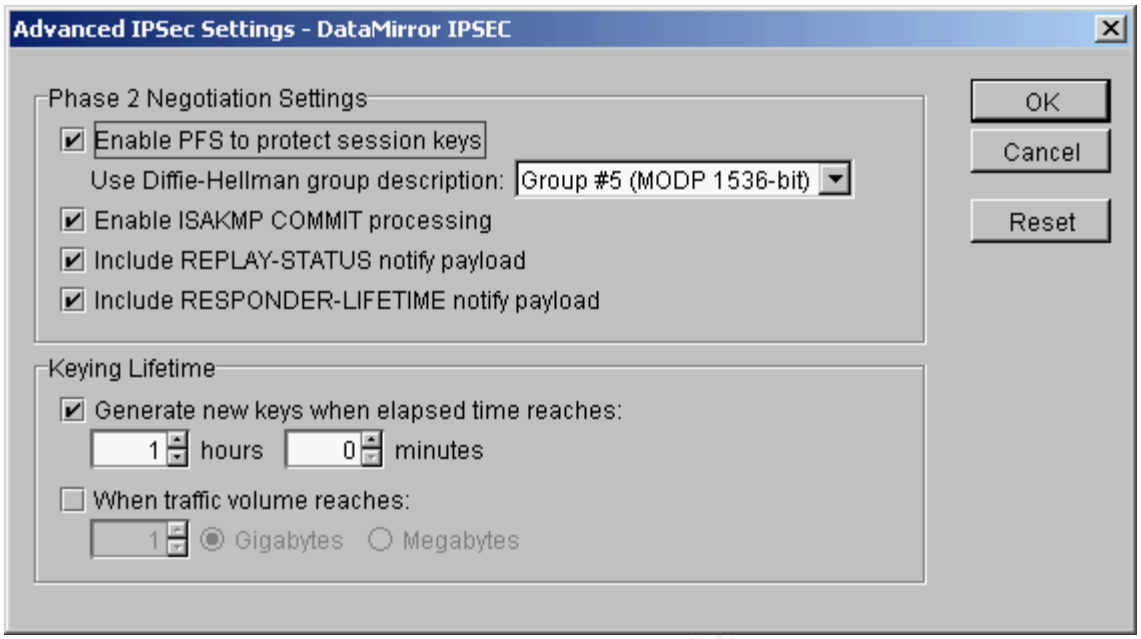


- Fill in the following parameters and then click 'Advanced'.



- Under advanced, ensure the following parameters are set, and then click OK twice.

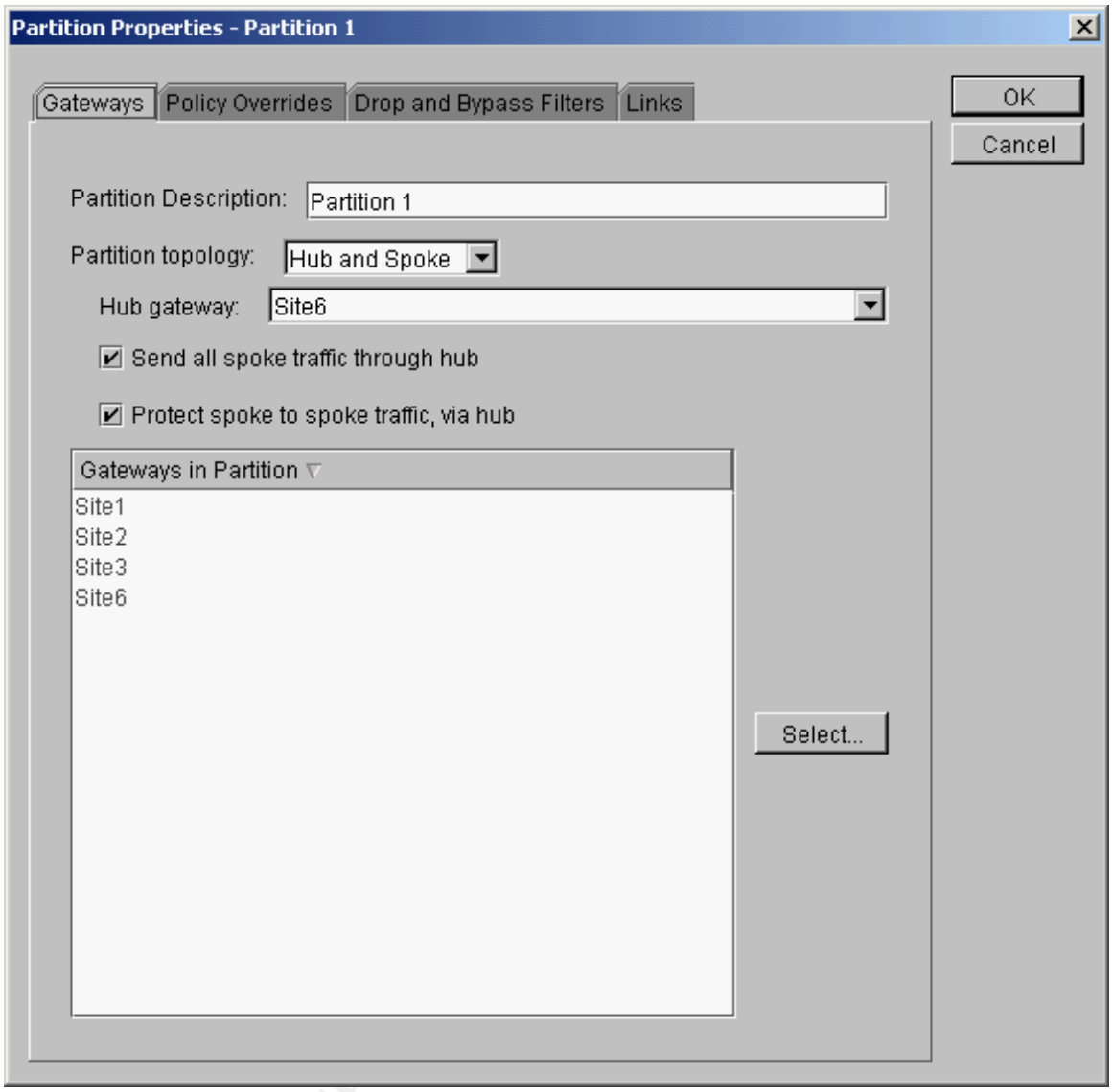
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



- You have now created an IKE and IPSec policy for your VPN. All that remains is the creation of a Partition, which is a logical grouping of VPN nodes. Select the Partitions item, and select Edit-New, and create two partitions as shown below:

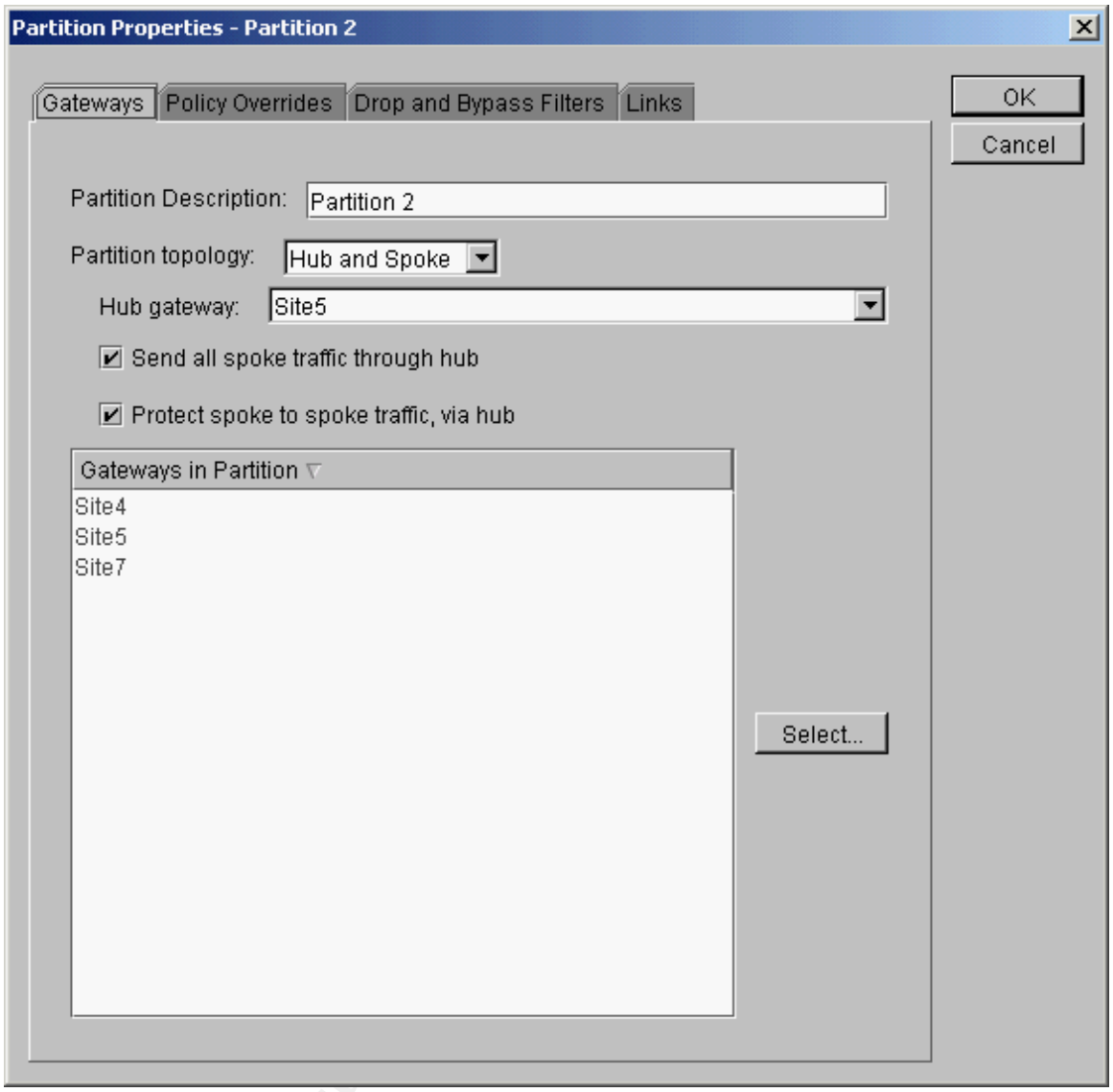
© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



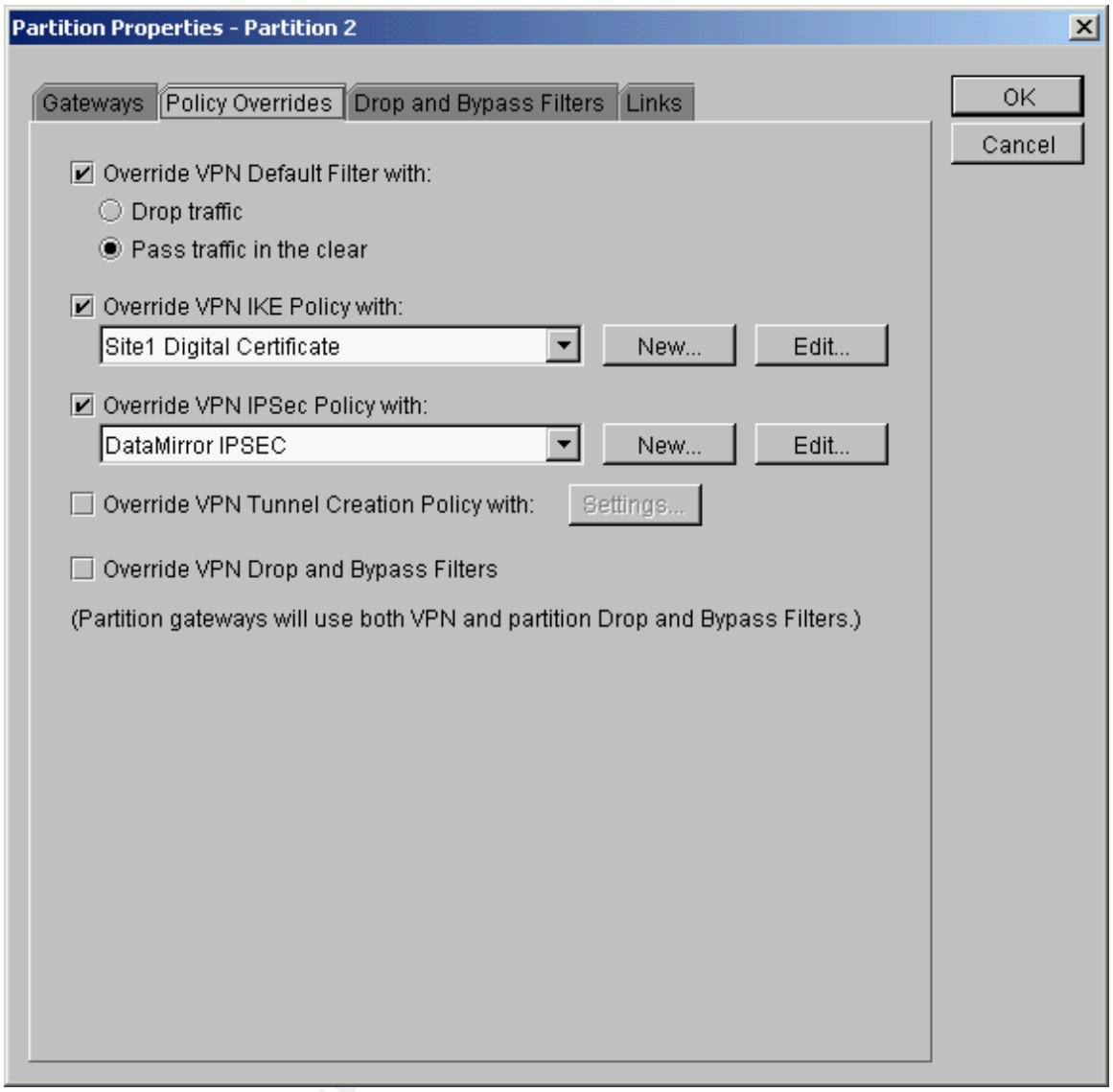
- It is very important that the hub gateway is correctly specified in all cases. Also, ensure that both check boxes are selected. This will force all traffic through the hub sites, and route spoke to spoke traffic. Create Partition 1as above and Partition 2 as follows:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



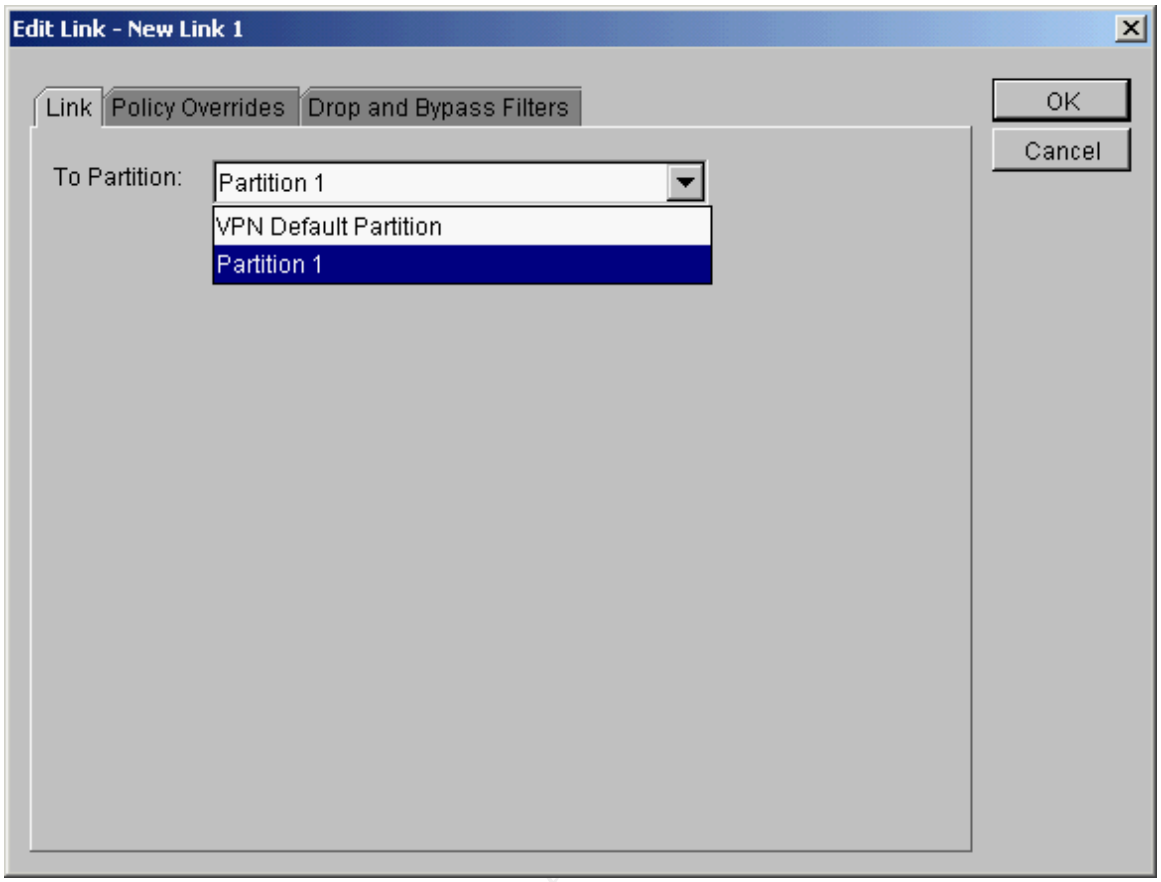
- Once you have completed the Partition definitions, click the Policy overrides tab, and ensure the devices are set to use the IKE certificate policy and IPSec Policies created earlier. Verify this for BOTH partitions.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



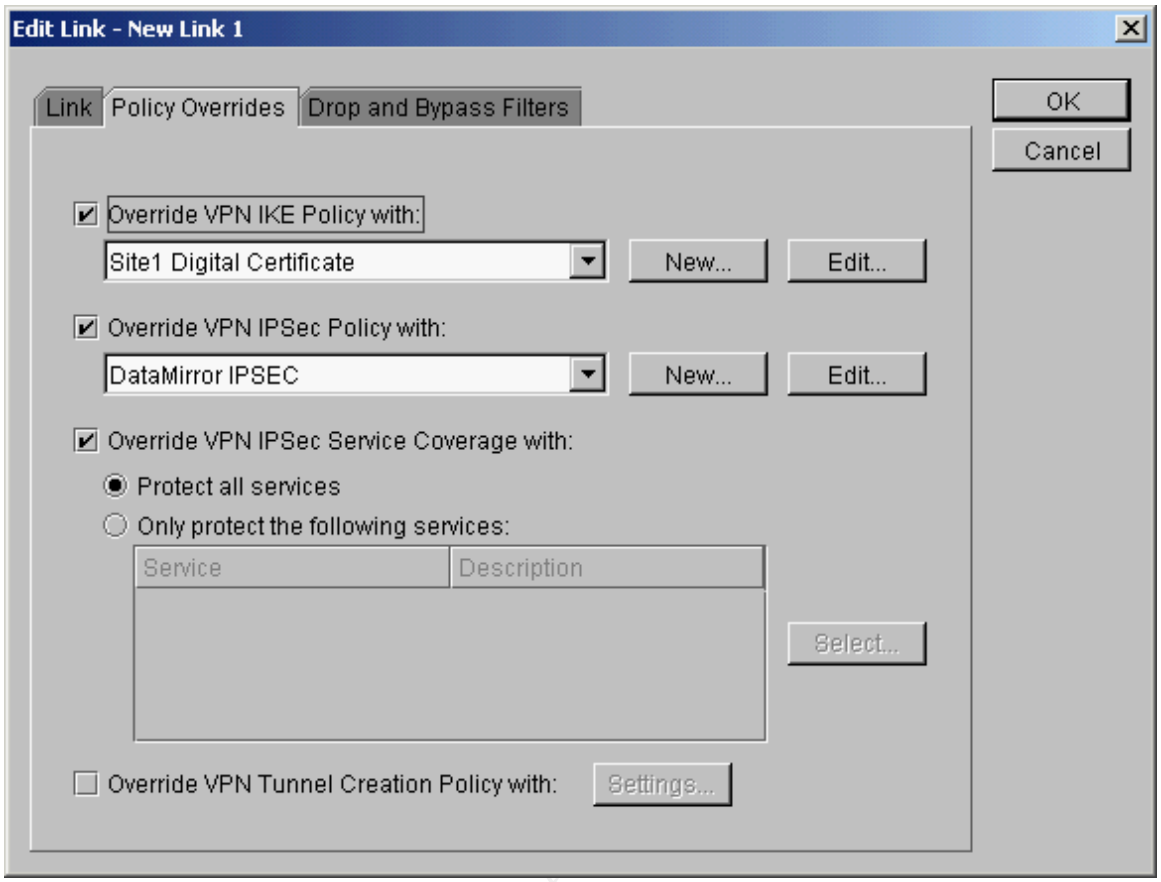
- Once this is done, all that is left to configure is the link between the two sites – select the Links tab in either partition. You only need to do this in any one of the partition definitions. Select 'New' and select the complimentary partition's name in the pull-down box. The other partition will automatically be set.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



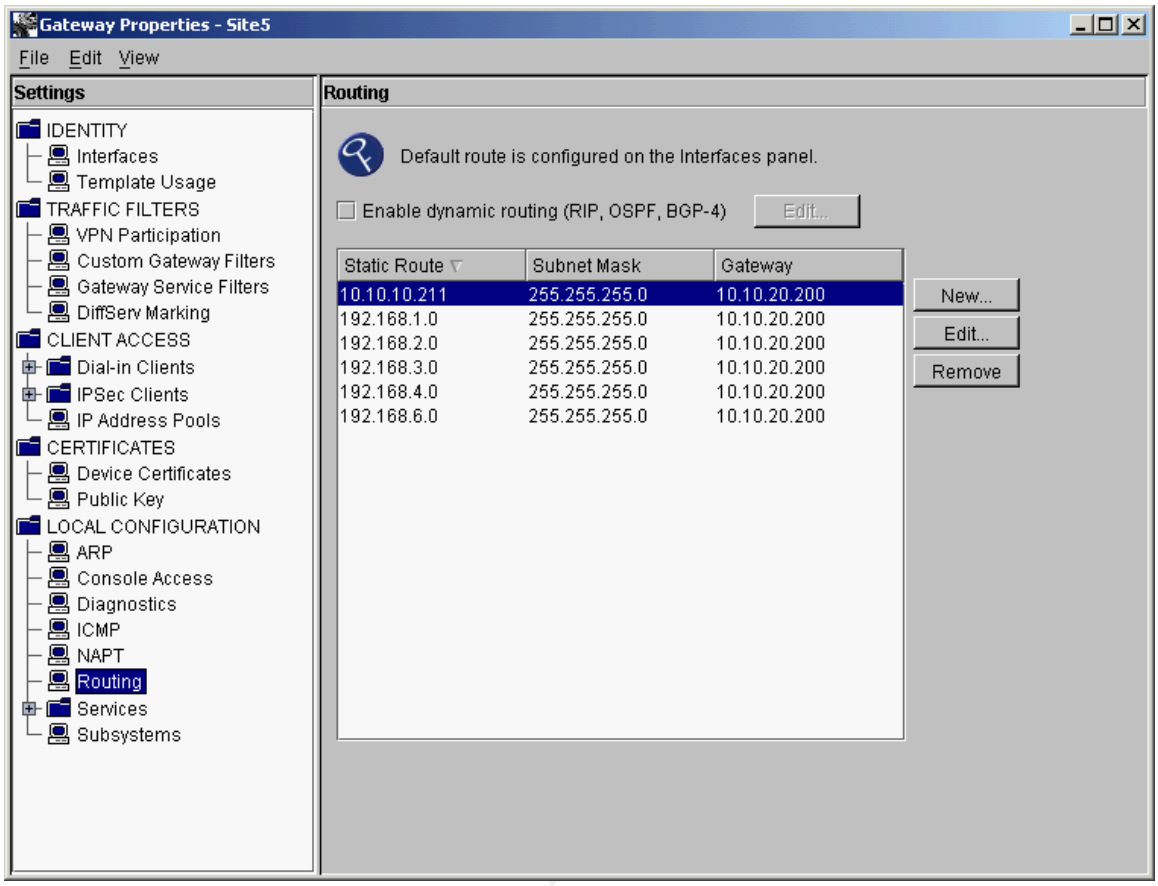
- Then select the 'Policy Override' tab. Specify the IKE and IPSec Policies as before.

© SANS Institute 2003,



- The tunnel definitions are now complete. All that needs to be done at this point is to ensure that the routing is correct at the hub site with the firewall. Close the VPN Global Properties Window, and open (double click) the Site5 device. Select the Routing item. Add static routes by selecting the 'New' button, and ensuring the routes are added as shown. These routes are to prevent asymmetrical routing of VPN traffic through the firewall. There is also another route in order to prevent asymmetrical routing to the management server, 10.10.10.211. This last route is not necessary if the manager is behind the firewall.

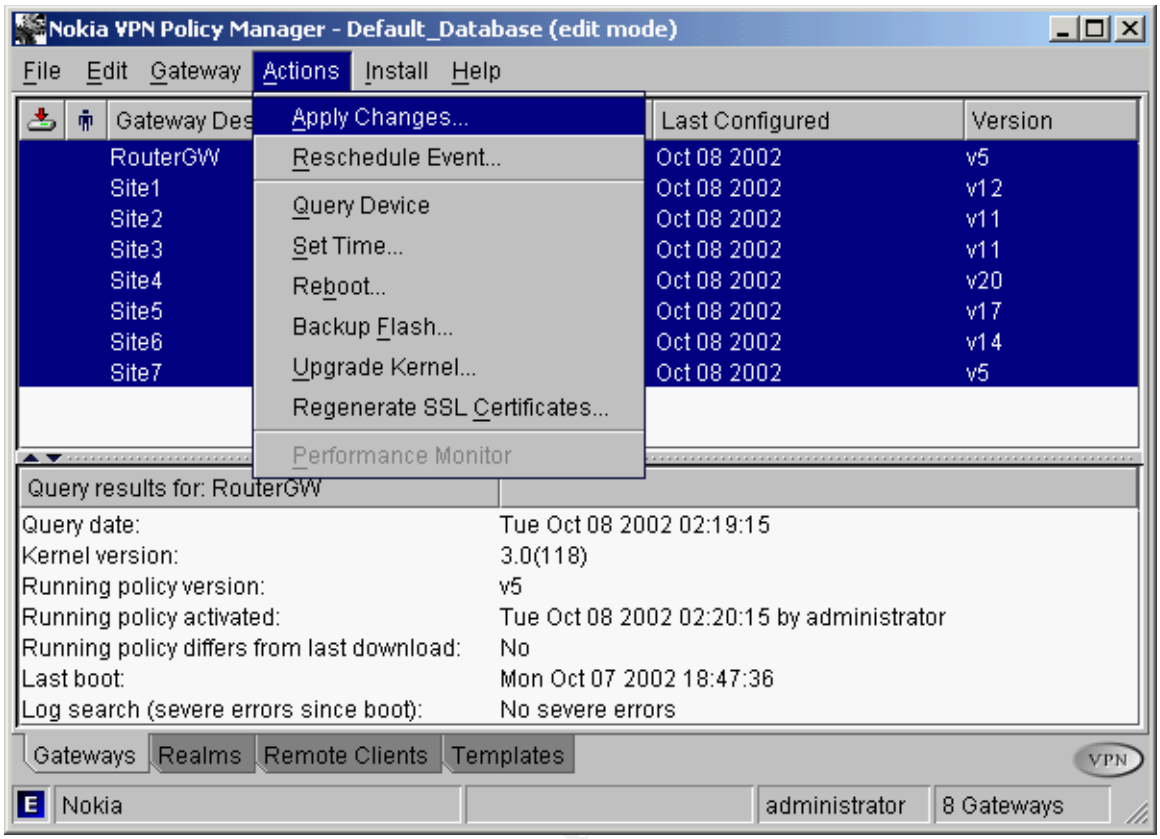
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



- Once this has been accomplished, the VPN configuration is complete. Close the device panel, and select all of the VPN devices by using the mouse in coordination with the 'Ctrl' key. Once this is done. Click Actions-Apply Changes. When prompted for a time, select immediately, and click OK.

© SANS Institute 2003,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The Nokia VPN devices are now configured for forced-tunneling hub and spoke topology.

4.6 Adding Additional Sites

Adding additional nodes can be accomplished by creating a Nokia VPN node normally, and adding it to the appropriate partition [3].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5 Discussion (Post-Implementation)

Subsequent to this implementation, CompanyX's security was enhanced in the following ways, which correlate back to the discussions in section 3:

- The VPN traffic into the hub sites is inspected, protected, logged and auditable by the firewall is each hub site, which are logging centrally to headquarters.

- Internet access is no longer passing directly through the non secure CryptoClusters. This poses a considerable security enhancement to the previous configuration, as a large amount of Internet risks can be mitigated through these measures.

- Internet access is centralized and auditable, as opposed to unmonitored.

- Spoke to hub traffic is inspected by the hub firewalls, which can be used to scope down open services and mitigate attack.

- It is now possible to centralize intrusion protection systems (a.k.a. IDS), antivirus, and content filtering services at the hub sites, further enhancing content security.

- The CryptoClusters need not be configured to pass clear traffic, or to accept any return traffic from the Internet other than ESP. This is much more secure than the initial situation, as they can now be "stealthed" accordingly [3].

The following exposures still exist:

- Spoke traffic is still effectively unregulated. This could be addressed by configuring the CryptoClusters to block or accept certain services. A central log server (SYSLOG) should also be implemented in order to collect log information from the VPN concentrators.

- Intrusion protection systems (IPS) are not in use anywhere in this design, as well as gateway antivirus and content solutions. These elements add another layer of monitoring and security to the overall design [5].

- The underlying protocols being used across the VPN are largely Microsoft networking (NetBIOS ports 137, 138, and 139) protocols. These are non-secure in a variety of ways, and the exploits of these services are numerous. This is where IPS becomes a useful endeavour, as well as the exploration of different, more secure methods of sharing files and information [6].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Vulnerabilities to current automated threats (NIMDA, SQL Slammer) is still not mitigated, although this could be addressed at the firewall. IT has not to date.

Overall, the doctrine that security is an iterative process requiring several revisions holds true in this case, since this first iteration to improving CompanyX's environment represents only a first step in the security lifecycle. Much work is left, including regular vulnerability assessments, and design reviews [6].

6 Conclusion

The forced-tunnel VPN implemented by CompanyX has resulted in an increase in security, and is therefore deemed a successful implementation. There is, however, a long way to go. Moving forward, a gap analysis will have to be performed, as well as additional vulnerability and threat assessments [5].

The methodology with which the solution was generated must also be revised. Technical feedback was the only criterion which was used to arrive at a security design. Executive-level stakeholders must be brought closer to this process, as well as sign-off on the decisions reached by the committee.

Overall, the security of the enterprise has been refined, but the processes supporting it still have a long way to go. Suggested actions to be taken are as follows:

- Form a security team with members from not only the network team, but management and human resources *et al*. This will help support a multi-dimensional approach to corporate security [6].

- Institute formal reviews of personnel, their roles, and their responsibilities. Ensure accurate job descriptions are available, and that access controls based on these roles are in place and enforceable [6].

From these key actions, a new security lifecycle will emerge, and contribute to the helath and welfare of the organization and its assets.

© SANS Institute 2003, Author retains full rights.

REFERENCES

[1] Jeff Mousseau, "Nokia VRRPmc / Check Point NG FP2 High Availability Configuration Document", 2002
URL: http://www.digitalmigrations.com/vrrp_ha_fp2_v1.8.pdf

[2] Dameon D Welch-Abernathy, Essential Check Point FireWall-1, Addison-Wesley, 2002

[3] "Nokia VPN Configuration Guide v4.0", 2001
URL: https://support.nokia.com/vpnproducts_docs/4.1/nokia-vpn-gateway-config-guide.pdf

[4] Naganand Doraswamy and Dan Harkins, IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Prentice-Hall PTR Inc., 1999.

[5] Ronald L. Krutz and Russell Dean Vines, The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, Wiley, John and Sons Inc., 2001

[6] Micki Krause and Harold F. Tipton, Handbook of Information Security Management, CRC Press LLC,
URL: http://www.cccure.org/Documents/HISM/ewtoc.html

ONLINE RESOURCES

Check Point FireWall-1 Resources:

- www.checkpoint.com/techsupport/index.html
- www.phoneboy.com

Nokia Firewall/VPN Resources:

- www.nokia.com
- support.nokia.com
- www.digitalmigrations.com

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.