2004-09

An analysis of VPN solutions and best practices for use in conjunction with cyber attack and defend exercises

Sherman, Michael A.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF VPN SOLUTIONS AND BEST PRACTICES FOR USE IN CONJUNCTION WITH CYBER ATTACK AND DEFEND EXERCISES

by

Michael A. Sherman

September 2004

Thesis Co-Advisors: Cynthia E. Irvine
J. D. Fulp

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Analysis of VPN Solutions and Best Practices for Use in Conjunction with Cyber Attack and Defend Exercises			**5. FUNDING NUMBERS**
6. AUTHOR(S) Sherman, Michael A.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

An effective method of practicing cyber attack and defend techniques is through cyber-exercises, coordinated over the Internet. The Virtual Private Network (VPN) is an effective way to link cyber attack and defend teams, providing for the encryption of exercise traffic that transits the public network infrastructure. However, VPNs and the technologies and devices behind them are not yet widely understood. Research and evaluation of VPN solutions will identify those most conducive to supporting a cyber-exercise. Users demand a solution that is secure, reliable, and easy to employ. The research in this thesis applies directly to the selection and implementation of an optimal VPN solution to support cyber-exercises.

14. SUBJECT TERMS Virtual Private Network, Cyber-Exercise, IPSec, Encrypted Tunnels			**15. NUMBER OF PAGES** 186
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN ANALYSIS OF VPN SOLUTIONS AND BEST PRACTICES FOR USE IN CONJUNCTION WITH CYBER ATTACK AND DEFEND EXERCISES

Michael A. Sherman
Major, United States Marine Corps
B.S., United States Naval Academy, 1990
M.S., Boston University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Michael A. Sherman

Approved by: Cynthia E. Irvine
Thesis Co-Advisor

J. D. Fulp
Thesis Co-Advisor

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

An effective method of practicing cyber attack and defend techniques is through cyber-exercises, coordinated over the Internet. The Virtual Private Network (VPN) is an effective way to link cyber attack and defend teams, providing for the encryption of exercise traffic that transits the public network infrastructure. However, VPNs and the technologies and devices behind them are not yet widely understood. Research and evaluation of VPN solutions will identify those most conducive to supporting a cyber-exercise. Users demand a solution that is secure, reliable, and easy to employ. The research in this thesis applies directly to the selection and implementation of an optimal VPN solution to support cyber-exercises.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AES	Advanced Encryption Standard
AH	Authentication Header
AIM	Advanced Integration Module
BNP	Bastion Network Project
CA	Certificate Authority
CISR	Center for Information Systems Security Studies and Research
CLI	Command Line Interface
CRL	Certificate Revocation List
CRMO	Cyber Risk Management Organization
DES	Digital Encryption Standard
DH	Diffie-Helman
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol
L2TP	Layer 2 Transfer Protocol
MD5	Message Digest Five
MSCA	Microsoft Certificate Authority
NAT	Network Address Translation
NCMS	Netscape Certificate Management System
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
PFS	Perfect Forward Secrecy
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PSTN	Packet Switched Telephone Network
RIP	Routing Information Protocol
SA	Security Association
SAD	Security Association Database
SCEP	Simple Certificate Enrollment Protocol
SDM	Security Device Manager
SHA	Secure Hash Algorithm
SPD	Security Policy Database
SPI	Security Parameter Index
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
VPN	Virtual Private Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

I would first like to thank God for all He has done for me and all those close to me. Second, I would like to thank my wife for her support throughout my thesis and my time at the Naval Postgraduate School. Third, my parents for the grounding, education, and guidance they gave and continue to give me. Fourth, I would like to extend a special thanks to my thesis co-advisors, Dr. Cynthia E. Irvine and Mr. J. D. Fulp for their assistance, guidance, time spent mentoring me, and helping me bring this thesis to successful completion.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CYBER-EXERCISES

The more computers are integrated into all aspects of daily life, the more likely citizens are to be victims of cyber-crime. In order to combat cyber-crime, computer scientists are continuing to learn how to defend against attacks and attackers. For several years, the Black Hat organization, as part of its annual DEFCON convention in Las Vegas, began holding an annual Capture the Flag (CTF) cyber-exercise. This exercise serves as a test bed for computer attack and defense techniques. [DEF01]

In addition to cyber-crime affecting the private citizen, cyber-attacks are also a real and present threat against the United States government, more specifically against the Department of Defense. In recent years, there has been a marked increase in attacks against DoD computers [LEW01] and direct threats against the United States by terrorist groups such as Al Qaeda. [VER02]

Many governmental personnel charged with the defense of DoD computer systems practice, perfect, and validate their cyber-defense techniques against other teams at the DEFCON CTF competition. The DEFCON CTF, although an excellent exercise, is held on site at Las Vegas. All participants must travel there to participate. The information assurance community could benefit from more frequent training in cyber attack and defense training. This is especially true in academic circles. In order to comply with the geographic and temporal demands of academic institutions, cyber-exercises are moving toward being conducted over long distances. Each team operates from is own location, connected through the Internet.

Conducting cyber-exercises over long distances presents several challenges. On one hand, the academic network of each participant contributing to the exercise needs to be protected from outside attack. Though protecting any network is always a smart thing to do, having a cyber-exercise network vulnerable, or even able to be observed, by outside hackers adds an unwanted, uncontrolled dimension to the otherwise controlled exercise. On the other hand, as genuine computer attacks are

being launched within the cyber-exercise, the public Internet at large must be protected from the techniques and technicians participating in the cyber-exercise. Therefore cyber-exercises require dual protection, protecting the public from the cyber-exercise, and protecting the cyber-exercise players from the public. Two techniques that can help are encrypted tunneling and internet protocol security (IPSec). Each will be introduced here and discussed in detail in subsequent chapters.

B. ENCRYPTED TUNNELING

There are several possible solutions to the dual protection that is required when conducting a cyber-exercise. Firewalls and password schemes might figure into protecting the integrity of the cyber-exercise, but the most complete way to isolate a cyber-exercise from the rest of the public Internet is through virtual private network (VPN) technology. [MER99] If properly constructed, a VPN can allow the cyber-exercise to proceed unobserved and unmolested by non-participants, and can also protect the integrity and restrict participation in the cyber-exercise to only the invited participants.

There are several possible ways to implement a VPN within the seven layer Open Systems Interconnection (OSI) network model. Current commonly accepted ways of VPN implementation are at the link layer (layer 2), at the network layer (layer 3), or in the upper layers (layer 5, six and seven). [MAI02] The higher layer VPN, commonly called an "application layer" or "layer 5" VPN, takes into account that the application layer is layer 5 in the Department of Defense (DOD) network model. [FOR01]

C. INTERNET PROTOCOL SECURITY (IPSEC) IMPLEMENTATION DECISIONS

Internet Protocol Security (IPSec) and how it works is at the very heart of understanding how a VPN operates. IPSec is examined in great detail in this thesis. IPSec was designed to provide secure, reliable data transfer through the standardized use of many pre-existing protocols. [THA98] Besides choosing the best layer in which to implement the VPN, there are many other decisions relating to IPSec that must be consciously made for a VPN to be effective. The proper key exchange method, security protocol, VPN mode, and gateway device must be chosen.

1. Key Exchanges

The internet key exchange (IKE) protocol provides the method for creation of a secure tunnel between two VPN peers. The creation of this tunnel is a complex process involving up to four internet protocols that are captured by the IKE parent protocol. [MAI02]

The building of the secure tunnel for a VPN takes place in two phases, titled IKE phase I and IKE phase II. During IKE phase I, an authenticated secure channel between the VPN peers is constructed. During phase II, the IPSec parameters are negotiated to allow the secure transfer of data.

It is perhaps worth reminding the reader that this VPN tunnel is not an actual (physical) "tunnel" but rather a virtual tunnel. The contents of the traffic, due to the proper employment of encryption, cannot be observed or surreptitiously modified. Thus the traffic is considered "tunneled", or hidden/protected.

2. Security Protocol

There are two choices of security protocol when using IPSec, authentication header (AH) and encapsulating security payload (ESP). The AH protocol is designed to provide integrity, authentication, and replay protection for the processed datagram. ESP provides all these features also, and through the use of encryption, offers confidentiality as well. [MAI02]

3. Security Mode

IPSec can be run in one of two modes, either transport mode or tunnel mode. Transport mode can only be used when the VPN gateway device is also the VPN client device; i.e. the *user* of the VPN tunnel is also the *provider* of the VPN tunnel. Tunnel mode allows the VPN gateway device to be placed in front of a network of computers. All computers on this network can then utilize the VPN tunnel, provided by the gateway device operating in tunnel mode.

4. Gateway Device

The final decision to be made regarding implementing a cyber-exercise VPN is exactly what physical devices will best perform the technical processes delineated above. There are three generalized choices. VPNs can be constructed with a general-

purpose computer running VPN software. VPNs can be constructed using a VPN-capable router. Finally, VPNs can be constructed using a dedicated VPN device, often called a VPN concentrator or VPN appliance.

D. FOCSU AND DIRECTION OF THIS RESEARCH

The focus of this thesis is VPN creation. This thesis will first provide the reader with a thorough examination of the underlying theory and structure of a VPN. Then using the theory learned, commercially available hardware will be used to construct actual working VPNs that ultimately link networks and cyber-exercises. Knowledge gained through detailed examination and implementation of VPNs will benefit the DoD by increasing knowledge about the requirements and structure of VPN technology, as well as the benefits derived from participation in the cyber-exercises that result from the linking of two networks via VPN.

The remainder of this thesis is organized as follows:

Chapter II. "Virtual Private Networks Explained" will look at cryptography, endpoint authentication, and the interaction of a VPN with the network layers.

Chapter III. "IPSec Virtual Private Network Management" will examine in detail the workings of IPSec, digital certificates and the concept of split tunneling.

Chapter IV. "Cyber-Exercise Needs" will discuss the unique concerns of a cyber-exercise VPN in relation to the detailed topics examined in the previous chapters.

Chapter V. "Three VPN Alternatives" wll examine, step by step, the building a VPN on commercially available hardware, relating the theoretical to the practical.

Chapter VI. "Summary and Conclusions" ties all points together and recommends an optimum VPN solution for a cyber-exercise.

To begin this process, the basic components of a VPN must be understood. A logical place to begin is with an examination of cryptography, endpoint authentication, and the interaction of a VPN with the network layers. Chapter II examines each topic in detail.

II. VIRTUAL PRIVATE NETWORKS (VPNS) EXPLAINED

In understanding how a virtual private network (VPN) is constructed, several items must be examined. The role of cryptography, VPN endpoint authentication, and VPN interaction with the network structure must receive a careful look. In this chapter, these essential topics will be examined in detail.

A. CRYPTOGRAPHY: THE KEY TO PRIVACY

The technique that makes a virtual private network "private" is the use of cryptography. Cryptography, when combined with robust protocols, attempts to provide any or all of the three information security attributes: confidentiality, integrity, and authenticity. In VPNs, confidentiality is concerned with ensuring that transmitted information is not able to be viewed by non-participants. Integrity is concerned with the transmitted data being altered while enroute. Authenticity is concerned with assuring the receiving party that the sender is indeed who they say they are. VPNs make use of cryptography to address each of these concerns. [FUL04]

1. Hashing for Integrity and Authenticity

Hashing is a component of cryptography that, when properly employed, is able to assure the receiver of a message that the message has not been altered. In other words, hashing is a method to support data integrity. Through the addition of a key, or any such form of a "shared secret", hashing can also be used to ensure authenticity. A one-way transform is an accurate description of how a hash algorithm functions. It is important to point out that "hashing" is the one-way process of converting a message into a "hash". A hash is the resulting fixed length string of symbols. The hash is also known as a message digest or a one-way transform. Each type of hash function is based on a mathematical algorithm.

No matter which hash algorithm is used, the hash algorithm is designed to provide integrity. It does this by applying the hash algorithm to the message. Any message, no matter how large or small, can be reduced in size to, in the case of well known hash functions, 128, 160, 172 or 256 bit string of symbols, or hash. In the VPN

arena, there are two often used hash algorithms, the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA).

The MD5 hash algorithm was designed by Professor Rivest of the Massachusetts Institute of Technology (MIT) in 1991. It generates a 128 bit hash value. Theoretically, all hash algorithms can be defeated. Ideally; however, hash algorithms are created to be robust enough so that their defeat is, in a practical sense, not feasible. Unfortunately in 1994, only three years after its introduction, laboratory experiments were successful in defeating MD5 by causing a "collision". [ENC01] Researchers, given a particular target hash, were able to generate two messages that produced that hash. The occurrence of a collision was a blow to MD5. Though MD5 was defeated in the laboratory, MD5 is not considered broken and is still widely used in real world applications, including the Cisco devices used in this thesis.

The SHA was designed by the National Security Agency (NSA), and was first published by the National Institute of Standards and Technology (NIST) in 1993 and was called the Secure Hash Standard. Due to a security flaw, it was quickly withdrawn and republished in 1994 as the present SHA-1. The SHA-1 is very secure. It takes the original message and produces a 160-bit hash. As recently as 2000, NIST published three new SHA algorithms that are designed to work with the advanced encryption standard (AES). [WIK01]

In examining the future security of hash algorithms, in August 2004 Dr Xiaoyun Wang demonstrated that she could create collisions using MD5 starting with any initial hash value. [WAN04] Dr Wang also had successful attacks against other hash algorithms, including MD4, Hashing Algorithm with Variable Length of Output - 128 (HAVAL-128), and Rate Adaptive Compression with Error (RACE) Integrity Primitives Evaluation Message Digest (RIPEMD). Currently SHA-1 remains secure, however this recent defeat of the other hash algorithms foreshadows that SHA-1 is one day likely to be defeated as well. [MIL04]

a. Hashing Keys or Data Alone

Sending the key, or shared secret (i.e. the authentication material), and the data to the peer that makes up the other end of the VPN is the cornerstone of

establishing authenticity and ultimately ensuring data integrity. As a user attempts to implement data integrity and authenticity through the use of a hash function, the dependent security relationship between the data and the key must be understood. The key must be agreed upon prior to (i.e., "pre-shared") the establishment of the VPN by users at both ends of the VPN. Sending the data together with the hashed key does not guarantee integrity nor authenticity, since an attacker could easily replay the authenticating hash with different data. The flaw in this protocol arises from the fact that the data being authenticated is in no way inextricably "combined" with authenticating key. Thus hashing keys separately from the data they are intended to protect fails to provide authenticity or integrity protection against malicious data modification. The simple solution to the above is to hash both the key and the data together prior to transmission.

b. Hashing Keys and Data Combined

A better way to provide both integrity and authenticity through the use of the hash function is to apply the hash function to both the data and the key together as one entity. [FUL04] For example, Alice and Bob want to establish secure communication between them. Alice and Bob agree on a shared secret, i.e. key or password, to use for their communication. Alice has data she wishes to send to Bob. Unlike the scenario above where Alice applies the hash function to the keys and data separately, Alice instead combines the data and secret, and then applies the hash function. Alice then sends the data and the hash of the combined data/secret to Bob. When Bob receives the transmission, he retrieves his copy of the stored shared secret, combines it with the data in the previously agreed upon way, and then applies the same hash function (just as Alice did before sending). Bob then compares the resulting hash to the hash that Alice sent. If they are the same, Bob knows that the data did not change and that the data came from Alice. Thus the hash function applied in this manner provides both integrity and authenticity.

c. Addition of Nonce (or Cookie)

Another challenge is defeating the replay attack. On a communications channel, a potential attacker could be watching the aforementioned exchange between Alice and Bob and could capture data that was sent. The attacker could later replay

both the hash and data to Bob. Since the hash contained the shared secret, Bob would think that this latest transmission came from Alice. In reality it came from the attacker. To prevent this, Alice can introduce a nonce into the process. A nonce is a meaningless random value with certain properties. Similar to the scenario above, every time Alice sends a message to Bob, Alice combines the message, the shared secret, and a new nonce value. She then applies the hash algorithm and sends the hash as well as the data in a message to Bob.

Bob receives the message, which consists of the hash and the data, and verifies that the nonce value has not been previously received from Alice. If this is the case, the message is valid and is processed. However, if the nonce has already been received, then Bob infers that this is a replay attack and discards the message.

2. Encrypting to Provide Confidentiality

So far, hashing functions have enabled VPN integrity and authenticity. VPN confidentiality is provided through the use of encryption. Encryption is used during, IKE phases one and two, and during the actual operation of the VPN. During the actual operation of the VPN, exercise data being exchanged is encrypted.

a. IKE SA: Phase I and Phase II

During Internet Key Exchange (IKE) phase I, encryption is used to protect the identification information of the peers. During IKE phase II, encryption is used to protect the key material payloads being exchanged between the peers. [DAV01] In both cases, an encryption algorithm must be chosen for the IKE Security Association (IKE SA) encryption. Use of these encryption algorithms ensures confidentiality. The information cannot be viewed except by the VPN participants that need to view them.

Commonly used encryption algorithms are the data encryption standard (DES), the triple-DES (3DES), and the advanced encryption standard (AES). DES was developed by the National Security Agency (NSA) and International Business Machines (IBM) during the 1970s. It was adopted by the government as an official standard. DES encryption, using a 56-bit key, is commonly accepted to be strong enough against a non-determined attacker. As computers have become faster and

cheaper and thus computing power more accessible for brute force attacks, DES is no longer considered strong enough for sensitive information. [BLA96] NIST has proposed withdrawing DES from government use, although DES will still be used as a component of 3DES. [JAC04]

Instead of investing resources in a new encryption algorithm, 3DES leverages the existing mechanics of the DES algorithm by running it three consecutive times with two different keys. This results in an increase in security. 3DES has an effective key length of 168-bits. Brute force attacks against 3DES are currently considered infeasible. The disadvantage of 3DES is that more computing power is required to encrypt and decrypt data. If a VPN has a heavy traffic load, 3DES may not be able to provide an acceptable level of service.

In a search for not only a secure but also a more efficient (i.e., less CPU and memory intensive) encryption algorithm, NIST wanted to develop a new, more efficient algorithm, the advanced encryption standard (AES). The algorithm selected was based on the Rijndael (pronounced rain-doll) algorithm. This algorithm was announced as the new AES in October 2000. [SMI01] Using 128, 192 or 256-bit keys, AES is to be an eventual replacement for DES and 3DES. AES was designed to run faster than DES and 3DES and use fewer resources [DUN96, HAR00] while providing more security than 3DES. [BEY02, LEN99] The setup of the VPN tunnel is explained in greater detail in Chapter III. The actual entry of the key into the VPN is graphically depicted in Chapter V.

b. IPSec SA

Once the VPN tunnel for data exchange is in place, the exercise traffic to be sent in the tunnel needs to be encrypted. Selecting from the same pool of encryption algorithms above, the exercise data is encrypted. It is not necessary to choose the same algorithm for the internet protocol security (IPSec) security association (SA) as was chosen for the internet key exchange (IKE) SA; however, the same concerns for security vs. efficiency apply. Since the exercise data is encrypted, it cannot be read by an attacker since the attacker does not possess the required key.

B. AUTHENTICATION OF END POINTS

Both of the VPN endpoints must be authenticated so that the VPN users are confident that the VPN peer at the other end of the tunnel is the intended source and destination of the information. There are generally two distinct ways to achieve this form of remote authentication. One method involves mutual revelation of a shared secret (without revealing it to an eavesdropper), and the other involves the proof of possession of certificate signed by a trusted intermediary (i.e., a Certificate Authority, or CA).

1. Pre-Shared Secret

The simplest way to verify the identity of the peer is to see if the peer possesses the same shared secret as the VPN initiator. One way to accomplish this is for the user to pick up the telephone and exchange a shared secret. This provides, in effect, a password. The other user enters this same password into the VPN peer's configuration. Possession of this pre-shared "symmetric" secret on both ends of the VPN tunnel allows the two VPN endpoints to authenticate each other and ultimately communicate.

2. PKI Certificates

A more intricate way to verify the identity of the peer is through the use of public key infrastructure (PKI) certificates. Currently, PKI is not widely implemented. Eventually; however, it will be easier for a VPN peer at one endpoint to authenticate the other VPN peer via the peer's PKI certificate than it will be to establish a pre-shared secret, as previously described.

C. LINK, APPLICATION, OR NETWORK LAYER

A VPN is built within the Open Systems Interconnection (OSI) 7-Layer network model. There are three generally accepted locations within the OSI seven layer model to implement a VPN. It is possible to implement a secure sockets layer (SSL) VPN between the session layer and transport layer, resulting in a layer 5 VPN. It is possible to implement an internet protocol security (IPSec) VPN between the network layer and data link layer, resulting in a layer 3 VPN. Finally, using either the layer 2 tunneling protocol (L2TP) or the point to point tunneling protocol (PPTP), a VPN can be built between the data link layer and the physical layer, resulting in a

layer 2 VPN. All three of these potential VPN implementation locations share common features.

Normal network traffic, as it passes down and up the OSI network stack, undergoes a process of encapsulation and de-capsulation respectively. Upon generation, as data comes from a higher layer and is sent down into a lower layer, that data is encapsulated. This means that a new header (and in some instances a trailer as well) is added by the lower layer. It is correct to say that the higher layer "is encapsulated inside" or "is tunneled inside" the lower layer. Likewise on the other end, data arrives from a lower layer and is passed up into a higher layer. As this happens, the header that was previously added is removed. The remaining data (including any remaining higher layer headers) is passed up to the next higher layer. This exact same principle is used when building a VPN. In any VPN, however, the encapsulation is more complex than the standard OSI packaging. VPN encapsulation necessarily involves encryption and hashing of the "carried" payload; i.e. the higher layers.

1. Layer 5 (Application Layer) VPN

The question remains, which is the best type of VPN to use for cyber-exercises? For the SSL VPN at layer 5, encapsulation and cryptography is applied as the traffic exits layer 5. Since this is at a relatively high layer, it offers the advantage of makes it easier to add an SSL layer 5 VPN implementation to a network. This is because it is not necessary to involve the operating system. However, the drawback is that the current design of layer 5 SSL VPNs will only encapsulate http traffic. Since cyber-exercise traffic involves much more than just http traffic, this limitation is impractical and makes an SSL VPN unsuitable for use with a cyber-exercise. Consequently, a layer 5 VPN is not recommended for cyber-exercises. Layer 5 VPNs are currently used for creating secure tunnels between e-commerce clients and servers, e.g. customers and vendors of credit card and PayPal online payment transactions. It allows each individual user to create a secure (typically one-way) VPN and send their secure traffic utilizing an http interface.

2. Layer 2 (Link Layer) VPN

For a layer 2 transfer protocol (L2TP) or point to point transfer protocol (PPTP) VPN, the encapsulation and cryptography are applied as the traffic exits layer 2, i.e. between layer 2 and layer 1. Layer 1 is the actual transmission media. Just as layer 5 was a little too high to be ideal for a cyber-exercise VPN, layer 2 turns out to be too low.

In a typical layer 2 VPN, the higher layer information goes through the encapsulation process and reaches layer 2. There it is then encapsulated and encrypted by cryptographic functions supported by the point to point protocol (PPP). Though this completely encrypted frame (i.e., involving layers two and higher) can be successfully conveyed across the public switched telephone network (PSTN) (i.e., a circuit-switched network, where the transmission path is pre-established prior to data transmission), it cannot be routed through the packet-switched network of the Internet. In order to successfully route these encrypted PPP packets over the Internet, the packets would need to be further encapsulated inside of an IP header by means of a generic routing encapsulation (GRE) header. The packet would then be placed in the appropriate layer 2 frame (e.g., Ethernet, ATM, Frame Relay, 802.11, etc.) for conveyance across the various layer 2 technologies that comprise the Internet.

This is a tremendous amount of unnecessary processing and header overhead considering that cyber exercises are expected to be conducted between networks already directly connected to the Internet. In simpler terms, layer 2 VPN solutions exist to support remote users whose access to the Internet is via the PSTN and where there is little choice in accepting the extra overhead of additional encapsulations. Layer 2 VPN solutions are not ideal for cyber-exercises.

3. Layer 3 (Network Layer) VPN

Finally, for the IPSec VPN, the encapsulation and cryptography is applied as the packet exits layer 3, i.e. between layer 3 and layer 2. This turns out to be the ideal solution for cyber-exercise VPNs. Unlike the layer 5 implementation described above, the only devices that need to be involved in VPN encapsulation and de-capsulation for a layer 3 IPSec VPN are the IPSec VPN endpoint devices. Additionally, all

applications in the upper layers above layer 3 now gain an advantage from the implementation of the VPN at layer 3, since layer 3 is a lower layer. The upper level protocol data unit (PDU) can be carried as a layer 3 VPN payload without any modifications made to the PDU before being VPN processed. A layer 3 IPSec VPN implementation allows all upper layer applications and their PDUs to be processed through the VPN encapsulation and cryptography. At the same time it allows the encapsulated packets to be freely sent over Internet routers, switches, and hubs.

Layer three is the best all around choice in which to implement a cyber-exercise VPN. Properly constructed, the layer 3 IPSec VPN allows all cyber-exercise traffic, regardless of application, to receive confidentiality, integrity, and authenticity protection. Confidentiality is achieved through the use of encryption. Integrity and authenticity are achieved through the proper combination of hash algorithms and the validation of shared secrets or PKI certificate essential credentials.

D. CHAPTER SUMMARY

This chapter has taken a look at the role of cryptography, VPN endpoint authentication, and VPN interaction with the network layers. Cryptography, when combined with robust protocols, attempts to provide any or all of the three information security attributes: confidentiality, integrity, and authenticity. VPN endpoint authentication, using either a pre-shared secret or digital certificate, is essential to ensure VPN function. Finally, a VPN must be properly integrated with the underlying network layers. The next step to understanding how a VPN works is to recognize the interrelations of a VPN with network protocols. An understanding of IPSec is essential. Chapter III begins an examination of this complex yet vital topic.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IPSEC VIRTUAL PRIVATE NETWORK MANAGEMENT

A functioning virtual private network (VPN) uses many varied network protocols, each of them working together to ultimately provide a secure channel for communications. Internet protocol security (IPSec) is a standardized collection of security protocols. If IPSec is improperly employed, all aspects of a VPN can be adversely affected. Therefore, it is crucial that IPSec be examined and understood.

A. IPSEC PROTOCOL BASICS

In addition to the encryption algorithms and authentication hash algorithms mentioned in Chapter II, other main components of IPSec that need to be discussed include security protocols and security modes. The design of IPSec is modular. As the components listed above change and strengthen, the overarching IPSec structure does not have to change but can absorb the new technology. In selecting a VPN implementation and beginning to explain and understand IPSec, it is easiest to start from the inside out, to begin with the most basic component and work outward.

As mentioned in Chapter I, the basic components of security are confidentiality, integrity, and authenticity. In building a VPN the user must know which of these components are required for the intended implementation. Unnecessary attributes may result in putting an unnecessary load on the processor.

B. SECURITY PROTOCOLS: AH AND ESP

IPSec involves two security protocols, authentication header (AH) and encapsulating security payload (ESP). The AH protocol is designed to provide integrity, authentication, and replay protection for the processed datagram. Integrity is provided through the use of an encrypted hash of the protected datagram. Network hash algorithms that are commonly implemented are Message Digest 5 (MD5) and several variants of the Secure Hash Algorithm (SHA). Authentication is provided via the use of the unique shared element, either the pre-shared secret or public key infrastructure (PKI) certificate. This element, which is the basis for encrypting the traffic between the two users, is then used in conjunction with the hash function to provide both integrity and authentication. Replay protection is provided via a

sequence number value available in the AH protocol header. Diagrams of a normal internet protocol (IP) packet and an IP packet with AH is shown below in Figures 1 and 2:

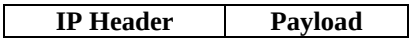

Figure 1. Normal IP Packet

Figure 2. IP Packet Using AH Protocol

AH processing takes the original IP header and payload, plus the pre-shared secret, and hashes this information. This information is carried in the AH header. This AH header is placed in between the IP Header and the rest of the packet, as seen in Figure 2. Upon arriving at the other end of the VPN, the VPN peer, who possesses the pre-shared secret, takes the IP header, payload, and key, and hashes it. The peer then compares this value to the hash value in the AH header. If they match, data integrity is assured. Realize that some of the fields in the original IP header are mutable, i.e. the values change in transit (e.g. the time-to-live field). These mutable fields are excluded from the hash. Therefore it is true that AH only provides partial protection of the IP header. Unfortunately, the AH protocol is not designed to provide confidentiality, i.e. encryption.

The IPSec encapsulating security payload (ESP) protocol is designed to provide integrity, authentication, replay protection, and through the use of encryption, ESP offers confidentiality. ESP can use many of the modern encryption algorithms, including the data encryption standard (DES), 3DES, and the advanced encryption standard (AES). The use of encryption provides a certain amount of protection against network sniffers. Authentication and replay protection are provided in the same way the AH protocol provides these services. With ESP, it is possible to use encryption by itself, but it is better if encryption, the integrity check, and authentication are all used together. If only encryption is used, packets could be manufactured by an attacker to mount a cryptanalytic attack where the manufactured packets could be sent through the VPN and then analyzed and compared to the original packets to eventually

determine the cryptographic key. However, if all three protections are used together, then this attack is defeated. [MAI01]

A VPN packet utilizing ESP will be provided confidentiality, message integrity, and authentication. A block diagram of an ESP packet is shown in Figure 3.

IP Header	ESP Header	**Payload**	ESP Trailer	ESP Authentication Information
Not encrypted, Not authenticated	Not encrypted, authenticated	Encrypted and Authenticated		Not encrypted, Not authenticated

Figure 3. IP Packet Using ESP Protocol

Compare this with the normal IP packet, Figure 1. ESP processing uses encryption and takes the original IP header and the original payload and encrypts them. This serves as the payload for the new packet. A new IP header is placed out front. An ESP header is placed between the newly generated payload and the newly generated IP Header. An ESP trailer and ESP authentication information (unencrypted) is placed at the end of the packet. It is important to note that when the packet arrives at the other end of the VPN, the peer checks the ESP authentication information first. If the arriving packet does not pass the authentication test, the packet is discarded. This prevents the wasting of processing power that might be used to decrypt the packet. This dropping of packets that do not meet authentication requirements also helps lessen the impact of a denial of service attack. Unfortunately, this encryption does not come for free. ESP processing adds approximately 24 bytes per packet. If traffic volume is critical, then this extra 24 bytes per packet must be taken into account.

C. SECURITY MODES: TUNNEL AND TRANSPORT

Now that AH and ESP have been explained, both protocols can work in one of two security modes, either tunnel mode or transport mode.

In transport mode, the ESP (or AH) generated header is inserted immediately before the original IP header, that is, between the packet payload and the original IP header, as shown in the diagrams above. The original IP header cannot be subjected in its entirety to a checksum integrity check since the original IP header contains mutable fields that will change enroute (e.g., the time-to-live field). Therefore in transport

mode only partial authentication can be provided for the header. The header information must not be encrypted since Internet routers must be able to read the header information in order to route the packet.

In order to use transport mode, the device that generates the VPN must also be the host computer. In other words, in transport mode the *user* of the VPN tunnel is also the *provider* of the VPN tunnel. In a cyber-exercise, this is seldom the case. In the typical cyber-exercise that is the focus of this thesis, there is a single device (a VPN security gateway) that is the VPN tunnel provider. Then there is a network of hosts behind this provider that are all VPN users. This VPN security gateway is the only entry and exit point into and out of the exercise network.

Using the AH protocol in transport mode, only the Open Systems Interconnection (ISO) transport layer (layer 4) and higher are affected. Transport mode leaves the layer 3 IP header information exposed, as shown in Figure 4.

IP Header	AH Header	**Payload**
partly authenticated	authenticated	

Figure 4. IP Packet Using AH Protocol in Transport Mode

Compare this to the normal IP packet, figure one. Similarly, using ESP in transport mode leaves the original IP header information exposed as shown in Figure 5.

IP Header	ESP Header	**Payload**	ESP Trailer	ESP Authentication Information
Not encrypted		Encrypted		Not encrypted

Figure 5. IP Packet Using ESP in Transport Mode

To summarize transport mode, as was explained above, the header is not encrypted. The actual source and destination of the VPN datagram is exposed, unencrypted, in the header of a transport mode packet. Even if an attacker can see the true source and destination of the packets, this is not an issue for a cyber-exercise. This means that traffic in transport mode is subject to traffic analysis. Additionally, private IP address space, as defined in RFC-1918 [REK96] is often used as the network address space for the participants of cyber-exercises. Detailed information

concerning VPNs and private address space is further addressed in Chapter V. Using transport mode makes it impossible to route private address space for a cyber-exercise, unless network address translation (NAT) is used.

In tunnel mode, the original IP header is left in place. The original payload and original IP header are then encapsulated, and an entirely new IP header is added in front of this packet. This is true whether tunnel mode is using the ESP or the AH protocol. This, in effect, makes the original IP header part of a new datagram. This has an added advantage in that the source and destination addresses in this new IP header only reflect the IP addresses of the VPN gateway secure tunnel endpoints. The tunnel mode header no longer reflects the IP addresses of the original origin and ultimate original destination of the packet. The original source and destination addresses are encrypted inside the tunnel mode packet as data. Thus tunnel mode provides some protection from traffic analysis. Additionally, tunnel mode is always used between two VPN gateways, i.e. tunnel mode is required when the VPN tunnel provider is not the VPN tunnel user. This is exactly the case in a cyber-exercise, where a VPN device is placed out front of a network of computers.

In tunnel mode, the entire packet is incorporated as data, and a new IP header is placed out in front, as shown in Figure 6. Using tunnel mode effectively hides the original IP header information.

New IP Header	AH Header	**IP Header**	**Payload**
partly authenticated	Authenticated		

Figure 6. IP Packet with AH in Tunnel Mode

Unfortunately, using AH in tunnel mode still does not provide any confidentiality as there is no encryption being used. However, using ESP in tunnel mode results in the original packet being encrypted and incorporated as data. Additionally, a new IP header, whose source and destination address reflects only the VPN gateway endpoints and not the original origin nor ultimate destination of the packet, is placed out in front. Using ESP in tunnel mode provides confidentiality and effectively hides the original IP header information, as shown in Figure 7.

New IP Header	ESP Header	**Original IP Header**	**Payload**	ESP Trailer	ESP Authentication Information
Not encrypted		Encrypted			Not encrypted

Figure 7. IP Packet Using ESP in Tunnel Mode

Protection in this last case is fairly robust. The original IP header information is not only hidden but is encrypted. The exposed IP header information will only expose the addresses of the two VPN secure gateways.

D. AUTHENTICATION AND ENCRYPTION ALGORITHMS

As the reader will recall from Chapter II, a VPN user setting up a VPN has a choice of authentication algorithms and encryption algorithms. Those same principles and concerns already discussed must be paid close attention to. Every time a user chooses to make a VPN more secure using a more robust encryption or hash algorithm, the user pays a performance penalty. Choosing the correct strength of authentication and encryption algorithms for a cyber-exercise VPN is a choice that deserves some careful consideration.

It is important to point out that cyber-exercises between universities do not require robust encryption. Though this statement may at first seem antithetical to the purpose of a VPN, remember that there is no expectation that sensitive (classified or otherwise) information is involved in any of the cyber-exercise traffic encompassed by this thesis. The "privacy" afforded by the VPN in support of cyber exercises is there simply to sufficiently obscure any attack signatures so as not to cause alarm or result in the infiltration of nodes from the intervening Internet infrastructure. The integrity and authenticity afforded by the VPN ensures the exercise participants that no interloper has inserted him/herself into the exercise. Further, as a safety feature, the VPN-encrypted traffic will pose no harm to non-participating Internet nodes in the off chance that malicious exercise related traffic gets misdirected.

E. INTERNET KEY EXCHANGE SECURITY ASSOCIATION (IKE-SA)

Once a user determines what needs to be protected and chooses the appropriate security protocols and modes, the actual VPN can be built. The Internet Security Association Key Management Protocol (ISAKMP) [MAU98] defines a framework for

authenticating and exchanging information with a peer, but does not specify the exact procedures utilized in each case. The internet key exchange (IKE) provides a specific key management system. IKE has two phases.

During IKE phase I, the IKE security association (IKE SA) is built. For phase I, the user is required to select an authentication method, which can be either a pre-shared secret or a digital certificate. This shared unique element serves to authenticate the end points and encrypt several parameters that will form the basis of operations conducted during the IKE phase II. When phase I is complete, both VPN peers have been authenticated and possess a shared secret key.

IKE phase I may be conducted in one of two modes, main mode and aggressive mode. Both main and aggressive mode are designed to meet all requirements of IKE phase I. Main mode accomplishes the goals of phase I with three two-way message exchanges for a total of six messages. Aggressive mode uses three messages total.

Using main mode, the first message exchange consists of both VPN peers agreeing on which algorithms and hashes to use. During the second exchange, authentication material, either the pre-shared secret or a public key, is traded in the clear, and the Diffie-Helman (DH) key exchange protocol is used. Through the use of DH, each peer generates the same shared secret key. During this second exchange, a nonce is also sent to thwart a man in the middle attack. The third and final exchange serves to complete the authentication of the peer.

Using aggressive mode, the first message from the initiating peer includes all the material included in the first two messages of the main mode. During the second message of aggressive mode, the responding peer sends back all information that is needed for a complete exchange, leaving the third message serving to confirm receipt of the second message.

Using either main mode or aggressive mode completes the requirements of phase I. A secure tunnel is now built between the peers. This tunnel can be used to exchange information to facilitate IKE phase II.

F. INTERNET PROTOCOL SECURITY (IPSEC-SA)

Once the endpoints of the tunnel are established and authenticated during IKE phase I, the second IKE phase begins. IKE phase II is concerned with the building of the IPSec SA. The purpose of the IPSec SA is to tell the VPN device how to protect the data packets that travel in the VPN tunnel.

1. Quick Mode

There is only one mode for IKE phase II, called the *quick mode*. Phase II consists of two messages. Working through the secure IKE SA tunnel established by IKE phase I, the two peers must agree on an IPSec SA. During the first message, Peer A authenticates itself to Peer B and proposes an IPSec SA. The IPSec SA consists of an encryption algorithm, a hash algorithm, security mode and security protocol, for example, 3DES, SHA-1, ESP, tunnel mode. During the second message, Peer B replies to Peer A, authenticating itself and letting Peer A know if Peer B has a matching IPSec SA. If a match does not exist, then the tunnel to transmit data cannot be built. However, if a matching IPSec SA exists, then during message three Peer A responds that it has correctly received information from Peer B. Data transmission can begin.

2. Static and Dynamic Keying

The IPSec SA includes a cryptographic key. This key is not chosen by the VPN initiator, rather this key is automatically negotiated as part of the IKE phase II protocol. A decision must be made about this negotiated IPSec SA key. Depending on the security and performance requirements of the VPN users, the VPN designer can choose to have the IPSec SA key remain constant throughout the duration of the VPN. Alternately, the key can be chosen to be a dynamic key and it will be automatically renegotiated after a user-chosen period. The renegotiation criteria are based on either time or kilobytes of data processed since the last IPSec SA key negotiation.

3. Perfect Forward Secrecy

A security concern exists with regard to the IPSec SA. Recall that the IPSec SA is the security association that is encrypting the data being sent. The key that is being used to encrypt the traffic can be automatically set to regenerate based on either time or number of kilobytes processed. If an attacker were able to obtain a current key

being used to encrypt data, the attacker might possibly be able to derive the next key to be generated. The attacker would then be able to decrypt all future packets. This concern is countered by a cryptographic concept known as perfect forward secrecy (PFS).

DH key exchange protocol allows two peers to generate a session key, i.e. a symmetric key to be used to establish the IKE SA. The same DH techniques are used to achieve PFS by having the peers periodically generate new symmetric keys within the IPSec SA. These new keys are not based on either previous symmetric keys or any long-term secrets that may be stored at either endpoint. This provides PFS and makes it unlikely for an attacker, upon breaking one key and having access to a block of packets, to be able to break the next key and decrypt more data. The attacker will have to work just as hard to break future keys as he/she did to obtain the first key.

G. SPD, SPI, AND SAD

These are three very similar terms that warrant explanation because they can easily be confused. Unfortunately, they are all interrelated in a circular fashion and the explanation of one involves the mentioning of the other. Therefore, these three items will simply be addressed in alphabetical order. Finally, an example will be given that will show the reader the interrelation of all three.

The security association database (SAD) is a list of IPSec SAs that is maintained by the peer. It maintains all the necessary information about each SA. This information includes the security protocol, the security mode, the encryption method, and authentication method.

The security policy database (SPD) conducts a type of packet filtering similar to that of a router access control list (ACL). The SPD maintains entries of all types of traffic. If an IPSec packet is detected, an entry in the SPD will tell the peer to go ahead and take the next step and look in the SAD to obtain the appropriate keys and protocols for use with that specific packet.

The security parameter index (SPI) is a field in the header of a packet that identifies which IPSec SA the packet belongs to. The peer device, upon receiving the

packet and looking at the SPI then knows which IPSec SA can successfully process that packet.

What follows is an example that relates all three terms. As a packet comes into the VPN peer device, the peer device looks at the header and determines that it is an IPSec packet due to a match found in the SPD. The peer inspects the SPI value in the header. The VPN peer then refers to the SAD, where it finds the correct SA keys and protocols to process the packet.

H. USE OF DIGITAL CERTIFICATES FOR VPN ENDPOINT AUTHENTICATION

In a cyber-exercise, there may potentially be more than two entities since several agencies may desire to participate. As the number of participants, and thus VPN endpoints, grow, there are inherent disadvantages to using pre-shared secrets as the underlying authentication method. Firstly, the cyber-exercise administrator must keep track of all keys for all participants. Secondly and more importantly, when it is time to change the keys, every user must update all the keys for all participants simultaneously.

Neither of these issues presents a truly insurmountable problem for cyber-exercises. However, the reason a cyber-exercise exists in the academic context is to educate the exercise participants. As the participants take the concept of the VPNs learned in the cyber-exercise and apply it to real world situations, the second issue of having all users update their pre-shared secret at the same time becomes a problem. For example, having learned the process for setting up a VPN as part of a cyber-exercise, exercise participants may one day be faced with a real world VPN. They would have the decision of whether to use the pre-shared key method for authentication. If there was a VPN being utilized between several banks, and one of the bank's pre-shared secret was compromised in the middle of the day, then it would be very difficult to have all the other banks update the compromised key information with the new key and keep the system up and running. A more scalable way to handle VPN endpoint authentication is to use x.509v3 digital certificates, commonly called "certificates". [ADA99]

Certificates can provide VPNs with easy scalability so long as the infrastructure that supports certificate management (i.e. PKI) is fully operational and utilized by all parties of the VPN. A centralized certificate authority (CA) issues certificates to each VPN endpoint in a hierarchical fashion. Through the use of digital signatures and this hierarchical structure, each VPN endpoint is able to verify the certificates of other VPN endpoints. If the certificate of one VPN endpoint was compromised, then that endpoint would apply for and be issued a new certificate by the CA. Once this new certificate is installed at the compromised end point, all other VPN endpoints can simply verify the new certificate using their own copy of the CA's public key, rather than having to manually update a new shared key on the VPN gateway.

There are multiple steps involved in configuring a VPN endpoint to use a certificate [MAS99, MAS04]. The VPN endpoint must:

(1) Identify a CA

(2) Generate Keys

(3) Enroll the Device

(4) Submit credentials to the CA for Certificate Generation

(5) Install the certificate

(6) Be configured to issue its certificate

(7) Be configured to accept certificates from other devices

(8) Be capable of verifying received certificates

1. Identify a CA

This is the CA that will provide a certificate. CAs can be contacted either in band or out of band. In the case of an in band request, the simple certificate enrollment protocol (SCEP) has been developed to facilitate in band requests. If the request is out of band, then voice, or CDs, floppies, or FAXes can be used to deliver the certificate information to the CA. Several commercial companies support CAs. It

is also possible to build a CA on site. NPS has built just such a CA, based on the Netscape Certificate Management System (NCMS).

2. Generate Keys

The VPN endpoint must generate a public and private key pair. RSA key pairs, consisting of a public key and a private key, can be generated in increments of between 512 and 2048 bytes. The private key is maintained (stored securely) by the endpoint, while the public key is used by the CA in the enrollment process.

3. Enroll the Device

The VPN endpoint makes a certified request to the CA for its certificates. The public key cryptography standard #10 (PKCS#10) certificate request is the standardized method used to do this. Information required by the PKCS#10 includes the common name of the endpoint, the organization name, locality, and state. This PKCS#10 request and the public key of the VPN endpoint are sent to the CA. As mentioned above, this certificate request can either be sent over the internet or via other out of band means.

4. Submit Credentials to the CA for Certificate Generation

The CA then generates a certificate for the VPN endpoint. The certificate is created when the CA uses its private key to encrypt ("sign") the hash of the user's identifying credentials together with his/her public key. The resulting certificate can be used for one of three common purposes: proof of identity, authentication, or encryption. Depending on the method of IKE-SA authentication, the purpose of the VPN gateway certificate will be authentication and/or identity. The CA has its own certificate. If the CA is at the top of the hierarchical tree then that CA has a root, or "self-signed", certificate. If the CA is a non-root CA then it will have a "subordinate" certificate; i.e., a certificate that is signed by a higher level CA (possibly the root CA). Once the appropriate certificates have been generated and copied to the CA's database, the CA sends the requested certificate(s) along with its own and any parent certificates to the requesting VPN endpoint.

5. Install the Certificate

Once the certificates are received by the VPN endpoint, they are validated and installed on the device. The exact process for this varies from device to device.

6. Be Configured to Issue Its Certificate

The endpoint device must be properly configured to issue its certificate in order to interact with peer devices that also use certificates for authentication. The exact configuration steps vary from device to device.

7. Be Configured to Accept Certificates from Other Devices

The endpoint device must be properly configured to accept digital certificates as the means for authentication from peer devices. This configuration action will be elaborated upon in Chapter V.

8. Be Capable of Verifying Received Certificates

Finally, the peer device must be able to verify that the certificate received from a peer is current and valid. A certificate revocation list (CRL) is maintained by CAs for this purpose. The endpoint device must be properly configured to check the certificate received from a peer and verify that the certificate received is not on the CRL. There are alternative methods of achieving certificate revocation validation (e.g., OCSP, SCVP, delta-CRLs, Merkle-Trees, etc.), but these mechanisms are even less widely supported than the simple full CRL method mentioned here. [HOU02, MYE99]

I. SPLIT-TUNNELING

In mentioning the security association database above, the idea of split tunneling must be addressed. Whether to permit split tunneling is a choice a VPN user needs to make. Traffic originating from a network can either go into the VPN tunnel, can be sent outside the VPN tunnel (unprocessed by IPSec), or can be dropped. Split tunneling occurs when the user makes the choice to allow some traffic to leave the network without entering the tunnel. There are two scenarios:

If a VPN designer desires that traffic to a targeted network or networks be processed by IPSec and sent via the VPN, yet other traffic sent in the clear, i.e. outside the VPN, then the user implements split tunneling. The entries in the security association database are compared to the destination address of an incoming packet. If it is destined for a targeted VPN network, then the SAD references the SPD, and the appropriate IPSec SA is applied. If the traffic is not destined for a targeted VPN

network, then the traffic is sent in the clear. This is a common scenario before a cyber-exercise. The traffic being sent to other agencies needs to go through the VPN. Yet at the same time participants are making final preparations and hardening their networks for the cyber-exercise. They need to be able to send traffic in the clear to various websites not involving the VPN.

If a user desires that traffic to a target network be tunneled, yet all other traffic be dropped, the user is in effect calling for the VPN to drop any packets whose destination address in not already recorded in the security policy database, i.e. packets that are not destined for another participating VPN endpoint. This is the case during the cyber-exercise. Since cyber attacks are being launched and potentially employing hacker tools, the administrators of the cyber-exercise desire that all exercise traffic be sent only through VPN tunnels to other competitors. Under no circumstance should there be an opportunity for a cyber-exercise attack packet to be sent in the clear to an address on the Internet that is not involved in the exercise.

J. CHAPTER SUMMARY

This Chapter has provided a review of IPSec, security modes, and security protocols. The interaction of the security policy database (SPD), security association database (SAD), and the security parameter index (SPI) were examined, as well as the interrelation of digital certificates and the employment of split tunneling. Now that these components of a VPN have been explained, they can now be mapped to the needs of building a VPN for a cyber-exercise. Chapter IV describes the characteristics of each VPN component, and tells how suitable that component is for building a VPN to support a cyber-exercise.

IV. CYBER-EXERCISE NEEDS

Building on what has been illustrated in Chapter III about all the potential choices in virtual private network (VPN) technology, the desired characteristics of a VPN for use in a cyber-exercise will now be reviewed.

A. ARCHITECTURE: LAYER 2, LAYER 3, OR LAYER 5

Since a cyber-exercise will be conducted between the networks of two or more universities or agencies, the VPN must span all participating networks. Chapter II discussed the interaction of VPN technology over three different layers of the Open Systems Interconnection (OSI) model. In examining the needs of a cyber-exercise, the most likely configuration for the exercise is two networks which are linked together. The cyber-exercise VPN gateway is placed in front of the cyber-exercise participant's network. Current technology to link networks utilizes an IPSec-based layer 3 VPN. The linking of these two networks is commonly called a LAN-to-LAN VPN. The building of this "LAN-to-LAN" VPN will be looked at in Chapter V. Linking cyber-exercises will require a LAN-to-LAN VPN.

B. IKE SA: PRE-SHARED KEY OR DIGITAL CERTIFICATE

Cyber-exercise participants could choose to use pre-shared keys or digital certificates for VPN endpoint authentication. Pre-shared keys are simpler to both understand and implement. Digital certificates are more complex to understand and implement, yet provide a greater measure of scalability. Since there will be a finite number of participants in a cyber-exercise, the ease and security of pre-shared keys makes them preferred to digital certificates. Additionally, since the skill level of the cyber-exercise participants is unknown, digital certificates may add an unnecessary level of complexity that is not needed. If a cyber-exercise participant is unable to get digital certificates working on their VPN, this would exclude them from the exercise.

C. IPSEC SA: STATIC KEY OR DYNAMIC RE-KEYING

A static internet protocol security (IPSec) security association (SA) key that processes all data and remains the same throughout the life of the VPN is simpler. However, if the cyber-exercise traffic was captured and the key decoded by a third

party, all exchanges between the VPN parties could be read. If the cyber-exercise were still in progress, the third party could continue to follow the conduct of the exercise.

A dynamic IPSec SA key that changes throughout the cyber-exercise is more complex to implement, but it would prevent the third party monitoring problem mentioned above. If the key is dynamically changed, even if all cyber-exercise traffic was captured and recorded, the third party could only read a subset of the traffic before needing to stop and decode the new IPSec SA key for the next segment of cyber-exercise traffic. Of course if the key was changed so often that there was not enough packet data to conduct and effective cryptographic analysis, then perhaps none of the cyber-exercise traffic could be read.

It is important to note that the primary concern of cyber-exercise participants is the simple obscuration of the traffic between the two schools. An extremely high degree of confidentiality, i.e. strong encryption, is not required. There is no confidential or otherwise classified traffic that needs to be protected. Therefore a static pre-shared secret will provide adequate security for a cyber-exercise. Dynamic re-keying would only be used if the cyber-exercise administrator felt the need to implement this dynamic re-keying mechanism for the educational benefit of the participants.

D. SECURITY PROTOCOL: AH OR ESP

Cyber-exercise participants must choose between the encapsulating security payload (ESP) and authentication header (AH) security protocol. After examining their characteristics in Chapter III, the reader will realize that cyber-exercise participants require the ability to obscure traffic between the VPN endpoints using encryption. AH does not allow the use of encryption. ESP is the only security protocol that provides this needed confidentiality. Despite the increased processor load and the extra 24 bytes per packet, the confidentiality needs of a cyber-exercise call for ESP to be used.

E. SECURITY MODE: TUNNEL OR TRANSPORT

Cyber-exercise participants must choose between tunnel or transport mode. During a cyber-exercise, the network for the participant will lie behind the VPN gateway device. As discussed in Chapter III, using transport mode means that the tunnel endpoint is the tunnel provider. This is an unlikely the case for cyber-exercises. Therefore tunnel mode should be used for a cyber-exercise. One rare exception to this is the case where a participant school with very few resources to allocate to the cyber exercise may wish to participate using only a single computer. The school will likely run multiple target servers and scanning/assessment software from this one machine. Only in this unlikely instance would transport mode would be appropriate.

F. ENCRYPTION ALGORITHM PERFORMANCE: DES, 3DES, AES

Within both the internet key exchange (IKE) SA and the IPSec SA, an encryption algorithm must be chosen. Common choices include the digital encryption standard (DES), 3DES, and the advanced encryption standard (AES128, AES192, AES256). General technical information about the algorithms has already been discussed in Chapter II, but here performance information will be considered.

Research into the comparative performance of modern encryption algorithms was unable to locate one resource that compared all algorithms under the same conditions. The relative performance of the algorithms changed with respect to the size of the traffic the algorithm was processing [DHA02, CIS777]. A recurring phrase was concerning the precise performance of an algorithm was “it depends”. Exact performance varies depending on the operating system, the type of processor, and, as mentioned, the size of the packets that are being transmitted. Therefore, the rankings in the table below are not able to be quantified with meaningful numbers, i.e. saying that a certain algorithm is always X-percent faster than another algorithm. Nevertheless a highest through lowest throughput ranking was able to be assembled after consulting several sources. The findings are detailed in Table 1.

Through reviewing test results from Dr Wei Dai and Cisco documentation, AES128 (i.e. Rijndael-128) provided the highest throughput [DAI01, CIS05].

AES192 provided the second highest throughput, followed by AES256 [DAI01]. Tests conducted by Dr. Bart Preneel during the New European Schemes for Signatures, Integrity, and Encryption (NESSIE) Project, and supported by Dr Dai's research, showed that DES provided lower throughput than all AES algorithms tested [DAI01, PRE01]. Finally, Cisco test results [CIS05] as well as testing at the Oak Ridge National Laboratory, found that 3DES provided the least throughput [AMP01, DUN96]. The algorithms are listed from highest throughput to the lowest throughput in Table 1.

Highest Throughput
AES128
AES192
AES256
DES
3DES
Lowest Throughput

Table 1. Encryption Algorithm Performance Comparison

G. ENCRYPTION ALGORITHM STRENGTH

It may be tempting to conclude that encryption algorithm strength is directly related to key length, but this is not necessarily the case when comparing distinct algorithms. Algorithm strength depends not only on key length but on how resistant the algorithm itself is to cryptanalytic attack. Research conducted by Dr Lenstra (results listed in Table 2) provided a ranking of the relative security of common algorithms [BEY02, LEN99]. A remark in a Cisco configuration guide supports this, concluding that AES is the most secure [CIS06]:

Most secure
AES256
AES192
AES128
3DES
DES
Least Secure

Table 2. Encryption Algorithm Strength Comparison

Additional research confirmed that DES offered adequate security until 1997 [LEN99, DES01]. In 1999, DES encryption was defeated as part of a computer challenge competition in just 22 hours. [ENC02] Taking a look at 3DES, as of 1998 3DES did not have a security problem [DEN98] but 3DES did have an efficiency problem [REA01]. The search for a faster, yet still secure algorithm, is what prompted the Advanced Encryption Standard (AES) series of conferences. [REA01].

H. HASH ALGORITHM PERFORMANCE: SHA-1 VS. MD5

To use both the IKE SA and the IPSec SA, a hashing algorithm must be chosen. Chapter II provided an overview of the functionality of Message Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA-1). When considering the optimum hashing function to use for a cyber-exercise, performance must be considered. When SHA-1 and MD5 throughput were compared, MD5 provided higher throughput than SHA-1 [BAL96, TOU96] as shown in Table 3.

Highest Throughput
MD5
SHA-1
Lowest Throughput

Table 3. Hash Algorithm Performance Comparison

I. HASH ALGORITHM STRENGTH: SHA-1 VS. MD5

When considering a hashing function to use for cyber-exercises, the strength of the hashing function must also be considered. As detailed in Chapter II, SHA-1 produces a 160-bit hash while MD5 produces 128-bit hash. The MD5 hash function, in certain cases, has been shown able to be defeated [ENC01]. Defeating a hash algorithm involves being able to generate a pair of messages that produce the same hash. The SHA-1, when used within the Hashed Message Authentication Code (HMAC) has not been defeated [GLE98]. The MD5 and SHA-1 hash algorithms are ranked according to security in Table 4.

Most Secure SHA-1 MD5 Least Secure

Table 4. Encryption Algorithm Strength Comparison

J. VPN GATEWAY DETAILS: CONCENTRATOR, ROUTER, OR COMPUTER

The first option for a VPN gateway is to build the gateway on a dedicated general-purpose computer using software. The advantage to this is that any organization that wishes to participate in a cyber-exercise, regardless of their budget, can configure an extra lab computer to act as their cyber-exercise VPN gateway. There are several freeware/open-source VPN software packages, such as FreeS/WAN, that allow a knowledgeable individual to turn a general-purpose computer into a VPN gateway. The disadvantage is that often the encryption options are limited to those built into the software by the software package programmer. Software based VPNs can be difficult to scale, especially if the user chooses to implement some of the advanced VPN features such as dynamic key sharing.

The second option for a VPN gateway is a router that is VPN-capable. It is similar to the software solution. Hopefully an organization that wants to participate in a cyber-exercise has a router that is either VPN-capable, or can purchase the necessary IOS upgrade to make it that way. This solution is more expensive than the software solution but also provides the VPN cyber-exercise administrator with more options in selecting security modes, encryption algorithms, etc. Additionally, router-based VPNs are likely to be more thoroughly tested for security, and are generally much easier to configure than the open source software counterparts.

Finally, the last option examined for use as a VPN gateway is the dedicated VPN Concentrator. Similar to the router, the VPN Concentrator that was examined as part of this thesis could actually perform the functions of many different network components: a DHCP server, a firewall, and an intrusion detection system. Schools wishing to teach and practice “defense-in-depth” via their involvement in cyber-

exercises may appreciate having a single device that can be used to employ multiple facets of network defense: firewalling, intrusion detection, and encrypted tunneling.

As shown in Chapter I, VPN users have a choice of VPN gateway devices. VPN concentrators, VPN-capable routers, and general purpose computers running VPN software can all be used to create a VPN. VPN concentrators are specialized devices and may not be available to all participants. End user computers running VPN software are accessible to all participants. However, the most popular open source VPN software, FreeS/WAN, has just had development discontinued as of March 1, 2004. [FSW01, SCH04] There was a final elease of FreeS/WAN 2.06 on April 22, 2004, but the development group no longer exists.

Routers, however, are accessible to all cyber-exercise participants. Making a router VPN-capable only involves a change in its internetwork operating system (IOS). As will be shown in Chapter V, Cisco routers incorporate an easy to understand graphical user interface (GUI) based configuration interface, called the security device manager (SDM). This GUI also allows the user to graphically picture all components of the VPN, i.e. the IKE SAs and the IPSec SAs. This aids in user understanding of the VPN. Since most cyber-exercise participants will have access to a VPN-capable router, coupled with the fact that the cyber-exercise participants are most easily able to visualize the building of the VPN on the router GUI, the VPN-capable router has advantages that surpass the other competing devices.

K. CHAPTER SUMMARY

This chapter has related the theoretical concepts of the VPN, discussed in Chapter I and Chapter II, to the building of a VPN for a cyber-exercise. VPN architecture, endpoint authentication, keying, and security protocols and modes have been related from the theoretical to the practical. Encryption and hash algorithms have been examined for performance and security. In light of the needs of cyber-exercise participants, gateway devices received a close look. The building of an actual VPN will take this theorectical knowledge and employ it within commercial devices. Chapter V shows the building of three VPNs.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THREE VPN ALTERNATIVES

Now that a close look has been taken at the theory behind virtual private network (VPN) technology, three techniques will be shown to build VPNs between two devices. The two devices are a Cisco 3005 VPN concentrator, and a Cisco 2651XM router. These devices were chosen because they are representative of typical devices that many cyber-exercise participants may already possess, or can easily obtain. The devices used in this thesis were donated by Cisco to the Naval Postgraduate School. The three techniques will entail: 1) a graphical user interface (GUI) based configuration of the concentrator, 2) GUI-based configuration of the router by way of the security device manager (SDM) interface, and 3) a command line interface (CLI) configuration of the router. In the end, the two devices will be interchangeable as VPN endpoints, e.g. a VPN could exist between the Cisco concentrator and Cisco router with SDM, or between the Cisco router with SDM and Cisco router using CLI, or any combination.

In Chapter IV, a cyber-exercise VPN was proposed that consisted of LAN-to-LAN connection using the encapsulating security payload protocol in the tunnel mode with a pre-shared static key. In the following example below, a VPN will be built on a Cisco router using the command line interface, on a Cisco router using the SDM, and on a Cisco VPN concentrator. The parameters used for this example are shown in Table 5.

IKE Policy
Encryption: 3DES
Hash: MD5
Authentication: Pre-Share
IPSec Transform Set
Mode: ESP, Tunnel
Encryption: 3DES
Authentication: MD5_HMAC

Table 5. VPN Parameters for the Example VPN

In Chapter VI, there will be a further discussion of precisely which encryption and hash algorithms should be chosen for the optimum VPN for a cyber-exercise.

A. ROUTER TO ROUTER USING CLI

One option for a LAN-to-LAN VPN is to use VPN-capable routers for both VPN gateways. The Cisco Corporation provided two 2651XM Routers for evaluation to the Naval Postgraduate School's Center for Information Systems Security Studies and Research (CISR). These two routers were used for construction of the router-to-router VPN discussed in this section.

1. VPN Capability of Intended Routers

The first step in setting up a router-based VPN is to determine if the routers are VPN-capable. VPN functionality is enabled in two phases within Cisco routers. First, the router's Internetwork Operating System (IOS) needs to be of capable of handling VPN commands. Second, the router may have a Cisco VPN Hardware Accelerator card installed. This card is a hardware component that can be user-installed within the router to enhance its performance. [CIS03]

The quickest and easiest way to determine if a router IOS is VPN-capable is to create the initial configuration, described below, and get to the router's configuration (config t) mode, and type "crypto ?" to see if the router recognizes the crypto series of

VPN commands which would be indicated by a reply listing related crypto options; e.g., ipsec, isakmp, map, etc. If the router understands the "crypto" command, then the router has VPN functionality incorporated into its IOS. An alternate way would be to try to reference the Cisco IOS the router is running and see if that IOS supports VPN functionality. There does not appear to be a free resource that does this. In order to get this information, a Cisco Connection Online (CCO) account is needed. CCO accounts are an item that Cisco sells. Thus, if a router purchase or router evaluation request is planned for a university and VPN functionality is desired for cyber-exercises, Cisco representatives will be able to discuss which IOS needs to be ordered with a router in order to assure VPN functionality.

If the router IOS is VPN-capable, the router may have a VPN accelerator hardware card installed. Cisco calls such hardware devices advanced interface modules (AIMs). [CIS01] The VPN accelerator AIM takes the encryption processing load off the router's primary CPU. According to Cisco documentation, an AIM equipped router results in up to a 10x performance increase over a non-AIM equipped device. The AIM that is compatible with the NPS BNP 2651XM router is either the AIM-VPN/Base Performance (BP), or the AIM-VPN/Enhanced Performance (EP) module. Realize that for cyber-exercises, the AIM is not normally needed, and was not used for this thesis.

To determine if a router has an AIM installed, from the router privilege mode, use the "show version" command. An abbreviated list of what is returned shown in Table 6. Notice the AIM, if installed, will be displayed as "1 Virtual Private Network (VPN) Module(s)" below the list of available interfaces [CIS02], as shown in Table 6.

```
BNP_VPN#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(15)ZJ3, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc2)

System image file is "flash:c2600-jk9o3s-mz.122-15.ZJ3.bin"

Cisco 2651XM (MPC860P) processor (revision 0x200) with 125952K/5120K bytes of
memory.
Bridging software.
4 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial(sync/async) network interface(s)
1 Virtual Private Network (VPN) Module(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)


Configuration register is 0x2102
```

Table 6. Verifying Router Installation of the AIM

2. Network Planning/Analysis for the Cyber-Exercise

The scenario for the cyber-exercise VPN for this thesis involves two networks. The first network is the NPS Bastion Network, behind the NPS firewall. The second network is made to simulate another university or agency participating in the cyber-exercise, which for the purposes of this thesis is called the University of C (U of C). This network is not behind a firewall, however if it was, techniques similar to those that NPS uses to pass VPN traffic through the NPS firewall would be used to allow VPN functionality with U of C.

If a cyber-exercise was being planned from scratch, much thought would have to go into the address spaces that lie behind the VPN gateways, i.e. on the "private" (vice "public") side of the VPN. It is easiest to use an IETF allocated private address space. Table 7 lists private address space, as defined in RFC 1918. [REK96]

Private: 10.0.0.0 - 10.255.255.255 (/8 prefix)
Private: 172.16.0.0 - 172.31.255.255 (/12 prefix)
Private: 192.168.0.0 - 192.168.255.255 (/16 prefix)

Table 7. Private IP Address Space

In the case of the planned cyber-exercise between NPS and U of C, the network structure was predetermined. The network information for both parties is shown in Table 8 and Table 9. A diagram of the router to router LAN-to-LAN network is shown in Figure 8.

NPS BNP_VPN Gateway IP: 131.120.8.199/22
NPS BNP_VPN Network Default Gateway: 131.120.8.1
NPS BNP Cyber-exercise Network ID: 10.1.0.0/24

Table 8. NPS Bastion Network Project (BNP_VPN) IP Information

U of C VPN Gateway IP: 63.205.26.67/27
U of C Network Default Gateway: 63.205.26.65
U of C Cyber-exercise Network ID: 192.168.0.0/24

Table 9. University of C (UofC_VPN) IP Information

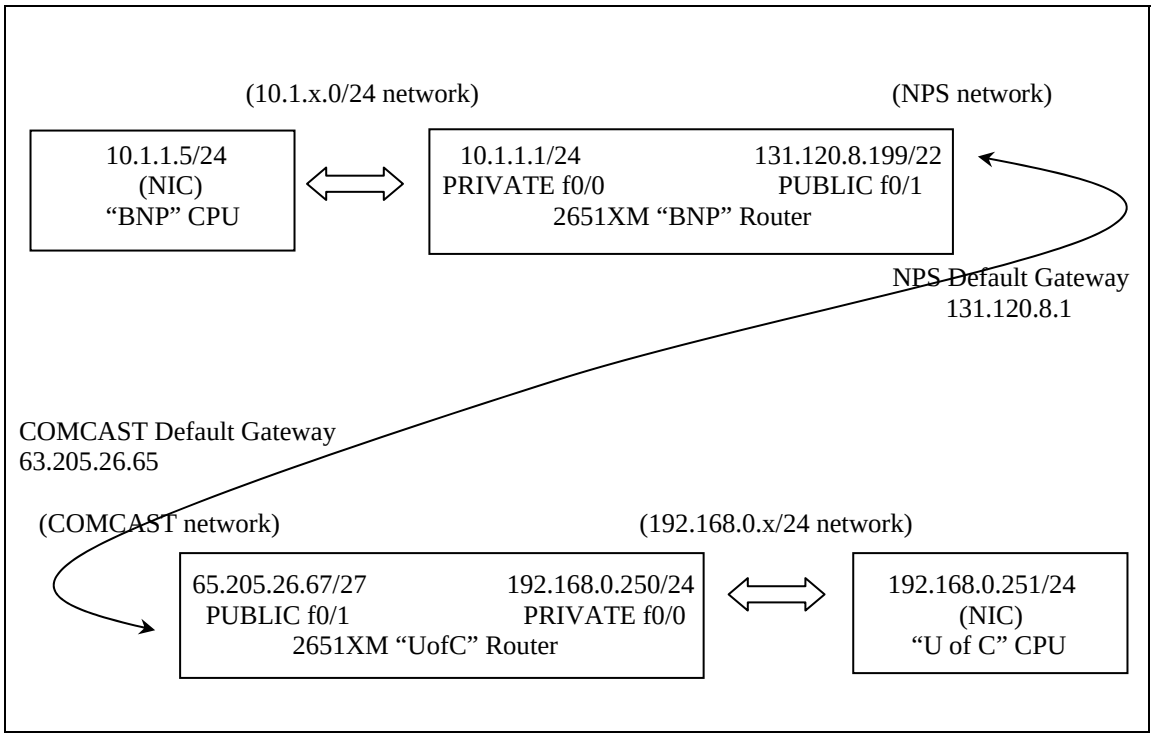

Figure 8. Router to Router Network Diagram

3. Basic Configuration of the NPS BNP Router

All router configurations usually begin with a router connected via a console cable. Instructions for how to do this can be found in Cisco Documentation, i.e. Cisco 2600 Series Routers Hardware Installation Guide.

Ensure that the router is powered off. Connect the provided console cable from the serial port (COM1) on a computer to the "console" port on the router. Open a hyperterminal connection on the computer and ensure the settings listed in Table 10 are entered. Data that is entered by the user is shown in bold. Information provided by the device is shown in normal font.

```
Connect using:   COM1
Bits per second: 9600
Data Bits:       8
Parity:          None
Stop Bits:       2
Flow Control:    None
```

Table 10. Configure the Hyperterminal Connection

This will open an active hyperterminal connection to the router. Power on the router. This will result in the IOS image of the router decompressing into the router's RAM. The progress of the decompression process is depicted on the hyperterminal screen via a sequence of many pound (#) signs.

Taking into account the NPS BNP information and the network diagram in Figure 8, the following commands in Table 10 are entered into the router.

```
Would you like to enter the initial configuration dialog? [yes/no]: y
Would you like to enter basic management setup? [yes/no]: n
First, would you like to see the current interface summary? [yes]: n
  Enter host name [Router]: NPS_BNP
  Enter enable secret: MyPassword2
  Enter enable password: MyPassword3
  Enter virtual terminal password: MyPassword4
  Configure SNMP Network Management? [yes]: n
  Configure LAT? [yes]: n
  Configure bridging? [no]: n
  Configure IP? [yes]: y
    Configure RIP routing? [yes]: y
  Configure AppleTalk? [no]: n
  Configure DECnet? [no]: n
  Configure CLNS? [no]: n
  Configure Async lines? [yes]: n
Do you want to configure FastEthernet0/0  interface? [yes]: y
  Use the 100 Base-TX (RJ-45) connector? [yes]: y
  Operate in full-duplex mode? [no]: n
  Configure IP on this interface? [yes]: y
    IP address for this interface: 10.1.1.1
    Subnet mask for this interface [255.255.255.0] : 255.255.255.0
Do you want to configure Serial0/0  interface? [yes]: n
Do you want to configure FastEthernet0/1  interface? [yes]: y
```

```
  Use the 100 Base-TX (RJ-45) connector? [yes]: y
  Operate in full-duplex mode? [no]: n
  Configure IP on this interface? [yes]: y
    IP address for this interface: 131.120.8.199
    Subnet mask for this interface [255.0.0.0] : 255.255.252.0
Do you want to configure Serial0/1  interface? [yes]: n
Do you want to configure Serial0/2  interface? [yes]: n
Do you want to configure Serial0/3  interface? [yes]: n
Do you want to configure Ethernet1/0  interface? [yes]: n
Do you want to configure Ethernet1/1  interface? [yes]: n
Do you want to configure Ethernet1/2  interface? [yes]: n
Do you want to configure Ethernet1/3  interface? [yes]: n
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to NVRAM and exit
    Enter your selection [2]: 2
```

Table 11. Configure the Bastion Network Project Router

In order to ensure compatibility with a sniffing hub, it is a good idea to set the port speed to 10MBps. Use the commands shown in Table 11.

```
BNP_VPN#config t
BNP_VPN(config)#int f0/1
BNP_VPN(config-if)#speed 10
BNP_VPN(config-if)#duplex half
BNP_VPN(config-if)#int f0/0
BNP_VPN(config-if)#speed 10
```

Table 12. Set Router Port Speed to 10MBps

There are only a few steps remaining. The VPN designer, before VPN functionality is added, must ensure connectivity from the router to the rest of the network. The IP default-gateway command ensures that if a packet's destination address is not in the router's routing table, the packet is sent to the router's default gateway where it will be properly routed. Do this according to the settings in Table 12.

```
BNP_VPN>en
BNP_VPN>password
BNP_VPN#config t
BNP_VPN(config)# ip default-gateway 131.120.8.1
BNP_VPN(config)# exit
BNP_VPN#exit
```

Table 13. Configure the Router Default Gateway

Taking into account the U of C information, Table 9, and the network diagram, Figure 8, a similar set of commands is entered into the peer router.

4. Entering VPN Functionality in the Routers

At this point both routers are configured to route traffic, but not to tunnel (VPN) traffic. It is wise to test the connectivity of the two routers to ensure that they

can communicate before any VPN functionality is added. Ping checks followed by a trivial file transfer protocol (TFTP) transfer of a small file is one recommended way to do this.

5. Command Line Configuration of the VPN

In order to implement this VPN via the CLI on the router, enter the commands as shown in Table 14.

Step	NPS BNP_VPN Router Commands	Purpose
1	BNP_VPN>**en** BNP_VPN>**password** BNP_VPN#**config t**	Puts router into general configuration mode.
2	BNP_VPN(config)#**crypto isakmp policy 1**	Begins the configuration of the IKE policy that will be used during the establishment of the IKE SA. This policy number, in this example, number "1", can be any number between 1-10000.
3	BNP_VPN(config-isakmp)#**encryption 3DES**	Notice the router entered "config-isakmp" mode. Specifies 3DES as the encryption algorithm within IKE policy #1.
4	BNP_VPN(config-isakmp)#**authentication pre-share**	Specifies a pre-shared secret as the authentication method. A pre-shared secret is a symmetric key.
5	BNP_VPN(config-isakmp)#**group 2**	Specifies Diffie-Helman Group Two for the exchange of keying material during the creation of the IKE tunnel.
6	BNP_VPN(config-isakmp)#**exit**	Done with IKE Policy 1. Exits out of config-isakmp mode.
7	BNP_VPN(config)#**crypto isakmp key 12345 address 63.205.26.67**	Specifies that the mutually authenticating pre-shared secret is "12345", and that the "peer" (i.e., other end gateway for this tunnel) router for the VPN is 63.205.26.67 Note that this command does not enter the user into a new configuration mode, i.e. the router prompt does not change.

Step	NPS BNP_VPN Router Commands	Purpose
8	BNP_VPN(config)#**crypto ipsec transform-set BNPTRANSFORMSET esp-3DES 256 esp-md5-hmac**	Begins the configuration of the Transform Set. In this case, the IPSec transform-set is named "BNPTRANSFORMSET". A transform set consists of a mode, and an encryption and authentication protocol pair. BNPTRANSFORMSET uses ESP mode, with 3DES encryption and MD5 hashing.
9	BNP_VPN(cfg-crypto-trans)#**crypto map BNPCRYPTOMAP 10 ipsec-isakmp**	Notice that the router entered "cfg-crypto-trans" mode. This command creates the crypto map, named "BNPCRYPTOMAP" in this example. Only one crypto-map can be applied to a router interface. In order to differentiate between multiple VPNs emerging from the same router interface, the crypto map sequence number can be varied to create several "crypto map entries". Here, BNPCRYPTOMAP 10 is being built. The "10" is a sequence number, a unique number between 0 and 65535, used to identify specific information for this crypto map and its peer. Each crypto map entry would be used to establish IPSec security associations for a VPN tunnel. It would therefore be possible to build BNPCRYPTOMAP 9, BNPCRYPTOMAP 11, etc. .
10	% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.	Comment produced by the router.
11	BNP_VPN(config-crypto-map)#**set peer 63.205.26.67**	Notice the router entered "config-crypto-map" mode. This command sets the other end of the VPN tunnel for BNPCRYPTOMAP #10 to be 63.205.26.67. Each crypto map entry must have a unique VPN peer.

Step	NPS BNP_VPN Router Commands	Purpose
12	BNP_VPN(config-crypto-map)#**set transform-set BNPTRANSFORMSET**	Specifies the transform set assigned to this crypto map. In this case, the BNPTRANSFORMSET has already been created and the crypto map entry assigned is BNPCRYPTOMAP 10. Only one transform set is allowed per crypto map.
13	BNP_VPN(config-crypto-map)#**match address 110**	The match address command within this crypto map entry points the router at extended Access List 110. An Extended Access List, numbered between 100-199, allows filtering on source address, destination address, and application port number as appropriate. The "match address" command tells the router to treat Access List 110 differently, telling the router which traffic to tunnel. Traffic not mentioned in this ACL will be not be tunneled unless that traffic is named in another crypto map entry.
14	BNP_VPN(config-crypto-map)#**set PFS group2**	(optional) Allows the use of PFS, as discussed in Chapter III.
15	BNP_VPN(config-crypto-map)#**exit**	Exits from configuring the crypto map.
16	BNP_VPN(config)#**interface FastEthernet0/1**	Prepares the router to configure the FastEthernet interface 0/1
17	BNP_VPN(config-if)#**crypto map BNPCRYPTOMAP**	Notice the router entered "config-if" mode. Applies the crypto map to the interface. Now, all traffic that matches the rule 110 that passes through f0/1 will be processed by the VPN crypto engine.
18	BNP_VPN(config-if)#**exit**	Exits from configuring the interface.

Step	NPS BNP_VPN Router Commands	Purpose
19	BNP_VPN(config)#**crypto ipsec security-association lifetime seconds 28800**	Defines the IPSec security lifetime as 28800 seconds (eight hours). The lifetime can be between 120 and 86400 seconds (24 hours). Note that this command does not enter the user into a new configuration mod, i.e. the router prompt does not change.
20	BNP_VPN(config)#**access-list 110 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.0.255**	Defines the Access List already mentioned and matched above. Tells the router to tunnel all traffic going from the BNP_VPN private network (10.1.0.0) to the UofC_VPN private network (192.168.0.0).
21	BNP_VPN(config)#**exit** BNP_VPN#**exit**	Exits out of configuring the router.

Table 14. NPS BNP_VPN Router Commands

Similarly, the U of C router is configured. Commands for the U of C router are listed in Table 15.

```
UofC_VPN>en
UofC_VPN>password
UofC_VPN#config t
UofC_VPN(config)#crypto isakmp policy 1
UofC_VPN(config-isakmp)#encryption 3DES
UofC_VPN(config-isakmp)#authentication pre-share
UofC_VPN(config-isakmp)#group 2
UofC_VPN(config-isakmp)#exit
UofC_VPN(config)#crypto isakmp key 12345 address 131.120.8.199
UofC_VPN(config)#crypto ipsec security-association lifetime seconds 28800
UofC_VPN(config)#crypto ipsec transform-set UOFCTRANSFORMSET esp-3DES 256 esp-md5-hmac
UofC_VPN(cfg-crypto-trans)#crypto map UOFCCRYPTOMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer and a valid access list
have been configured.
UofC_VPN(config-crypto-map)#set peer 131.120.8.199
UofC_VPN(config-crypto-map)#set transform-set UOFCTRANSFORMSET
UofC_VPN(config-crypto-map)#match address 110
UofC_VPN(config-crypto-map)#set PFS group2
UofC_VPN(config-crypto-map)#exit
UofC_VPN(config)#int f0/1
UofC_VPN(config-if)#crypto map UOFCCRYPTOMAP
UofC_VPN(config-if)#exit
UofC_VPN(config)#access-list 110 permit ip 192.168.0.0 0.0.0.255 10.1.1.0 0.0.0.255
UofC_VPN(config)#exit
UofC_VPN#exit
```

Table 15. U of C Router Commands

6. Verification of the VPN Built using CLI

Since both parties of the cyber-exercise will be sending ”attack” and possibly experimental traffic via the VPN over the infrastructure of the Internet, it is worth verifying that the VPN has been built correctly and is indeed sending encrypted packets. To do this, place a hub with a packet sniffer attached to it between the VPN gateway and the internet connection. The program “Ethereal”, available for free from www.ethereal.org, is an excellent program to sniff traffic for this purpose. Since the behavior of a hub is to broadcast all packets received out each port of the hub, the sniffing computer will receive all traffic entering or exiting the VPN gateway and will be able to determine if this traffic is ESP (i.e., VPN-encrypted) traffic.

Shown in Figure 9 is the Ethereal capture of a packet sniffed from between two host computers. The two host computers were not using a VPN, thus the packet was sent in the clear. The packet transferred was a text file that was sent using TFTP. The text file contained the characters “hello040225”. There are two items to note. First, inspection of the packet highlighted on line “40” of the trace, in the column labeled “Protocol”, the reader can see that the packet is a TFTP packet. Second, in the lowest area of the screen, in the characters to the right, one can see the contents of the packet in the clear, i.e. the words “hello040225”. Without a VPN there is no protection for confidentiality of the traffic.

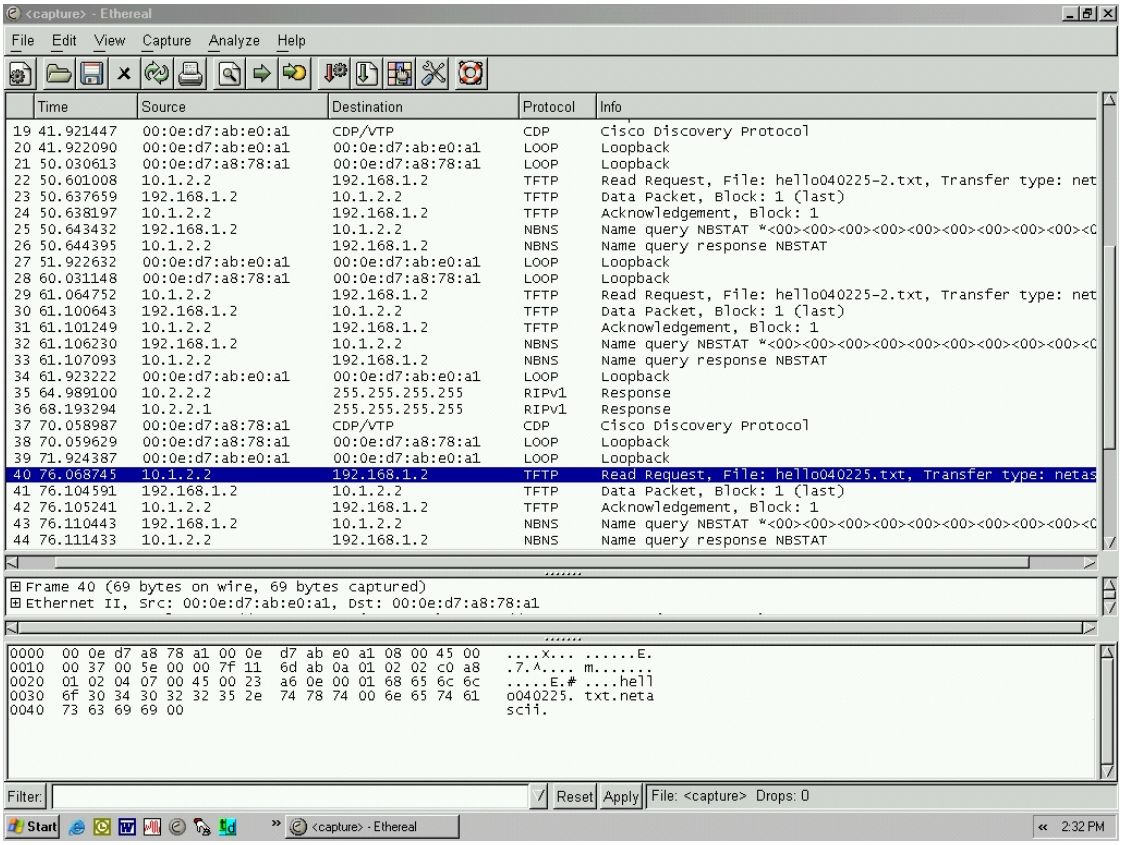

Figure 9. Ethereal Packet Capture in the Clear

Shown in Figure 10 is the Ethereal capture of a packet sniffed from between two host computers. This time, the two host computers were using a VPN employed in ESP mode, thus the packet was sent encrypted. The packet transferred was the same text file as sent previously, again using TFTP. Recall that the text file contained the characters “hello040225”. Making the same observations as above, except this time inspecting the packet highlighted on line “46376”, one can see that in the column labeled “Protocol” the packet is classified as ESP vice TFTP. An observer cannot tell what the actual payload is, only that it is being sent in a VPN using the ESP protocol. As further evidence of the “privacy” afforded by a VPN, in the lowest area of the screen, in the payload decoded characters to the right, one can see that the contents of

the transferred file ("hello040225") are no longer legible as plaintext.

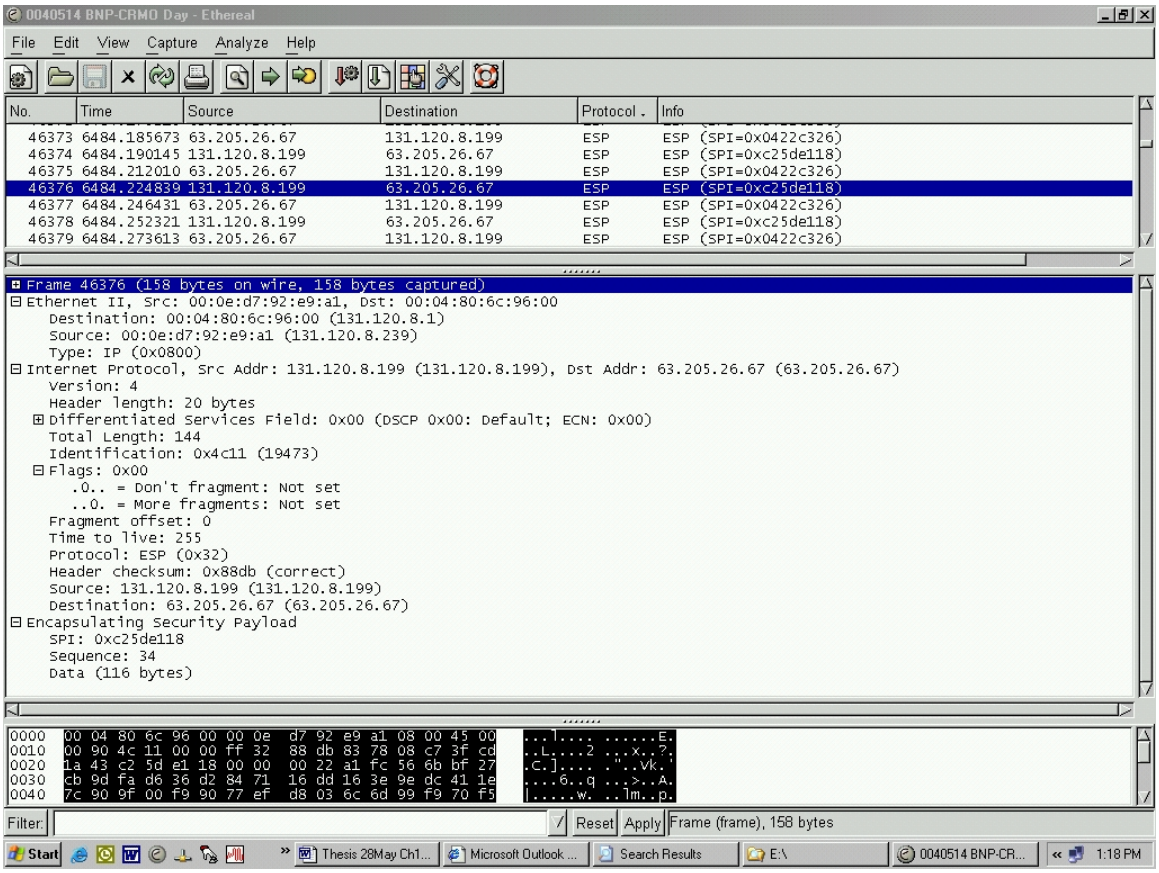

Figure 10. Ethereal Packet Capture with VPN

B. ROUTER TO ROUTER USING SECURITY DEVICE MANAGER

As previously mentioned, an alternative to the CLI configuration of VPN functionality on the routers is to utilize the security device manager (SDM) on routers that have it installed.

1. Verifying and Enabling SDM

The Cisco SDM is a graphical user interface (GUI) that enables the user to configure the router visually rather than through a series of commands. The SDM may or may not be supported on a device. The Cisco document "Release Notes for SDM Version 1.0" gives a list of which router and IOSs support SDM. To determine if a router has SDM functionality, enter the "dir" command from the privileged exec mode as shown in Table 16.

```
BNP_VPN>en
Password: myPassword
BNP_VPN#dir
```

Table 16. Determine Router SDM Functionality

Routers configured with SDM will show the SDM files in Flash memory depicted in Table 17.

```
Directory of flash:/
    1  -rw-    21959780        <no date>  c2600-jk9o3s-mz.122-15.ZJ3.bin
    2  -rw-         940        <no date>  sdmconfig-26xx.cfg
    3  -rw-       14617        <no date>  sdm.shtml
    4  -rw-     2617856        <no date>  sdm.tar
    5  -rw-        1446        <no date>  home.html
    6  -rw-      214016        <no date>  home.tar
```

Table 17. Router SDM Configuration

In order to use the SDM functionality, it must first be enabled via the CLI. After the basic configuration of the router (see Chap. 5, Sec. B.2), input the following additional commands in Table 18 to enable the SDM web browser interface:

```
BNP_VPN(config)#ip http secure-server
BNP_VPN(config)#ip http authentication local
BNP_VPN(config)#username BNP_VPN privilege 15 password 0 mypassword
```

Table 18. Enabling SDM Browser Interface

These further commands shown in Table 19 will allow access to the configurations screens of the SDM.

```
BNP_VPN(config)#line vty 0 4
BNP_VPN(config-line)#privilege level 15
BNP_VPN(config-line)#login local
BNP_VPN(config-line)#transport input telnet ssh
```

Table 19. Commands to Enable Access to the Router SDM

2. Logging in and Configuring SDM

In order to log into the NPS BNP SDM, the host computer must be configured with an IP address that puts it on the same network as the router's private interface. In this example, a cyber-exercise network computer is used to configure the NPS BNP VPN router via the SDM. The computer already has its IP address statically assigned to 10.1.1.5.

Log into the SDM via a web browser. Since https (i.e., secure http) was enabled, in this example, the address used is:

https://10.1.1.1

This results in the main SDM window is shown in Figure 11.

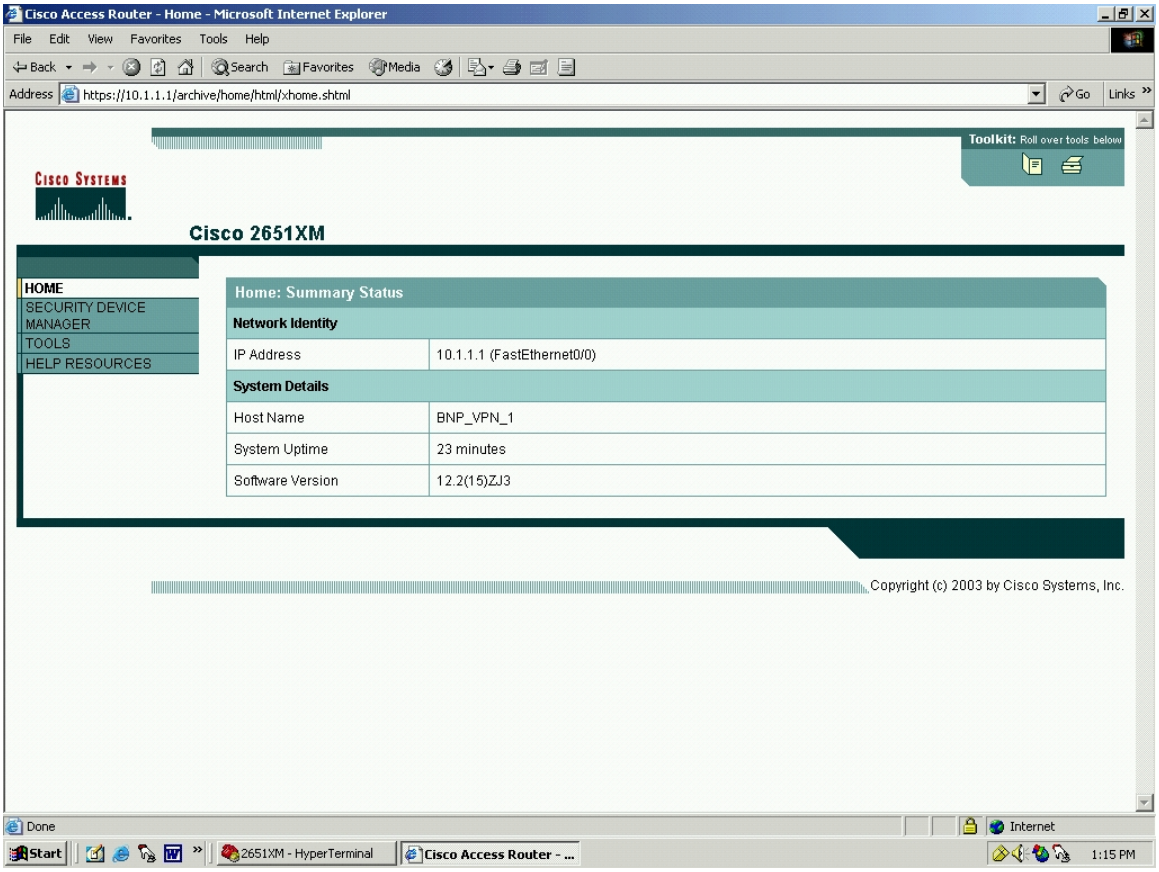

Figure 11. Cisco Security Device Manager (SDM)

Click on the “Security Device Manager” link. This will start the identification and authentication process for logging into the SDM. A pop-up window will appear, Figure 12, asking for a username/password.

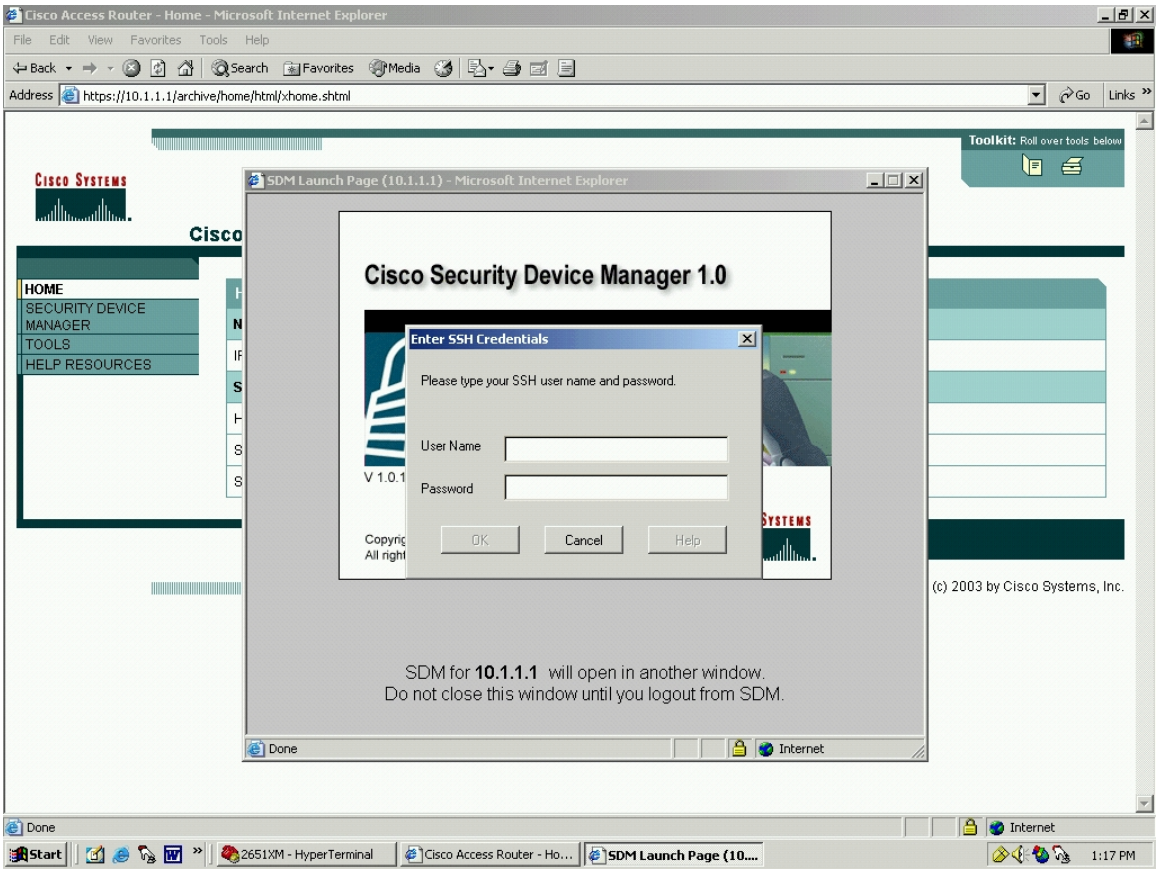

Figure 12. Cisco SDM Login

This is the username and password that was entered in the command:

username BNP_VPNprivilege 15 password 0 mypassword

Once access to the SDM is gained, the following steps will build the VPN.

First, build the IKE in the pop-up window shown in Figure 13.

From the SDM, select “Advanced Mode”, “VPN”, and under directory tree “VPN”, select “IKE”, select “IKE Policies” and click the “Add”. For this example, enter:

Priority: 1

Encryption: 3DES

Hash: SHA_1

Authentication: PRE_SHARE

D-H Group: group2

Life Time: 24h 0min 0sec

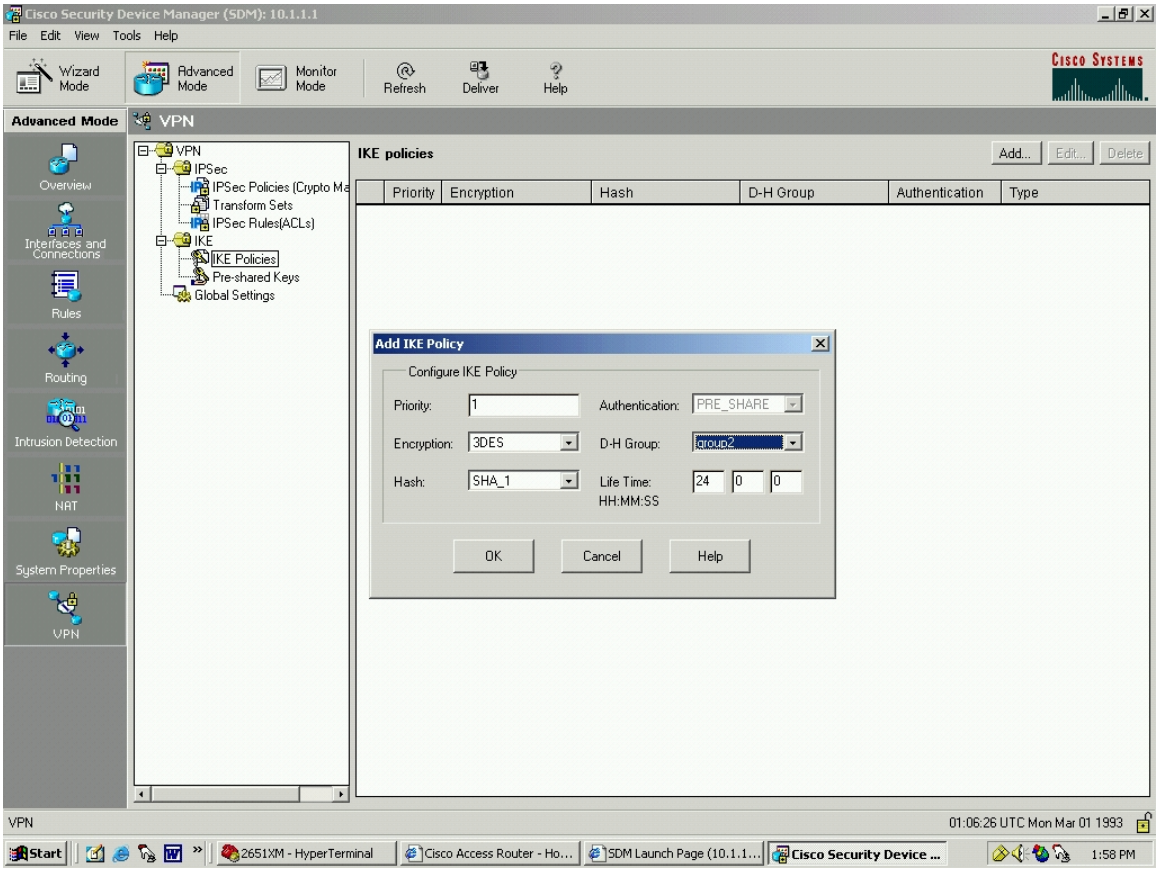

Figure 13. SDM Add the IKE Policy

Click “OK”.

The resulting screen is shown in Figure 14.

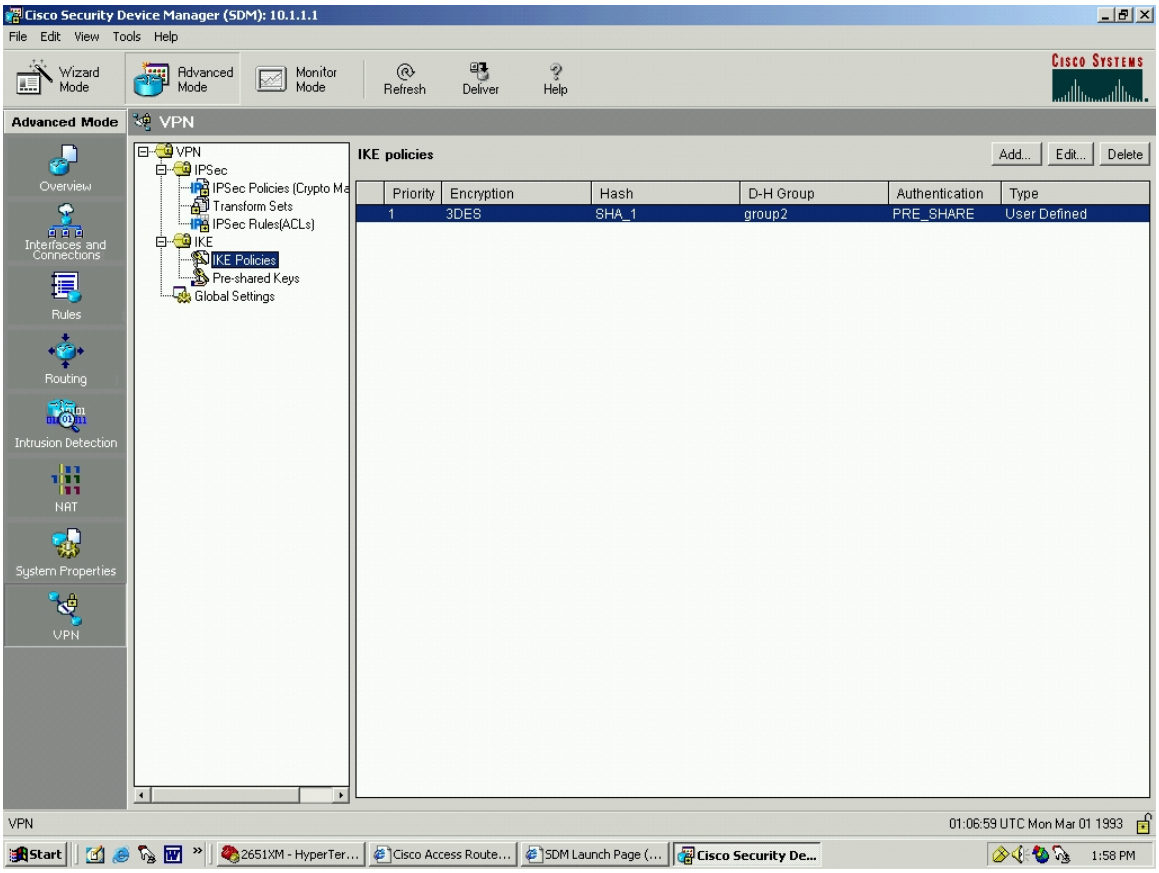

Figure 14. SDM IKE Policy Added

Now enter the pre-shared keys. From the SDM, select "Advanced Mode", "VPN", and under directory tree "VPN", select "IKE", select "Pre-shared Keys" and click the "Add". Note the SDM will eventually show the user what CLI text entries would need to be made if the router were being configured via the CLI. This makes it particularly convenient if one router is being configured via SDM and the other peer router does not have SDM but must rely on configuration from the CLI. Therefore in this example, the names are purposefully chosen to be descriptive so that later it will be easier to see how each entry in the SDM box relates to its corresponding CLI command.)

For this example, in the window in Figure 15, enter:

Key: SecretVPNKey#1

Re-enter Key: SecretVPNKey#1

Host/Network

Type: IP Address

IP Address: 65.205.26.67

Subnet Mask: 255.255.255.224 / 27

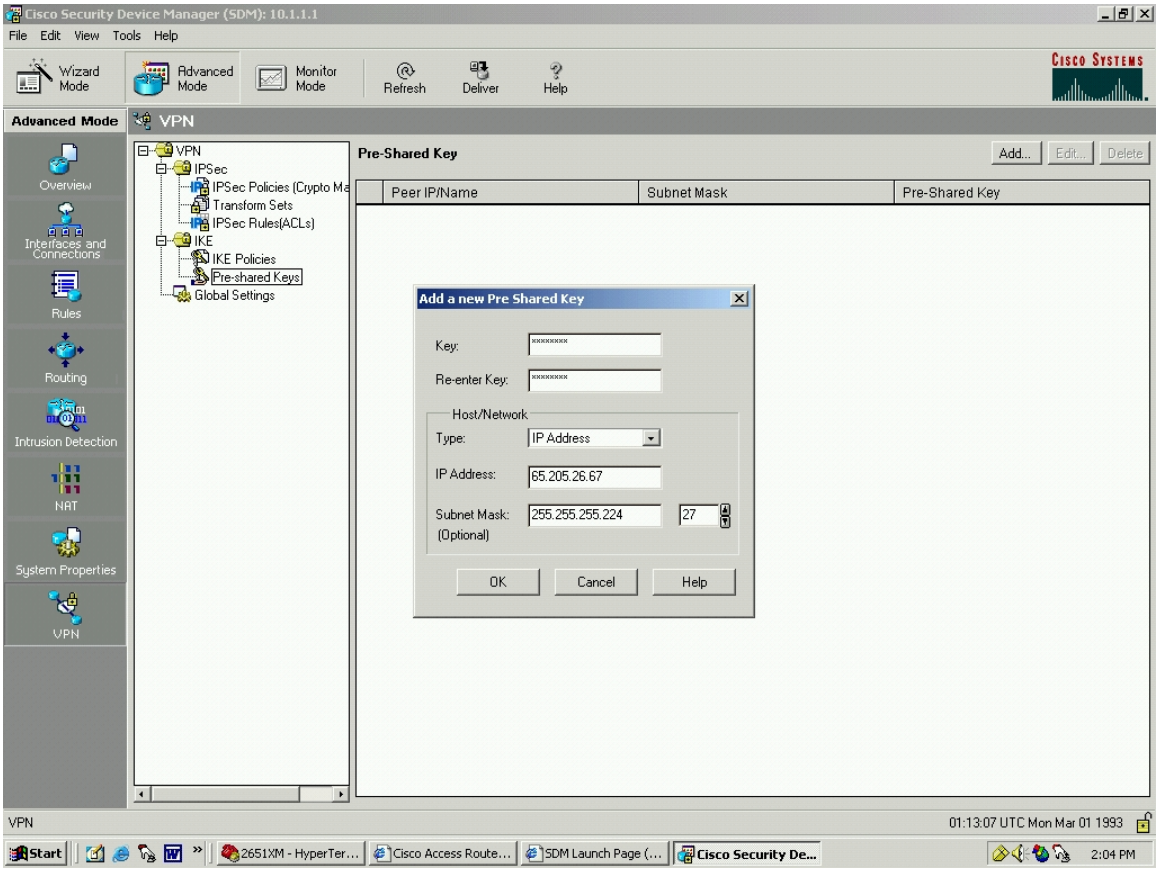

Figure 15. SDM Input the Pre-Shared Key

Click “OK”.

The resulting screen is shown in Figure 16.

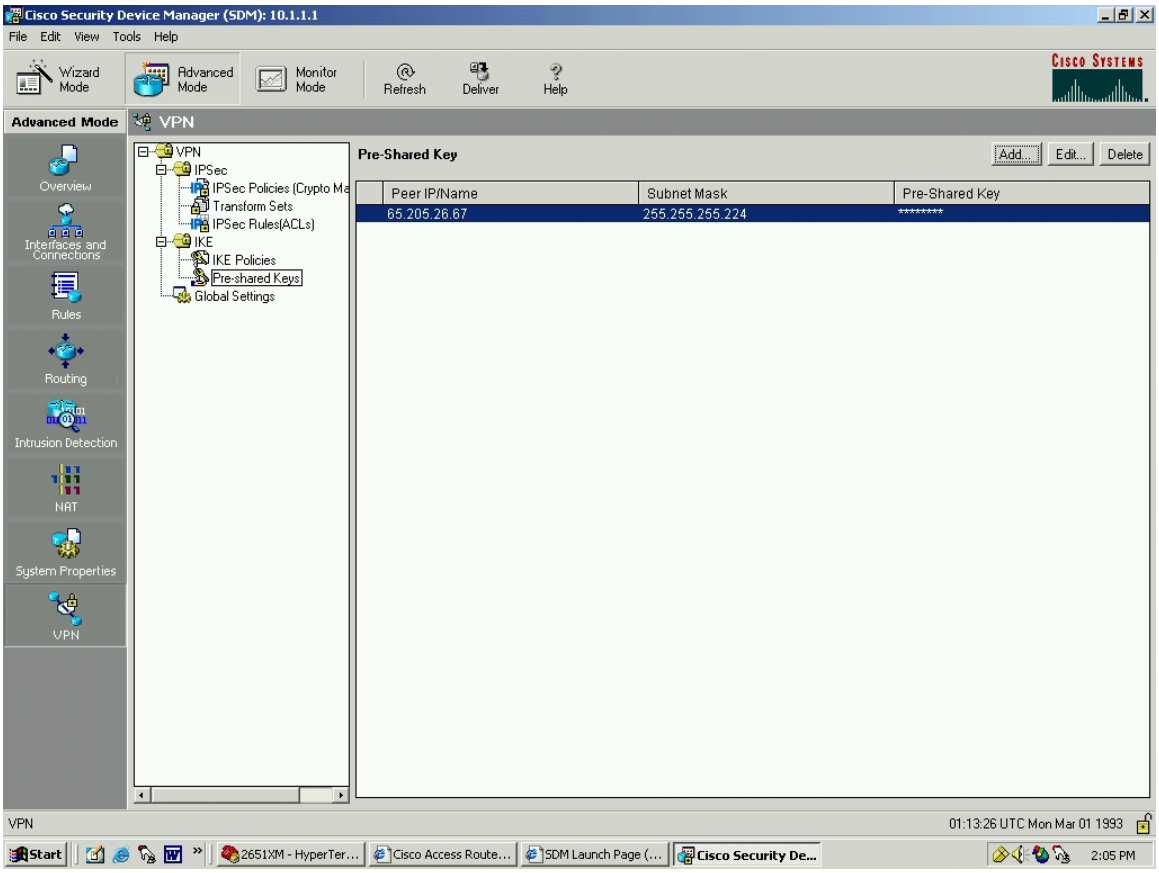

Figure 16. SDM Pre-Shared Key Complete

Next, it is necessary to build the VPN connection. This is best done by assembling each component first. The components the SDM provides are IPSec Policies, Transform Sets, and IPSec Rules. Then the user is able to select the components into the final VPN Connection, by expanding the "VPN" icon at the top of the menu tree.

First, build the IPSec Rule using an Access Control List (ACL). From the SDM, select "Advanced Mode", "VPN", and under directory tree "VPN", select "IPSec", select "IPSec Rules" (ACLs) and click the "Add". An Extended Rule is being built, Figure 17. It can have an alphanumeric name.

Name/Number: 115

Description: BNP_VPNDescription

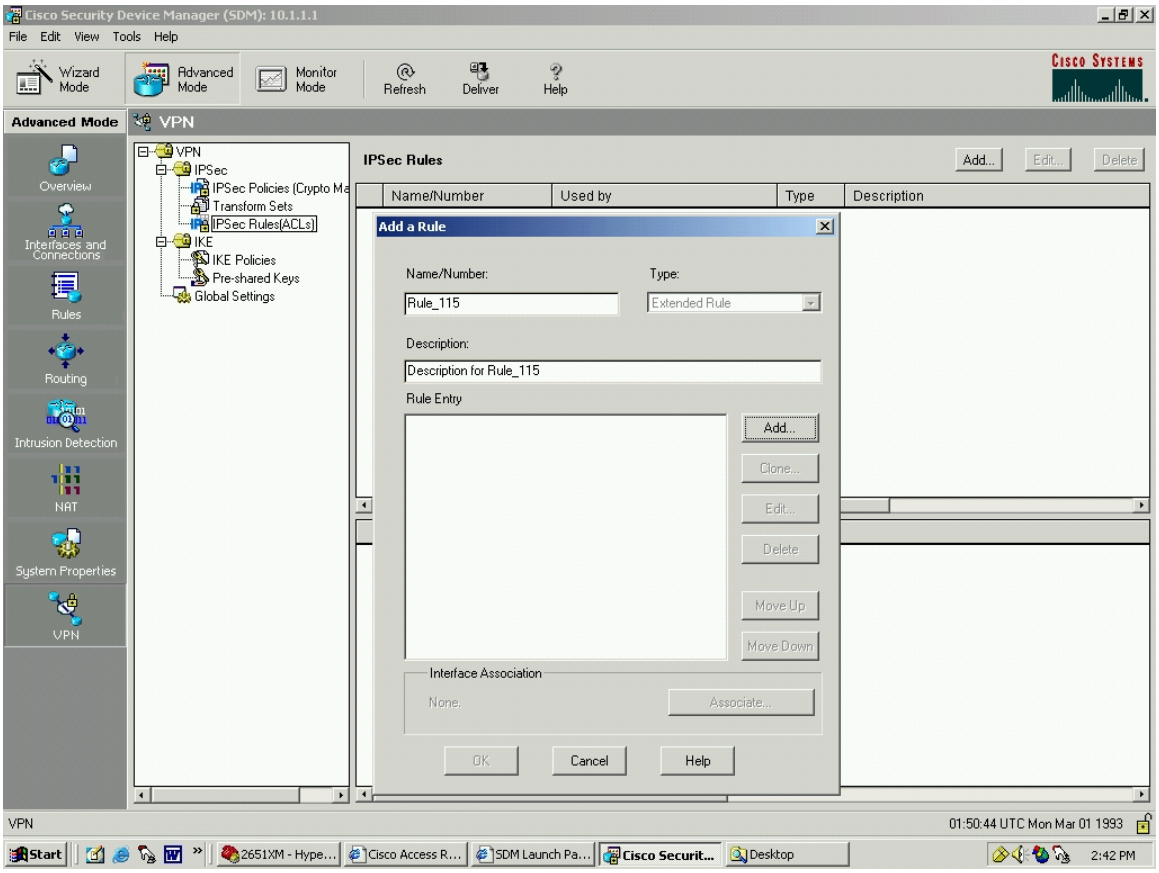

Figure 17. SDM Add an ACL Rule

Click “Add”

This brings up an “Add an Extended Rule Entry” screen, Figure 18. Enter:

Select an action: Protect the Traffic

Description: Extended Rule Description

Source Host/Network

Type: A Network

IP Address: 10.1.0.0

Wildcard Mask: 0.0.255.255

Destination Host/Network

Type: A Network

IP Address: 192.168.0.0

Wildcard Mask: 0.0.0.255

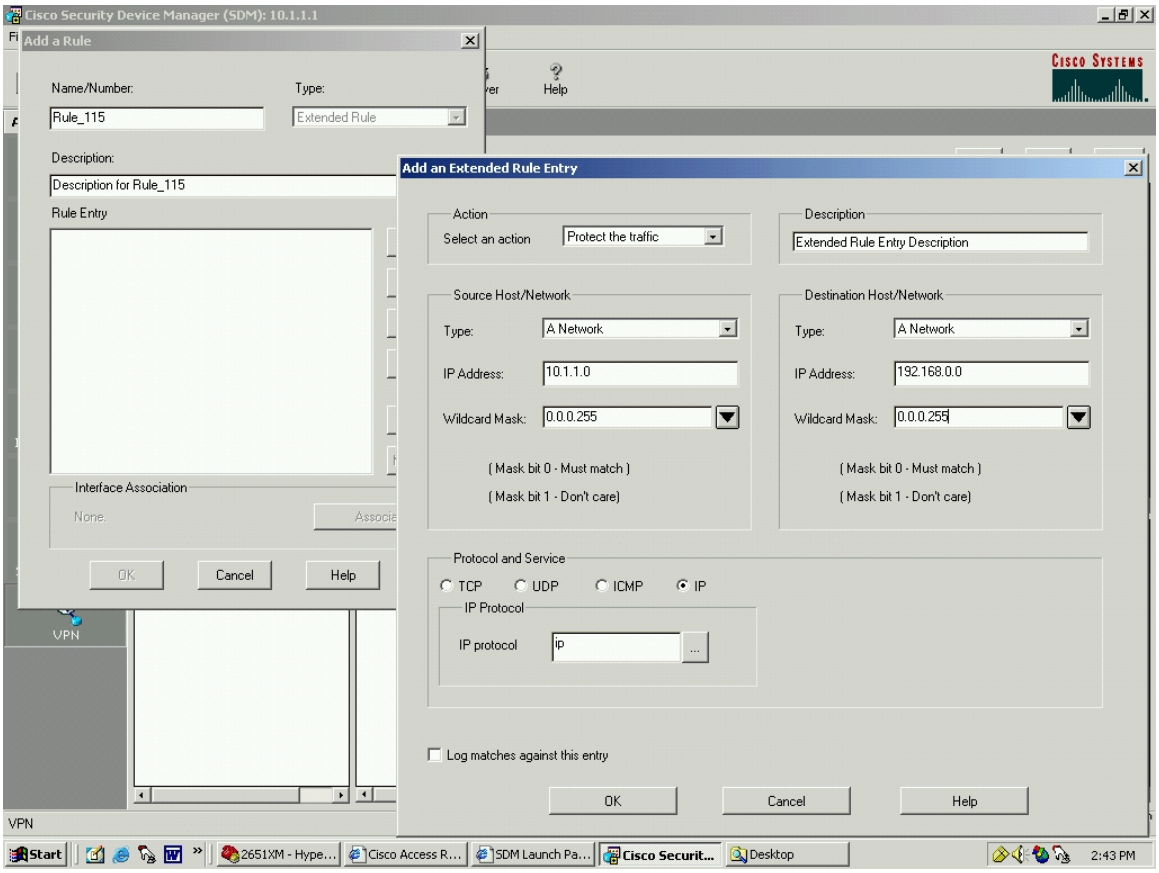

Figure 18. SDM ACL Rule Entry

Click “OK”. This results in the information being loaded back into the previous screen, as shown in Figure 19.

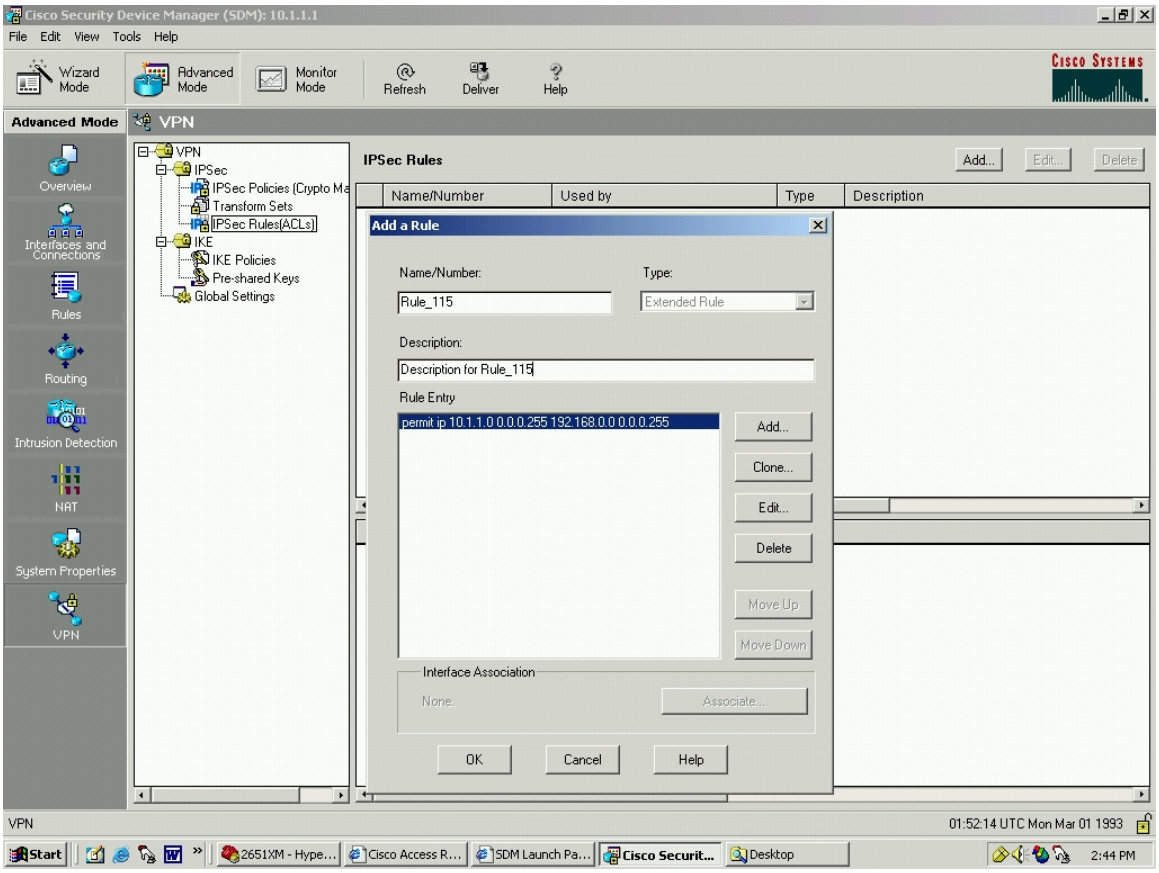

Figure 19. SDM Rule Added Complete

Click “OK”. Rule_115 is added, as shown in Figure 20.

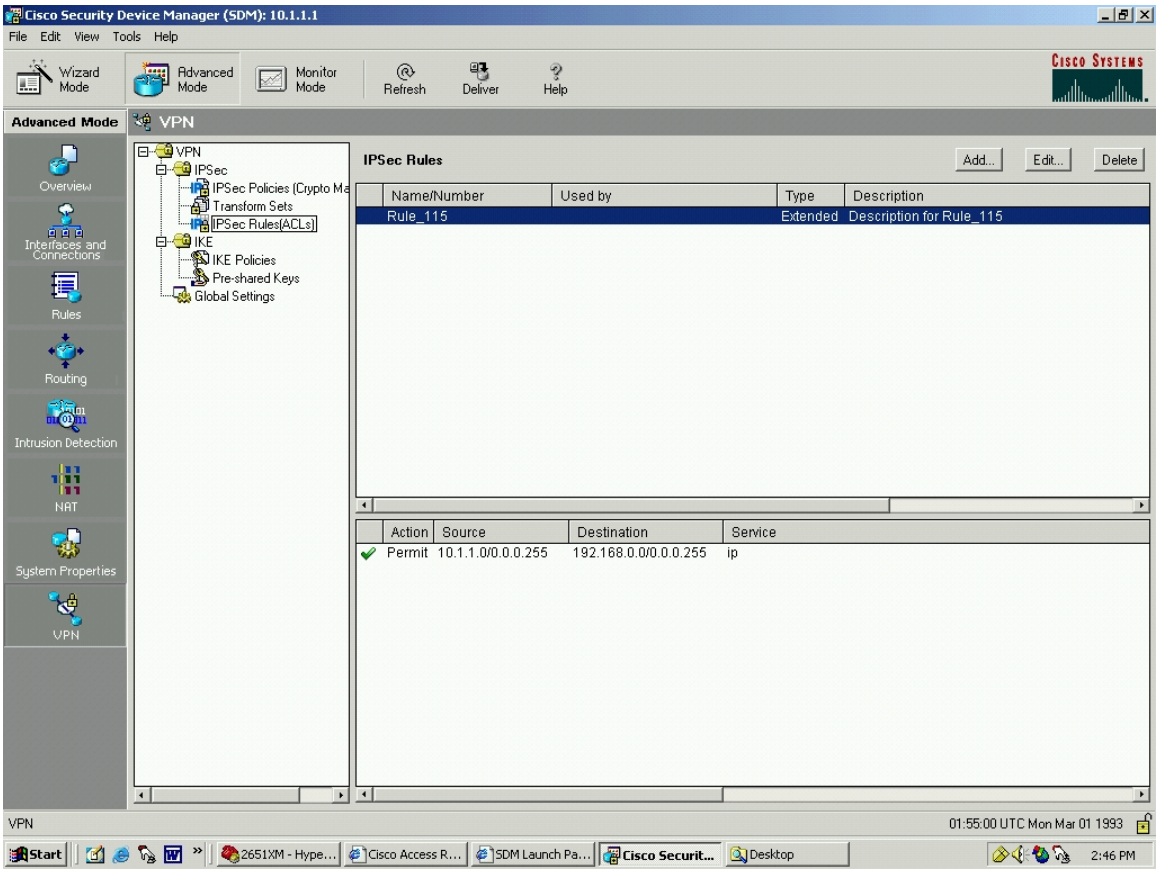

Figure 20. SDM IPSec Rule Complete

Now build a Transform Set.

From the SDM, select “Advanced Mode”, “VPN”, and under directory tree “VPN”, select “IPSec”, select “Transform Sets” and click the “Add”. In the window that appears, Figure 21, click the “Show Advanced”. Enter:

Name: BNP_VPN_Transform_Set_1

Data integrity and encryption (ESP): checked

Integrity Algorithm: ESP_SHA_HMAC

Encryption Algorithm: ESP_3DES

Since this VPN uses ESP, leave the "Data and address integrity without encryption (AH)" box unchecked. (It is an either/or consideration.)

Mode: Tunnel (Encrypt data and IP header)

IP Compression (COMP-LZS): leave unchecked

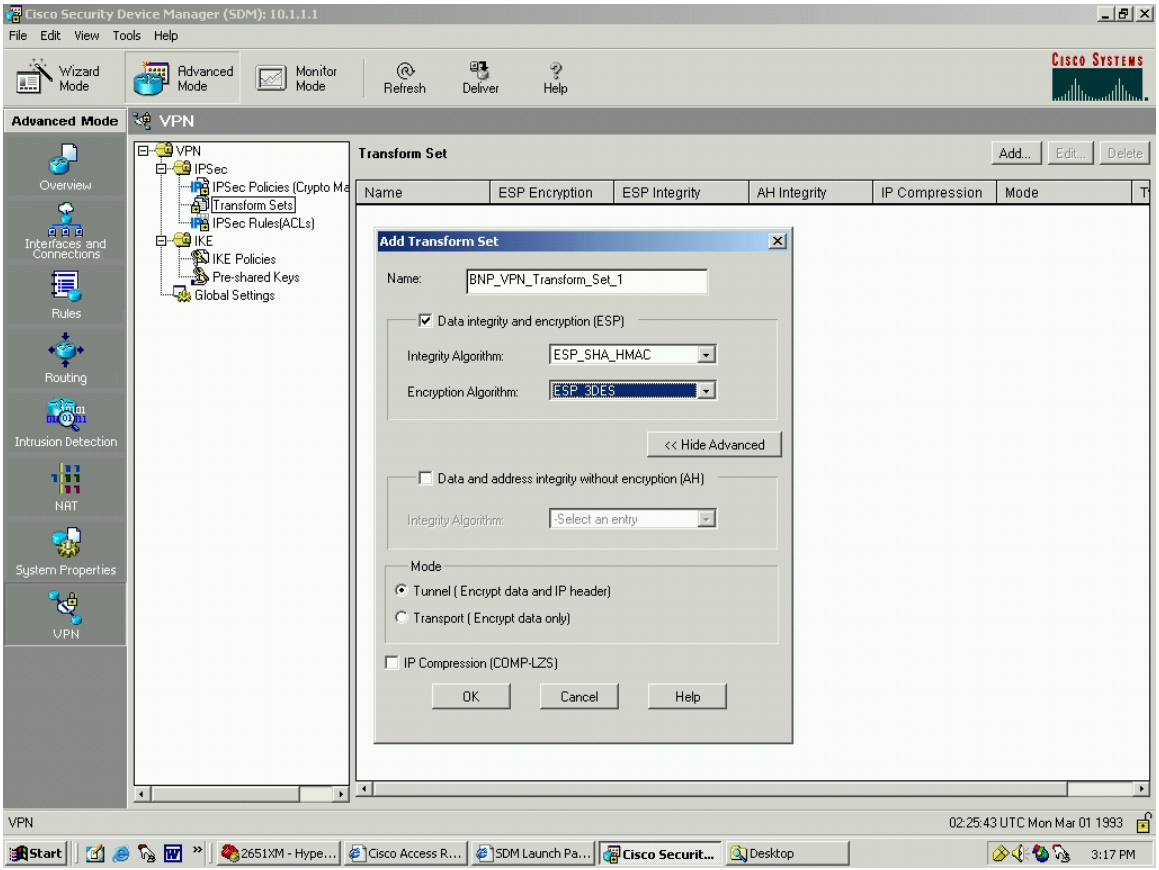

Figure 21. SDM Add a Transform Set

Click "Add". The result is shown in Figure 22.

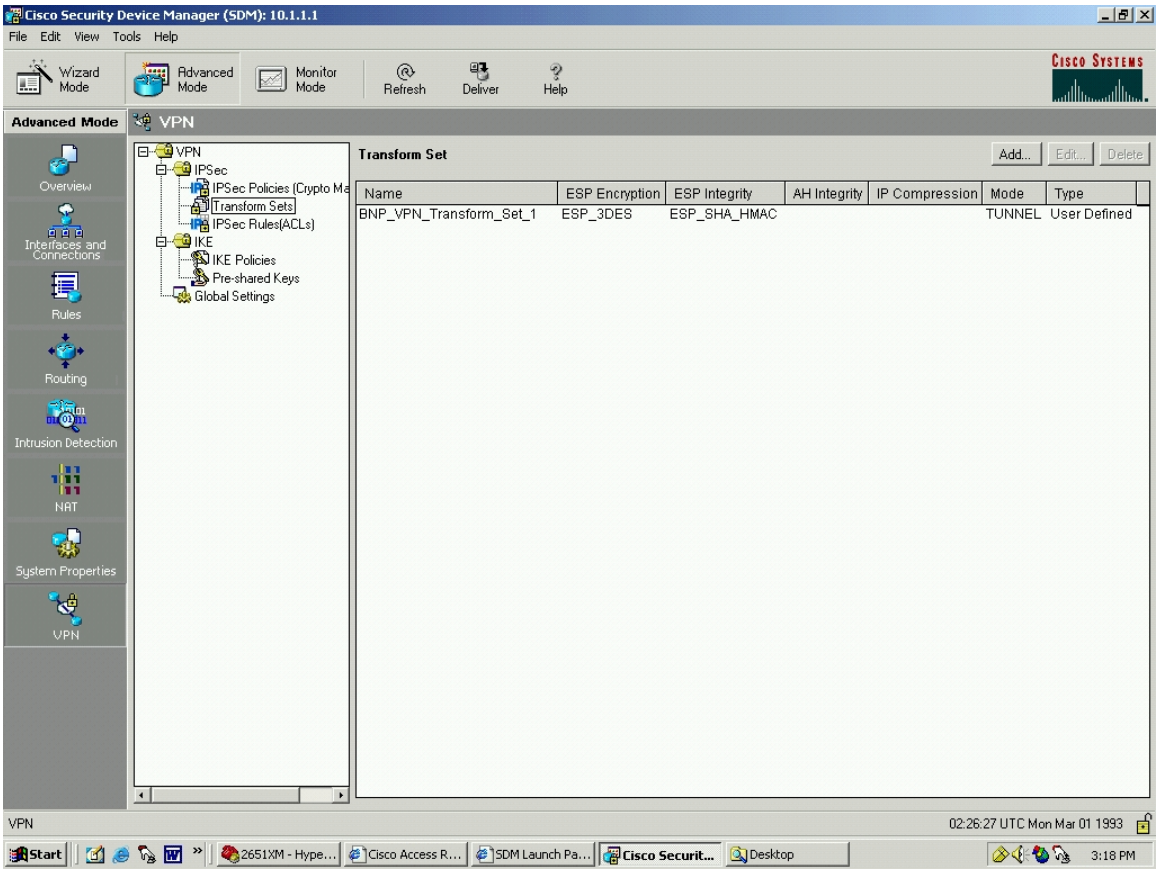

Figure 22. SDM Transform Set Added Complete

Now it is time to add IPSec Policies (Crypto Maps). Completing the other steps first will allow the selection of a Transform Set and an IPSec Rule (ACL) during this step. From the SDM, select “Advanced Mode”, “VPN”, and under directory tree “VPN”, select “IPSec”, select “IPSec Policies (Crypto Maps)” and click the “Add”. The input screen is shown in Figure 23. Enter the name.

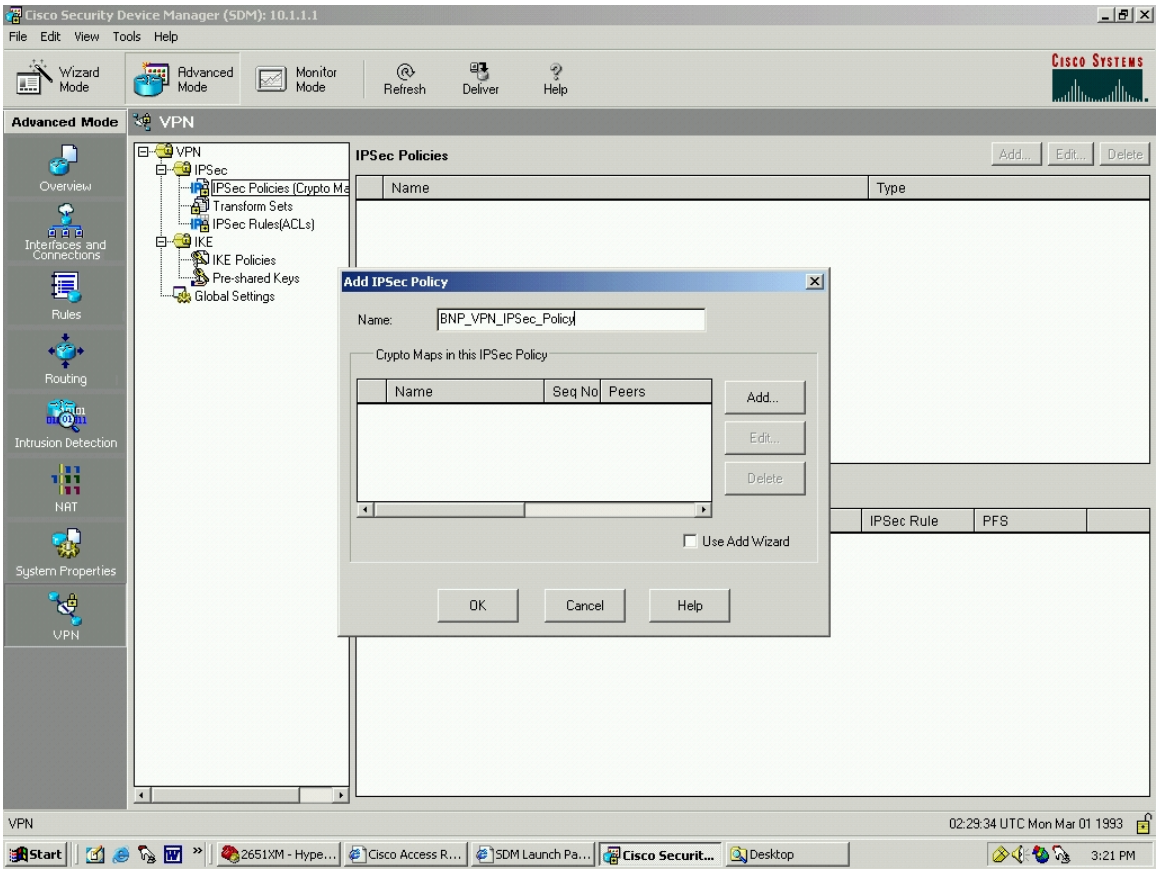

Figure 23. SDM Add IPSec Policy

Click “Add” and this brings up an “Add Crypto Map” screen with four folders, “General”, “Peer Information”, “Transform Sets”, and “IPSec Rule”, as shown in Figure 24.

The first folder is “General”. The Name of IPSec Policy is already entered and grayed out.

Description: BNP_VPN_IPSec_Policy Description

Sequence Number: 1

Security Association Lifetime:

Kilobytes: 4608000

HH:MM:SS: 24 0 0

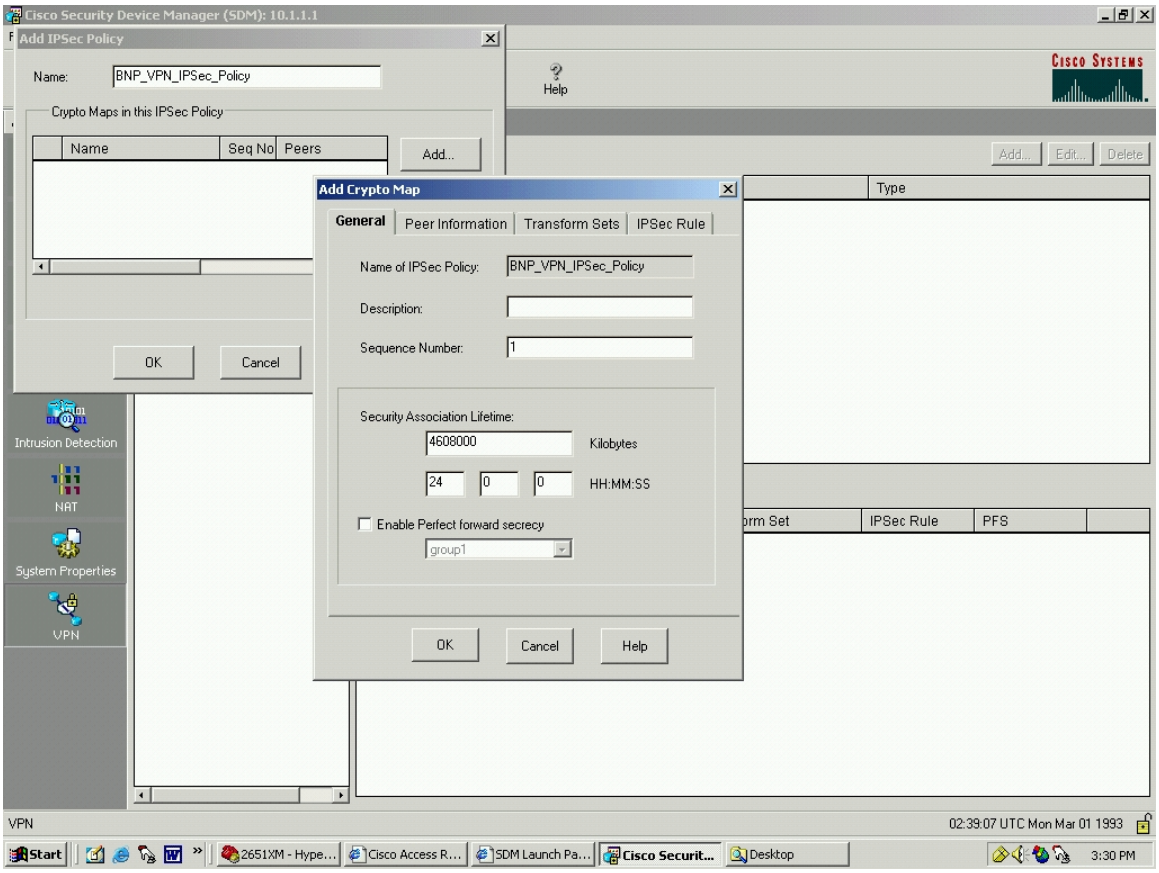

Figure 24. SDM Add Crypto Map: General Tab

It is on this screen, Figure 25, that a user can enable PFS, as discussed in Chapter III.

From here, click the next folder, “Peer Information”. Input the IP address of the peer network (or hostname) and click “Add” to move it to the “Current List”.

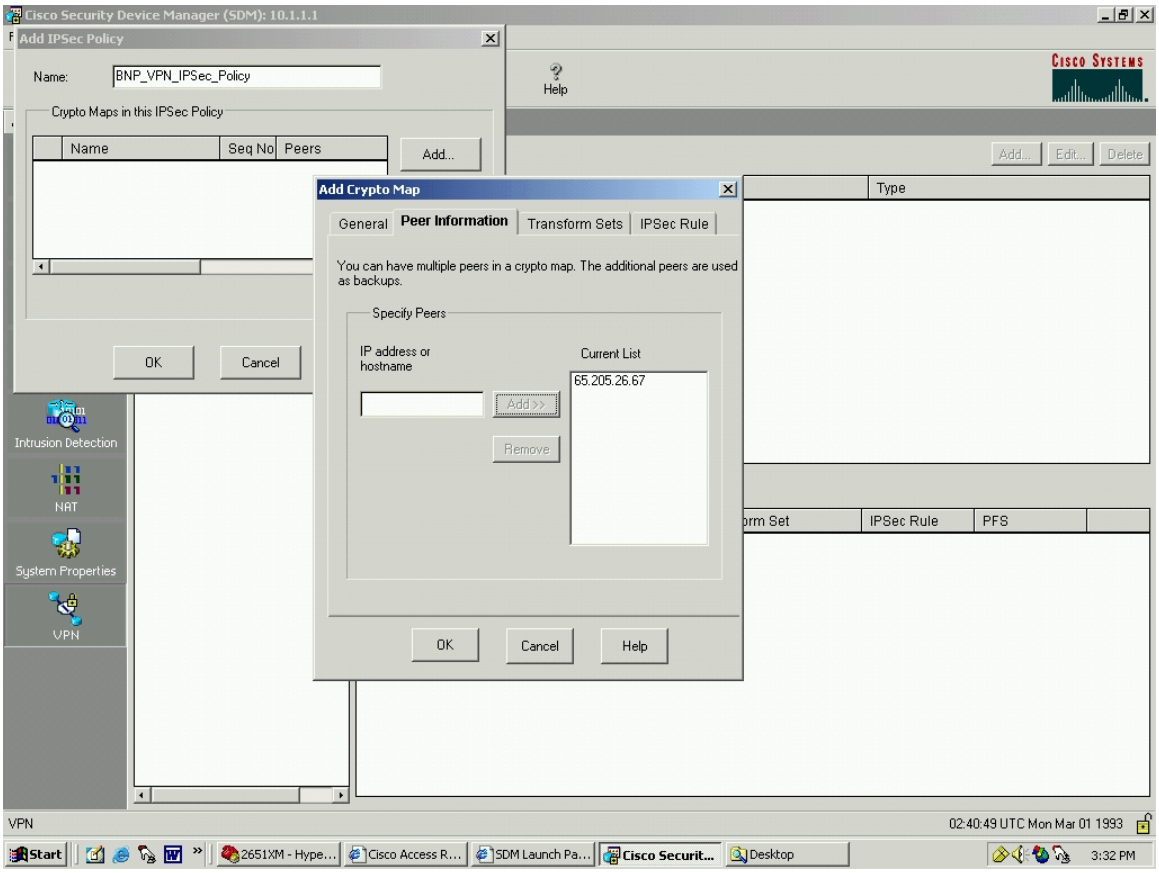

Figure 25. SDM Add Crypto Map: Peer Information

From here, click the next folder, “Transform Sets”. Since a Transform Set was already built, choose “BNP_VPN_Transform_Set_1” from the “Available Transform Sets” and click the “>>” button to move it to the “Selected Transform Sets” (Preference Order), Figure 26.

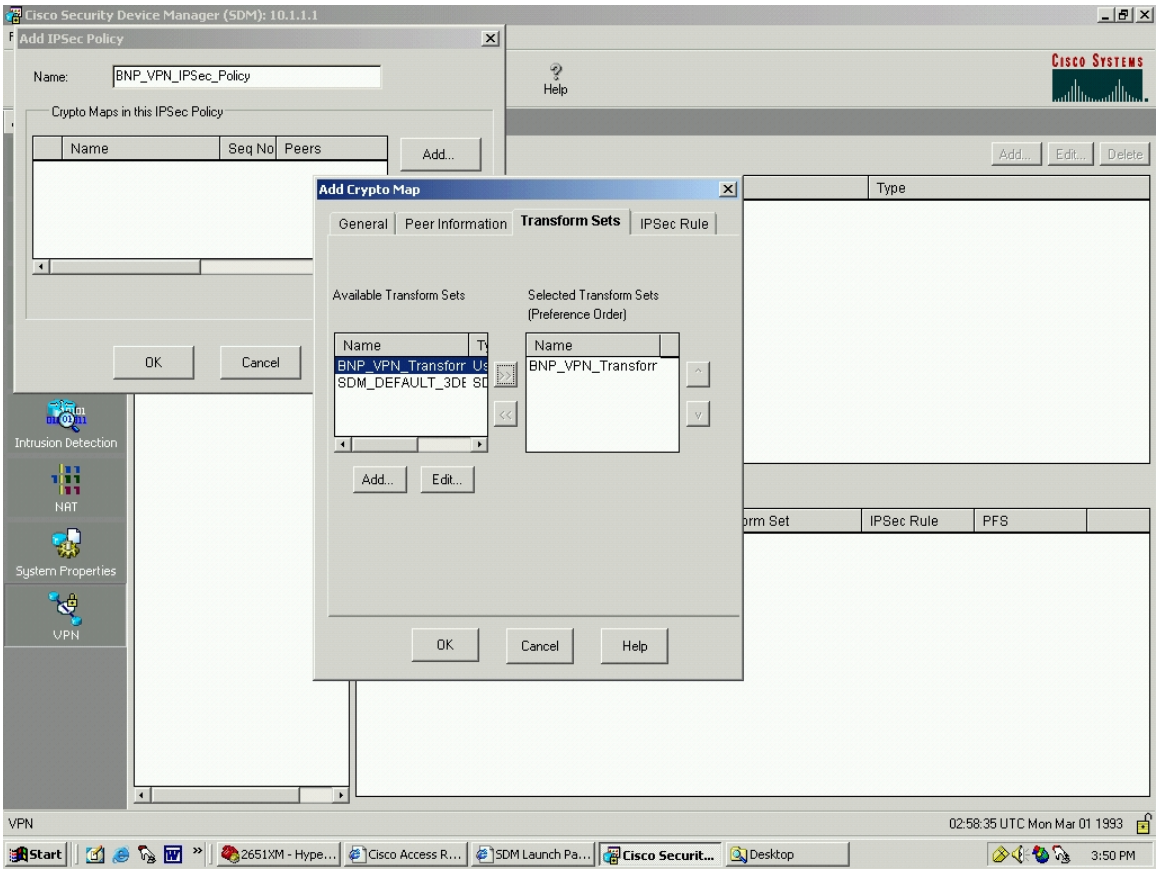

Figure 26. SDM Add Crypto Map: Transform Set

It is possible to hit the “Add” button and go through the same steps as was completed above in “Transform Sets”

From here, click the next folder, “IPSec Rule”. Similar to “Transform Sets”, an appropriate IPSec Rule for this example was already built. Click the box with the down arrow in it, resulting in Figure 27.

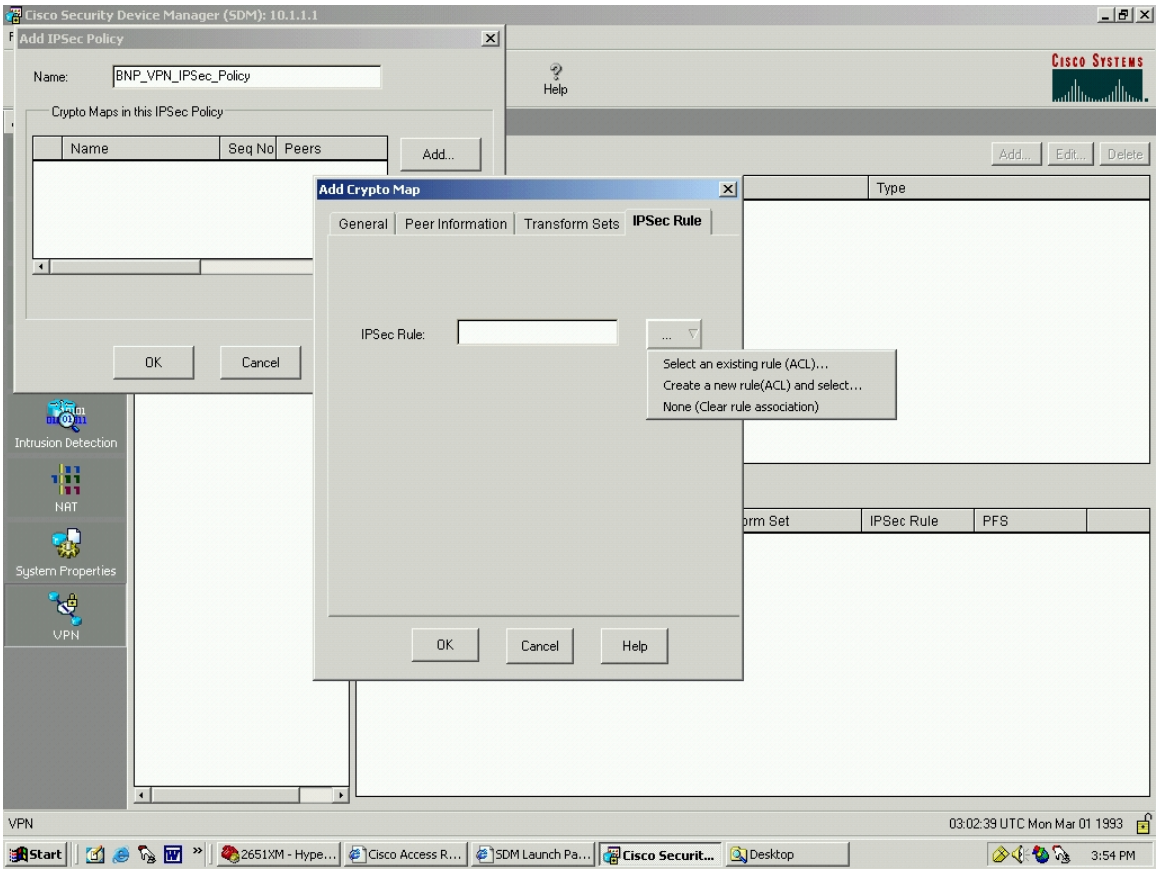

Figure 27. SDM Add Crypto Map: IPSec Rule

Click “Select an Existing Rule”. As shown in Figure 28, pick “Rule_115”:

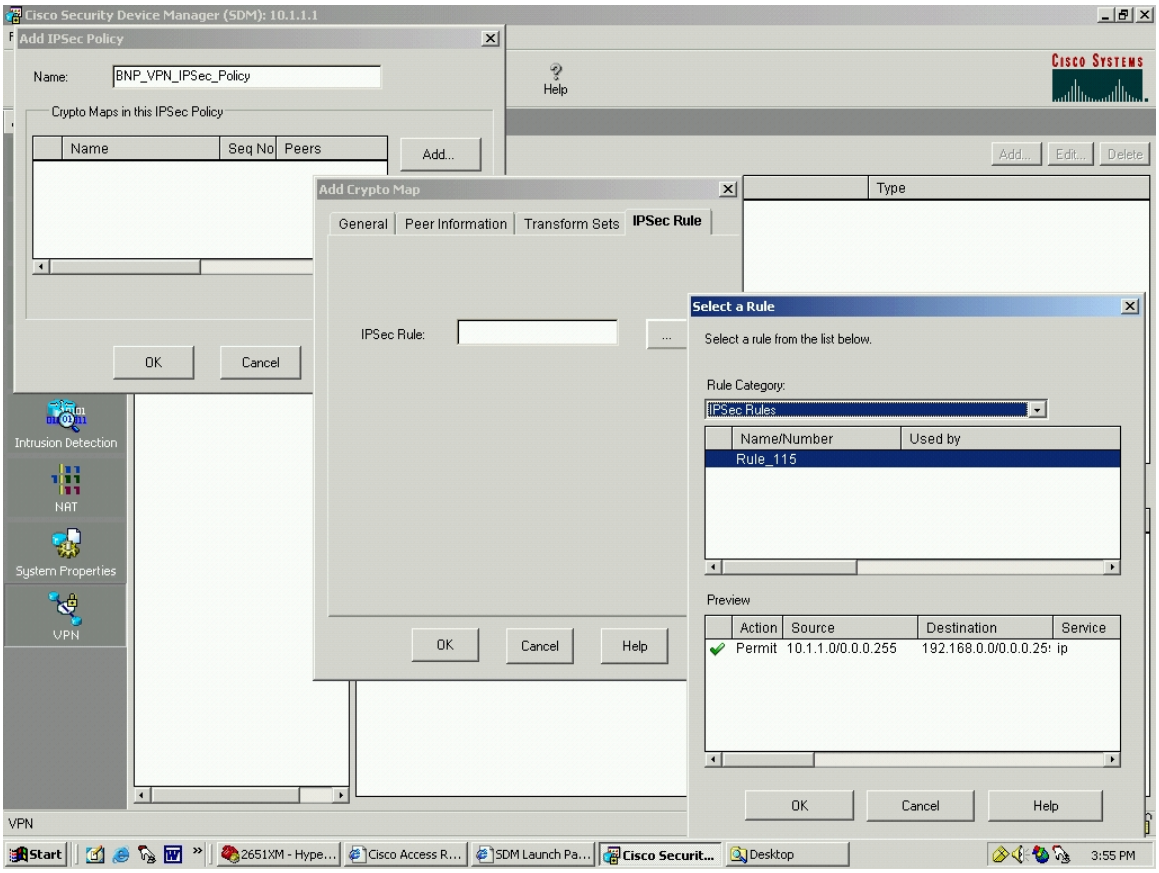

Figure 28. SDM IPSec Rule: Select a Rule

Click “OK”.

Now all folders in the “Add Crypto Map” section have been properly filled in, as depicted in Figure 29.

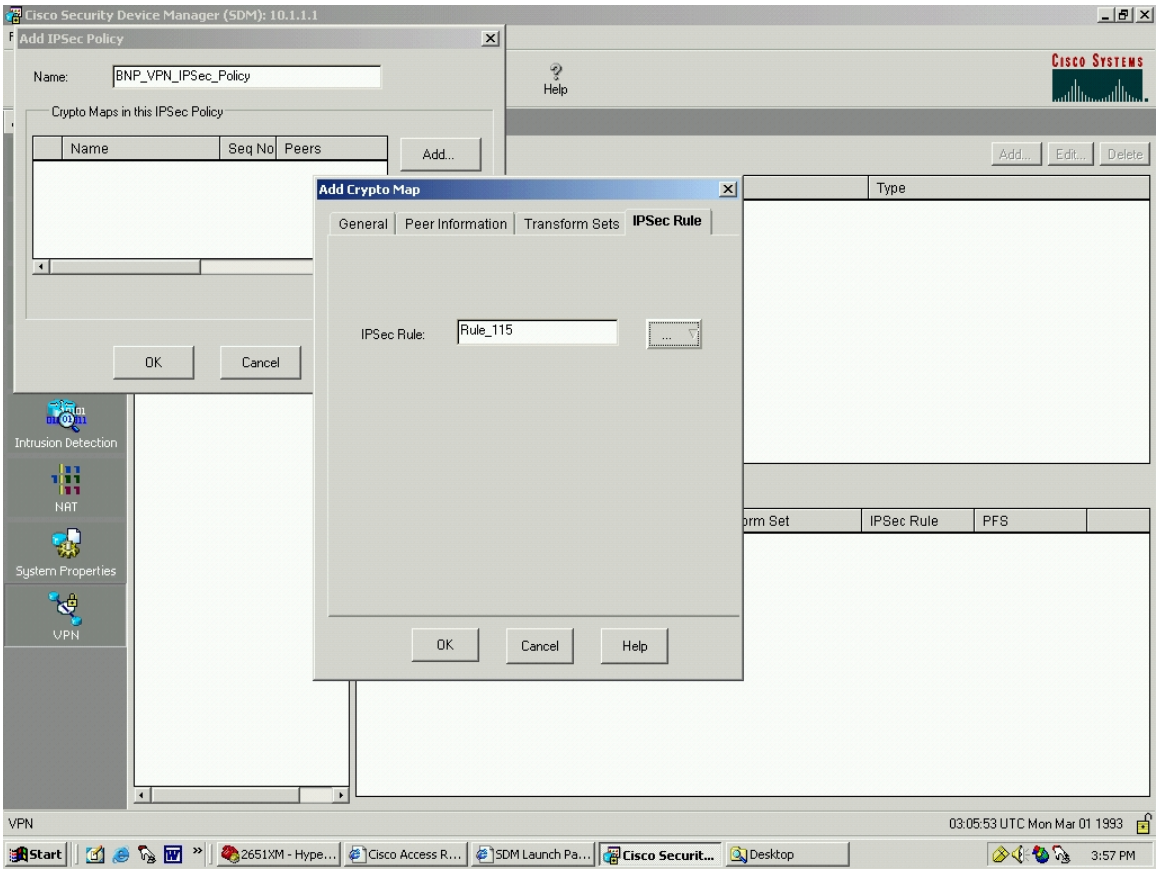

Figure 29. SDM Add Crypto Map: Rule Added

Click “OK”. This inputs the selections just made into the “Crypto Maps in this IPSec Policy” window, as shown in Figure 30.

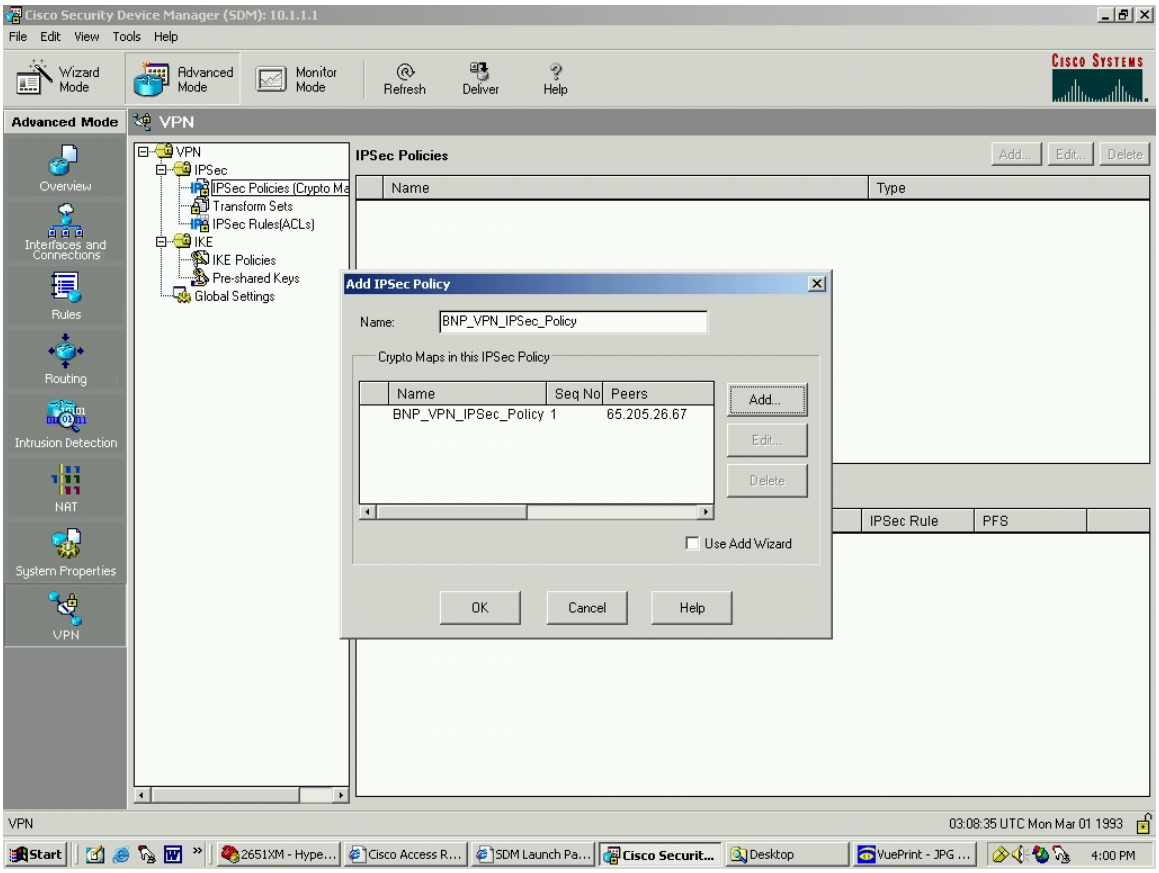

Figure 30. SDM IPSec Policy Added

Click “OK”. This adds the IPSec Policy to the Main Window, as shown in Figure 31.

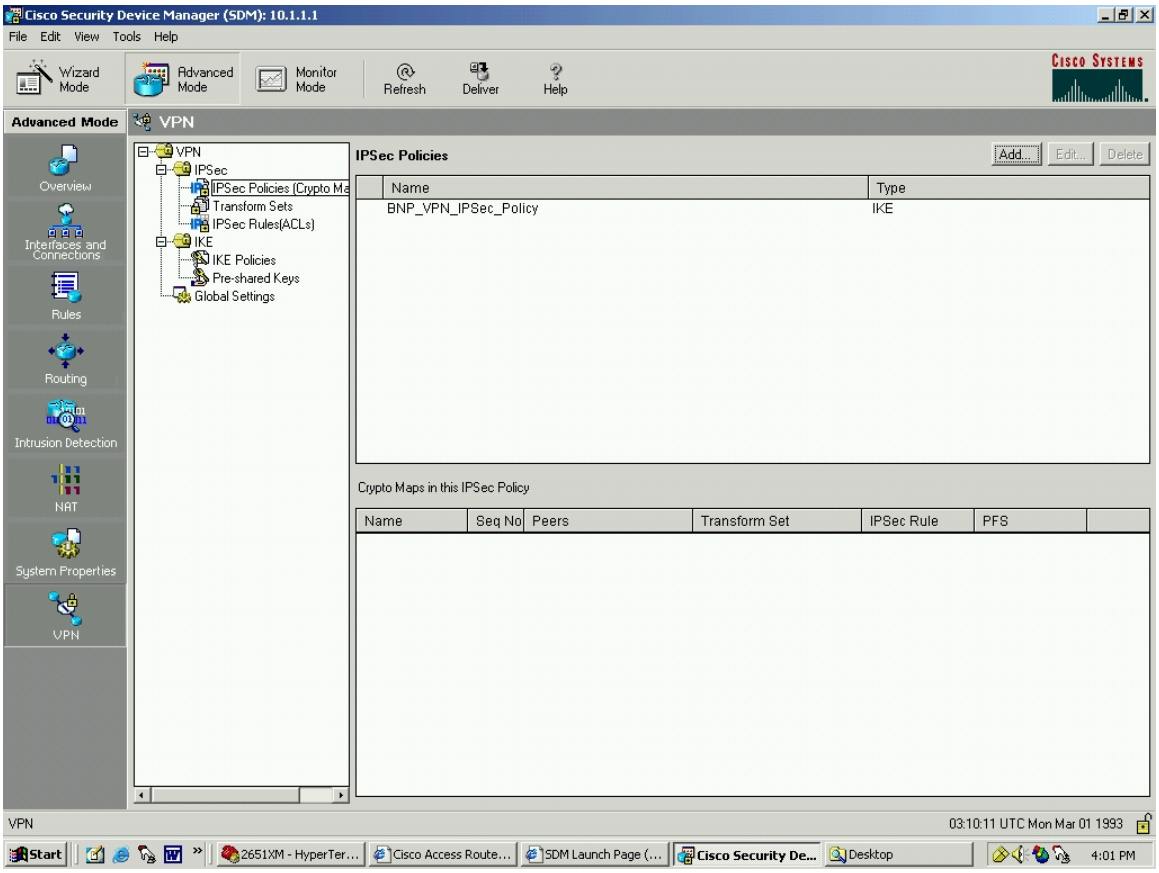

Figure 31. SDM IPSec Policy (Crypto Map) Complete

Finally, combine all these items, i.e. IPSec Policy, Transform Sets, and IPSec Rules (ACLs), into a VPN Connection. From the SDM, select “Advanced Mode”, “VPN”, and click “Add” and select “New VPN Connection”. The resulting screen is shown in Figure 32.

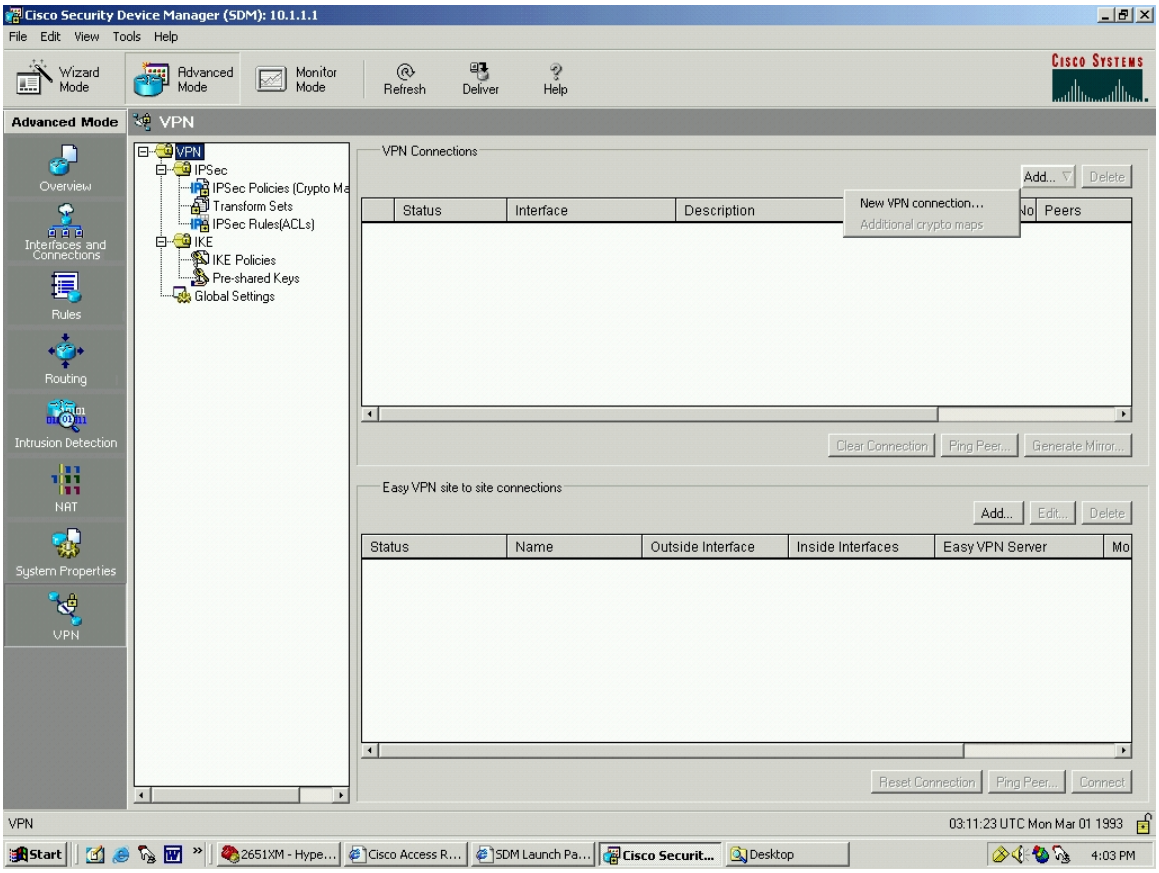

Figure 32. SDM Add New VPN Connection

Select Interface: FastEthernet0/1

Choose IPSec Policy: BNP_VPN_IPSec_Policy

This adds the policy to the lower dark gray window, as shown in Figure 33.

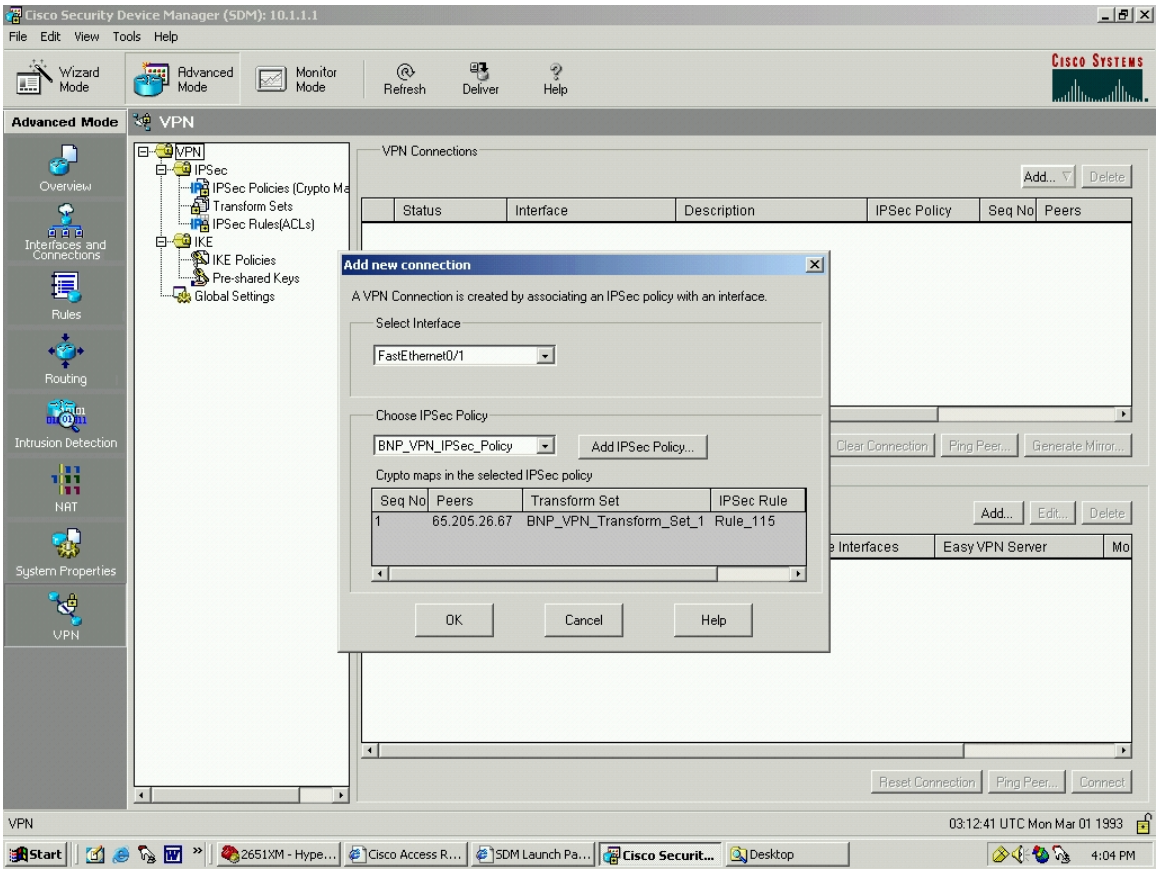

Figure 33. SDM Add New Connection: Interface and Policy

Click “OK” and this adds the new VPN Connection to the VPN Connections Window, as shown in Figure 34.

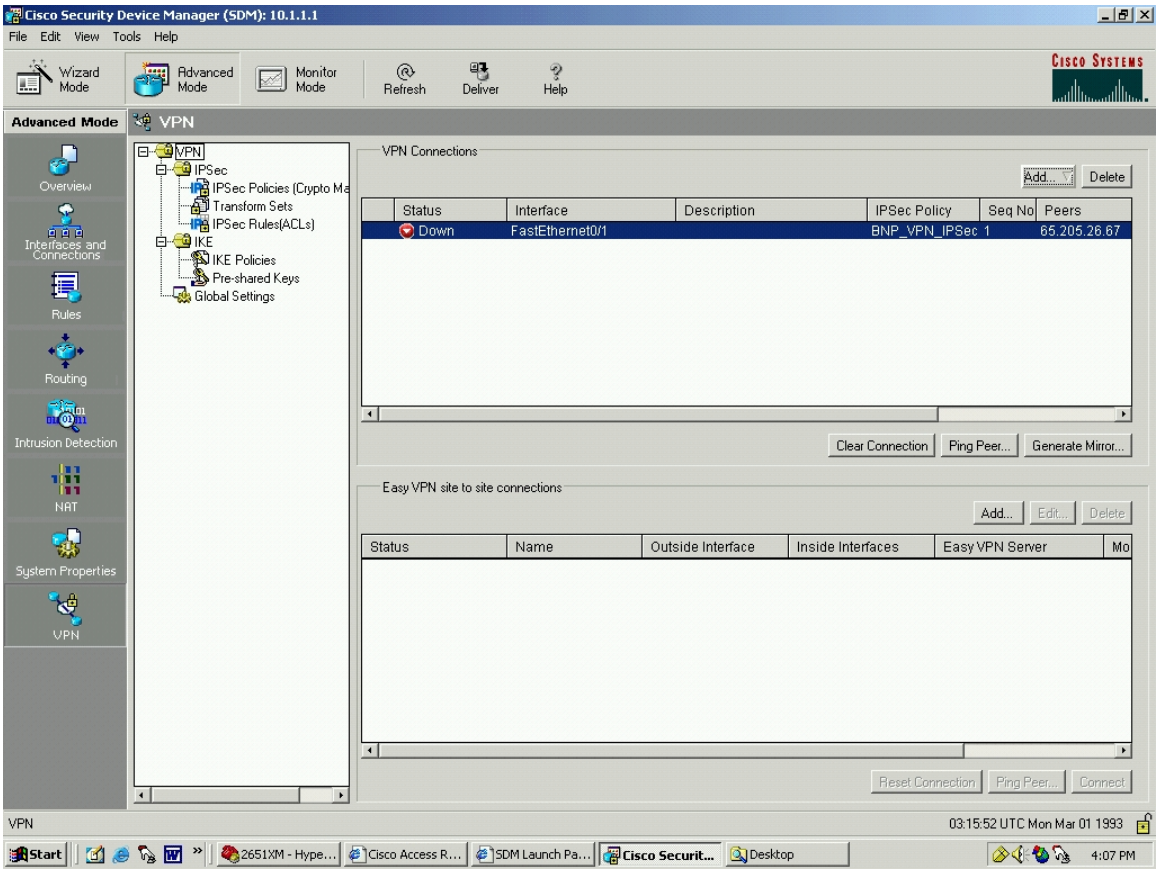

Figure 34. SDM VPN in Place

In the “VPN Connection” portion of the SDM window a red arrow down icon is displayed, Figure 34. This arrow will not turn into the green arrow up icon until the peer VPN is properly configured, and some traffic is exchanged. This process will be addressed later.

This screen indicates that the VPN is ready for operation. However if pings or other traffic were to be sent now, the VPN would not be operational because the commands have not yet been delivered to the router. The SDM GUI must now send the commands to the router to update the router’s running configuration. To do this, click on the “Deliver” button at the top of the screen. Once done, a very convenient preview screen of the CLI commands that will be delivered to the router will appear, Figure 35.

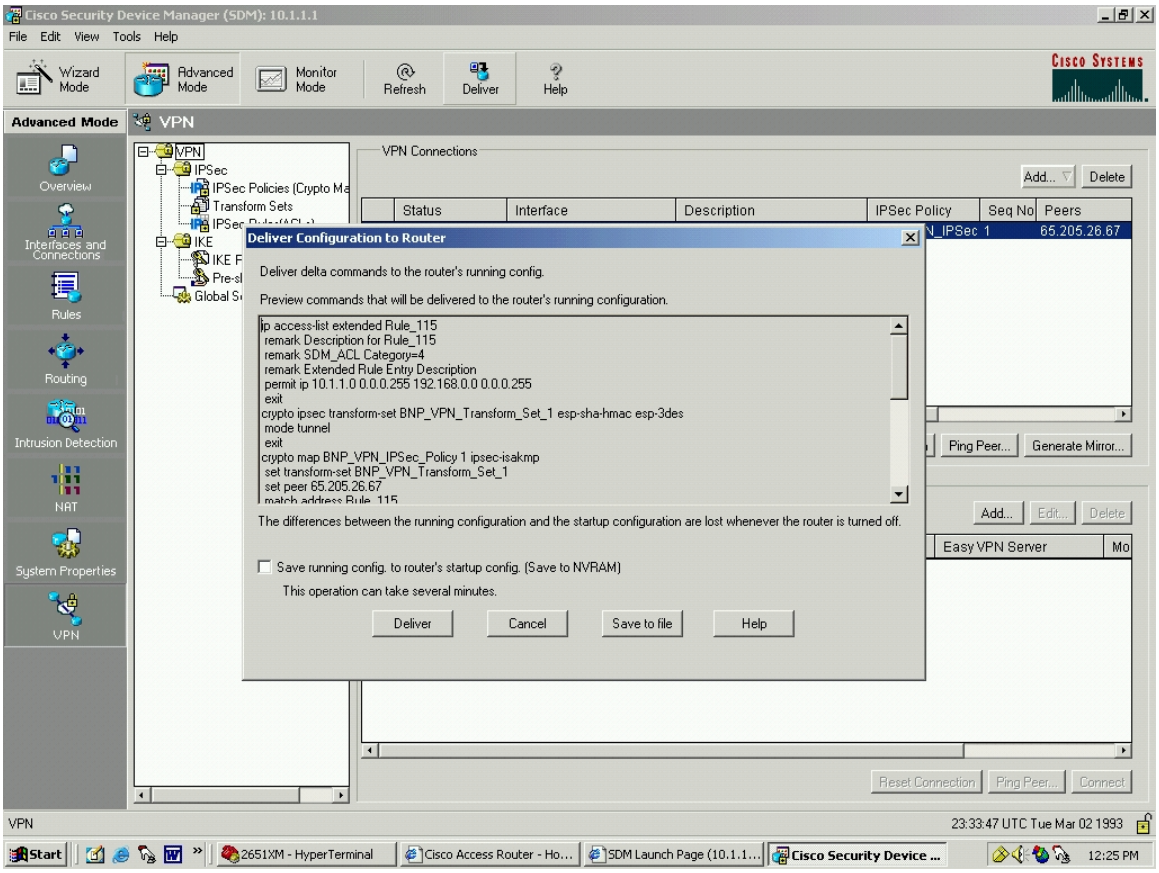

Figure 35. SDM Deliver Configuration to Router

It is possible to save these commands to a text file via the "Save to file" button on this screen. This is a convenient way to learn what the proper configuration commands are. Table 20 shows the result of the "Save to file" function. These commands are the CLI commands that the user would have had to enter in order to do the same things that were accomplished via the SDM GUI.

```
Configuration commands for the router: 10.1.1.1
saved on 26-May-04 12:26:28 PM
------------------------------------------------------------------------------
ip access-list extended Rule_115
 remark Description for Rule_115
 remark SDM_ACL Category=4
 remark Extended Rule Entry Description
 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.0.255
 exit
crypto ipsec transform-set BNP_VPN_Transform_Set_1 esp-sha-hmac esp-3des
 mode tunnel
 exit
crypto map BNP_VPN_IPSec_Policy 1 ipsec-isakmp
 set transform-set BNP_VPN_Transform_Set_1
 set peer 65.205.26.67
 match address Rule_115
```

```
set security-association lifetime seconds 86400
set security-association lifetime kilobytes 4608000
exit
interface FastEthernet0/1
no crypto map
crypto map BNP_VPN_IPSec_Policy
exit
crypto isakmp policy 1
authentication pre-share
encr 3des
hash sha
group 2
lifetime 86400
exit
crypto isakmp key ******** address 65.205.26.67 255.255.255.224
```

Table 20. SDM Save to File CLI Commands

Another worthwhile feature, if the user forgets to save the commands being delivered from the "Save to file" button just mentioned, is the "Generate Mirror" function. The "Generate Mirror" button exists on the Advanced Mode>VPN screen and will produce the CLI commands needed to configure the peer router via the CLI, as shown in Figure 36. This convenient feature drastically reduces the likelihood of making a mistake when configuring the peer router that will act as the VPN gateway at the far end of the tunnel.

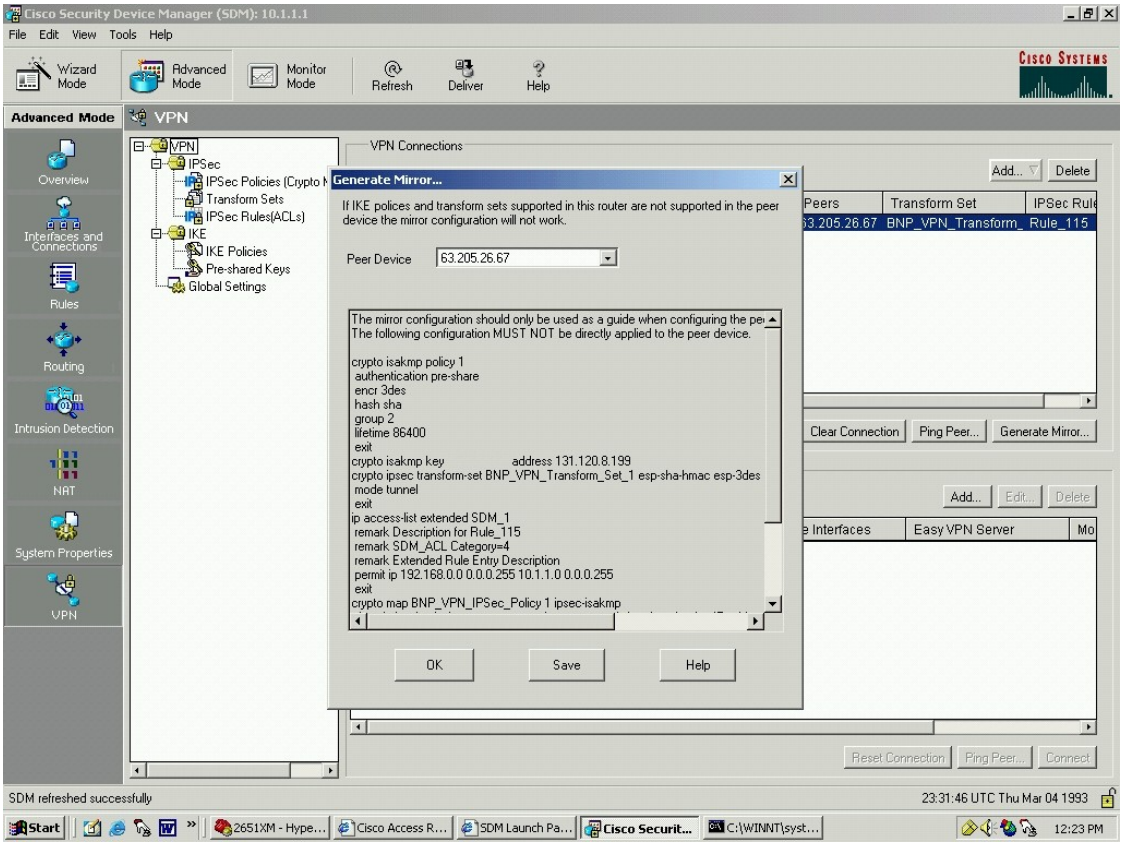

Figure 36. SDM Generate Mirror

The peer router commands for the UofC_VPN router that were produced by using the "Generate Mirror" command on the BNP_VPN router are shown in Table 21.

```
The mirror configuration should only be used as a guide when configuring the peer.
The following configuration MUST NOT be directly applied to the peer device.
crypto isakmp policy 1
 authentication pre-share
 encr 3des
 hash sha
 group 2
 lifetime 86400
 exit
crypto isakmp key !MyPassword! address 131.120.8.199
crypto ipsec transform-set BNP_VPN_Transform_Set_1 esp-sha-hmac esp-3des
 mode tunnel
 exit
ip access-list extended SDM_1
 remark Description for Rule_115
 remark SDM_ACL Category=4
 remark Extended Rule Entry Description
 permit ip 192.168.0.0 0.0.0.255 10.1.1.0 0.0.0.255
 exit
crypto map BNP_VPN_IPSec_Policy 1 ipsec-isakmp
 description Apply the crypto map on the peer router's interface having IP address
65.205.26.67 that connects to this router.
 set transform-set BNP_VPN_Transform_Set_1
```

```
set peer 131.120.8.199
match address SDM_1
set security-association lifetime seconds 86400
set security-association lifetime kilobytes 4608000
exit
```

Table 21. SDM Generate Mirror CLI Commands

3. Verification of the VPN Using SDM

Once the commands are delivered, the VPN is ready to have the tunnel built. A ping from the local network to the remote network will activate/build the tunnel. Even after the tunnel is constructed, the Advanced Mode>VPN screen will still show the tunnel as "Red Arrow Down". To rectify this, click on the "Refresh" button located near the top of the screen. The resulting green arrow is shown in Figure 37. For verification and a satisfying sanity check, the packets exchanged across the tunnel should be verified as IPSec encapsulated via a packet analyzer.

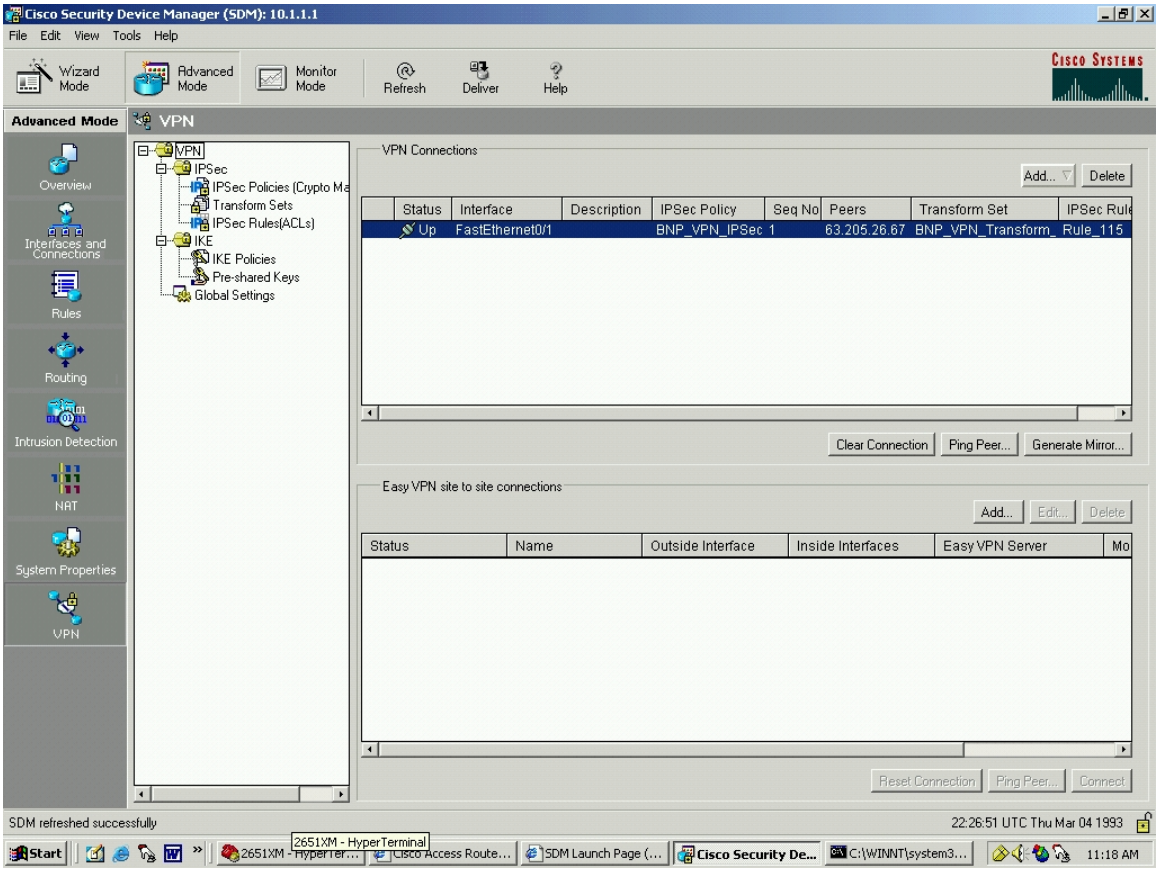

Figure 37. SDM VPN Connection Verified Up

There are several other functions pictured on the screenshot above that are worthy of note. The "Ping Peer" button sends pings in the clear. It allows the user to test the functionality of the router configuration without involving the VPN configuration. This is useful if the VPN does not work. Begin troubleshooting by checking that, in this case, the BNP_VPN router can ping the UofC_VPN router.

The other button that is worth mentioning is the "Clear Connection" button. If a tunnel is built, this button will reset the tunnel to a down status, awaiting the first traffic that will kick off IKE Phase One and cause the tunnel creation process.

The SDM also supports a VPN monitor mode, shown in Figure 38. The monitor mode allows the viewing of the traffic that is traversing the IPSec tunnel. It shows information about the status of the tunnel, as well as the number of packets sent and received, including encapsulated, nonencapsulated, and error packets.

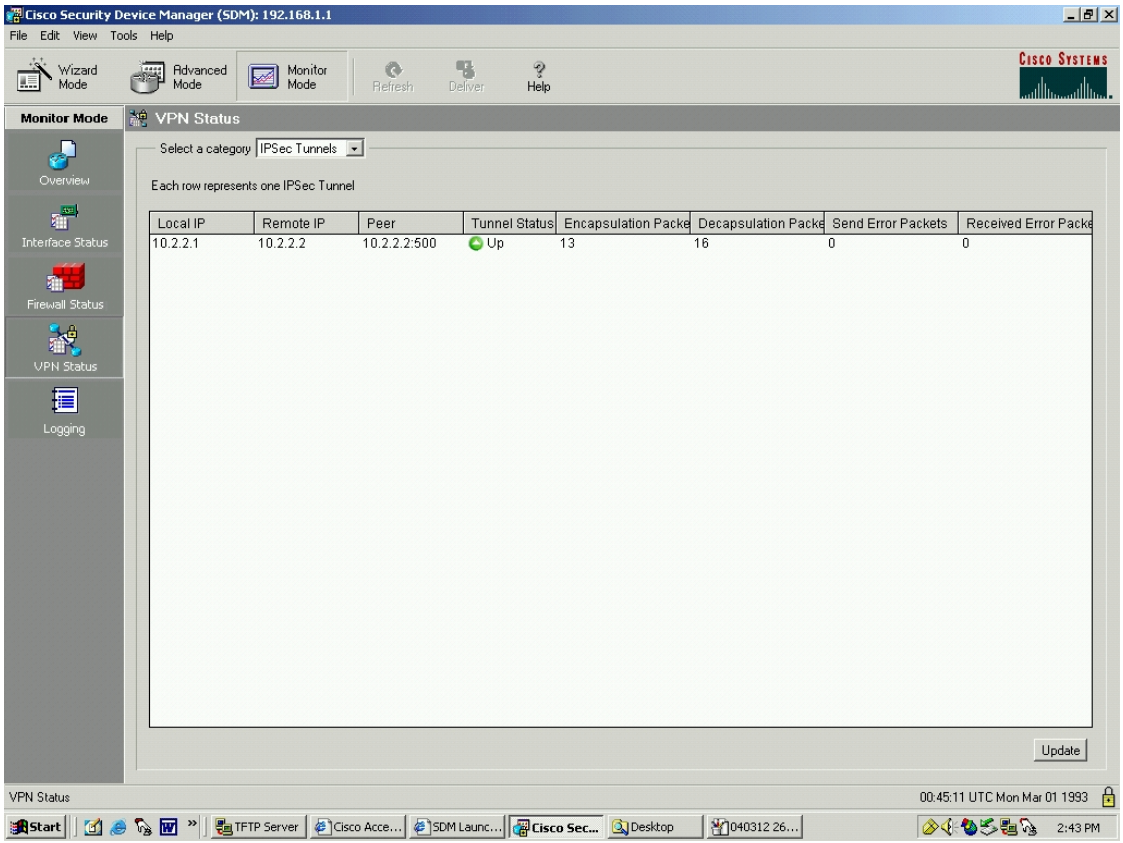

Figure 38. SDM VPN Monitor Mode IPSec Tunnels

With a change in the drop down menu, it is possible to monitor the IKE SA as well, as shown in Figure 39.

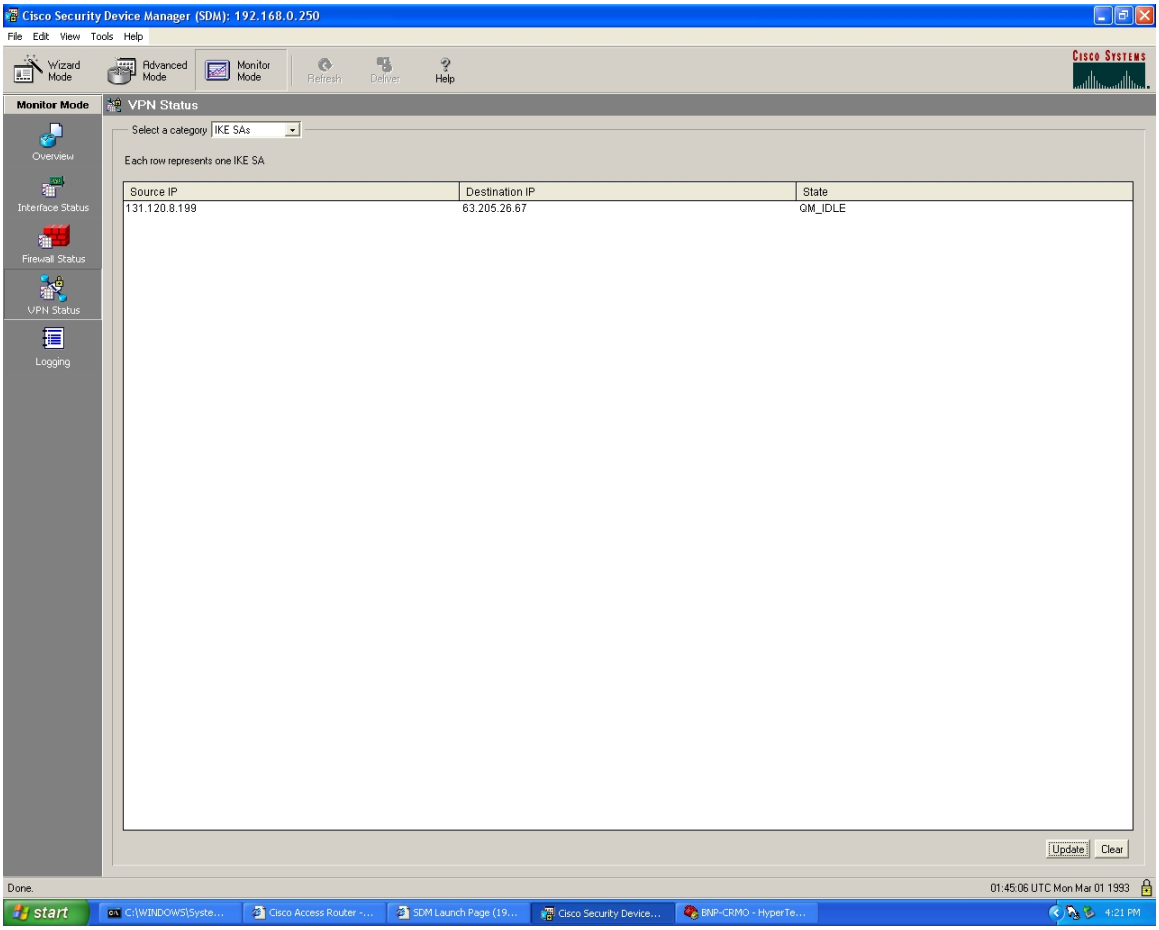

Figure 39. SDM VPN Monitor Mode IKE SAs

C. VPN CONCENTRATOR TO ROUTER

The second option is to utilize a VPN Concentrator as one of the end points. It would be possible to use a VPN Concentrator at both ends of the VPN, but NPS only has access to one Cisco VPN 3005 Concentrator. This section is a demonstration of how to build a VPN suitable for a cyber-exercise using a Cisco VPN Concentrator as one endpoint, and using the router as the other VPN endpoint. The same network is being used between NPS and U of C as was used in the discussion above. The network layout it repeated in Figure 40 for the reader's convenience.

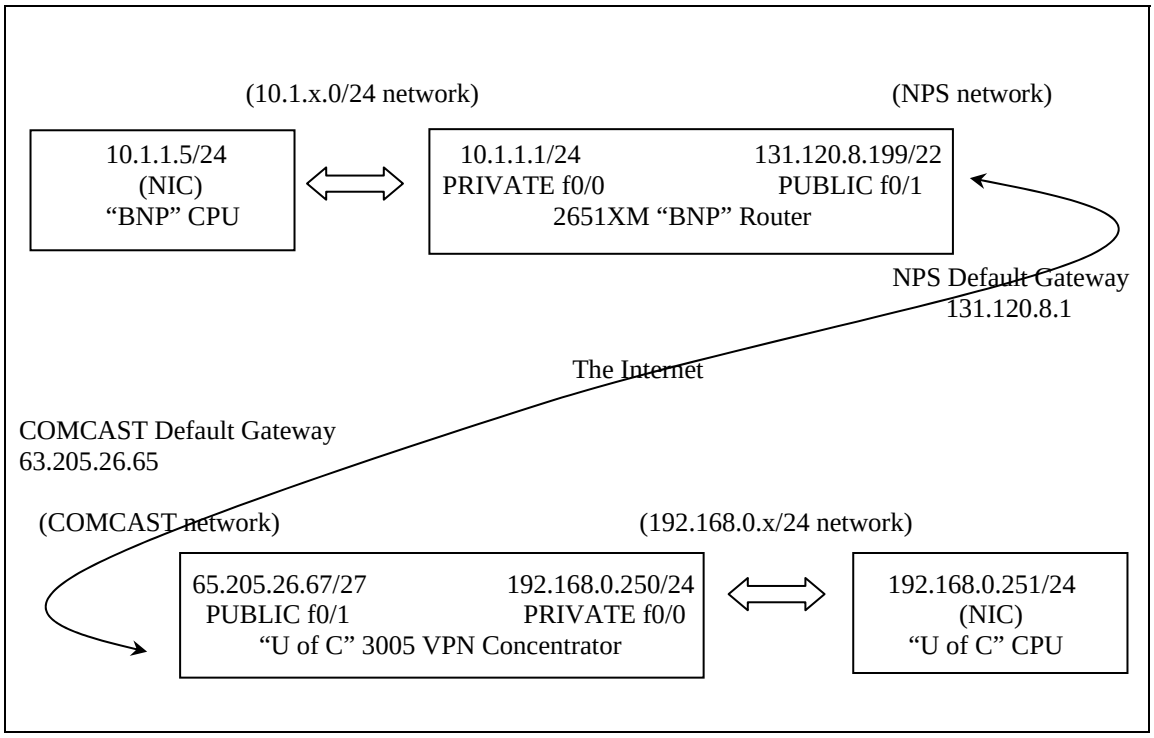

Figure 40. VPN Concentrator to Router Network Diagram

The first step is the basic setup of the VPN Concentrator. Establish a hyperterminal connection to the concentrator exactly as was done for the router. The commands are shown in Table 10. When the concentrator is turned on, configuration can begin. The commands are depicted in Table 22.

```
Starting power-up diagnostics...

...
Copyright (c) Integrated Systems, Inc., 1992.
Cisco Systems, Inc./VPN 3000 Concentrator Version 4.0.1.Rel May 06 2003 13:13:03
Features:
Initializing VPN 3000 Concentrator ...
Waiting for CAPI initialization to complete...
Initialization Complete...Waiting for Network...

08/01/2004 13:50:57.360 SEV=1 EVENT/37 RPT=1

Login: admin
Password: YourPassword

               Welcome to
              Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2003 Cisco Systems, Inc.

 -- : Set the time on your device. The correct time is very important,
 -- : so that logging and accounting entries are accurate.
 -- : Enter the system time in the following format:
 -- :       HH:MM:SS.  Example  21:30:00  for 9:30 PM
```

```
> Time
Quick -> [ 13:51:10 ] 13:54:00

 -- : Enter the date in the following format.
 -- : MM/DD/YYYY  Example 06/12/1999  for June 12th 1999.
> Date
Quick -> [ 06/01/2004 ] 08/01/2004

 -- : Set the time zone on your device. The correct time zone is very
 -- : important so that logging and accounting entries are accurate.
 -- : Enter the time zone using the hour offset from GMT:
 -- : -12 : Kwajalein  -11 : Samoa    -10 : Hawaii          -9 : Alaska
 -- :  -8 : PST         -7 : MST        6 : CST             -5 : EST
 -- :  -4 : Atlantic    -3 : Brasilia  -2 : Mid-Atlantic    -1 : Azores
 -- :   0 : GMT         +1 : Paris     +2 : Cairo           +3 : Kuwait
 -- :  +4 : Abu Dhabi   +5 : Karachi   +6 : Almaty          +7 : Bangkok
 -- :  +8 : Singapore   +9 : Tokyo    +10 : Sydney         +11 : Solomon Is.
 -- : +12 : Marshall Is.
> Time Zone
Quick -> [ -8 ] -8

1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support
Quick -> [ 1 ] 1

This table shows current IP addresses.
  Intf         Status       IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Ether1-Pri | Not Configured |        0.0.0.0/0.0.0.0    |
Ether2-Pub | Not Configured |        0.0.0.0/0.0.0.0    |
--------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

** An address is required for the private interface. **
> Enter IP Address
Quick Ethernet 1 -> [ 0.0.0.0 ] 10.1.1.1

> Enter Subnet Mask
Quick Ethernet 1 -> [ 255.0.0.0 ] 255.255.255.0

1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect
Quick Ethernet 1 -> [ 3 ] 2

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex
Quick Ethernet 1 -> [ 1 ] 3

> MTU (68 - 1500)
Quick Ethernet 1 -> [ 1500 ] 1500

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit
Quick -> 2

This table shows current IP addresses.
  Intf         Status       IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Ether1-Pri |      UP  |   10.1.1.1/255.255.255.0 | 00.03.A0.89.95.F3
Ether2-Pub | Not Configured |        0.0.0.0/0.0.0.0    |
--------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
```

```
DNS Domain Name:
        Default Gateway: Default Gateway Not Configured

        > Enter IP Address
        Quick Ethernet 2 -> [ 0.0.0.0 ] 131.120.8.199

        > Enter Subnet Mask
        Quick Ethernet 2 -> [ 255.255.0.0 ] 255.255.252.0

        1) Ethernet Speed 10 Mbps
        2) Ethernet Speed 100 Mbps
        3) Ethernet Speed 10/100 Mbps Auto Detect
        Quick Ethernet 2 -> [ 3 ] 2

        1) Enter Duplex - Half/Full/Auto
        2) Enter Duplex - Full Duplex
        3) Enter Duplex - Half Duplex
        Quick Ethernet 2 -> [ 1 ] 3

        > MTU (68 - 1500)
        Quick Ethernet 2 -> [ 1500 ] 1500

        1) Modify Ethernet 1 IP Address (Private)
        2) Modify Ethernet 2 IP Address (Public)
        3) Save changes to Config file
        4) Continue
        5) Exit
        Quick -> 3

        1) Modify Ethernet 1 IP Address (Private)
        2) Modify Ethernet 2 IP Address (Public)
        3) Save changes to Config file
        4) Continue
        5) Exit
        Quick -> 5

        Done
```

Table 22. Concentrator Initial Hyperterminal Configuration

Table 22 showed the initial configuration. The rest of the configuration will be accomplished using the graphical user interface provided for the 3005. Ensure that the computer that was used for the serial cable hyperterminal connection to the 3005 is assigned an IP address that is compatible with the network created on the “private” side of the 3005.

Utilize an ethernet cable between the PC network interface card (NIC) and the private port on the rear of the 3005. Open a network connection and login to the network address of the 3005 Concentrator.

Upon first login, the Quick Configuration window will appear, Figure 41.

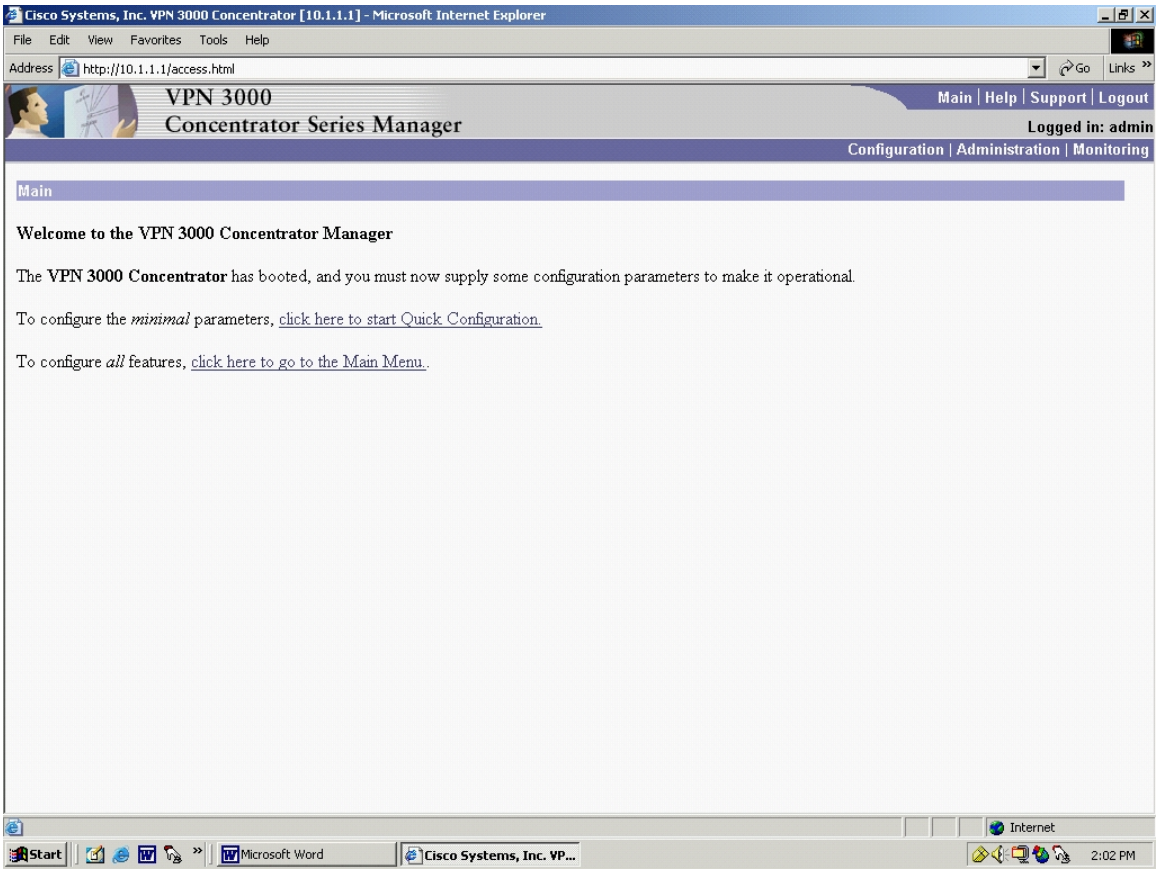

Figure 41. Concentrator Manager Welcome

If the user chooses not to go through the Quick Configuration, it will never appear again unless a system reset is performed which will require going through the hyperterminal setup again. Although it is possible to skip the Quick Configuration and then go into the individual configuration screens, it is recommended that the user take the guided tour through the Quick Configuration.

Choosing Quick Configuration brings up the Interfaces Screen, Figure 42.

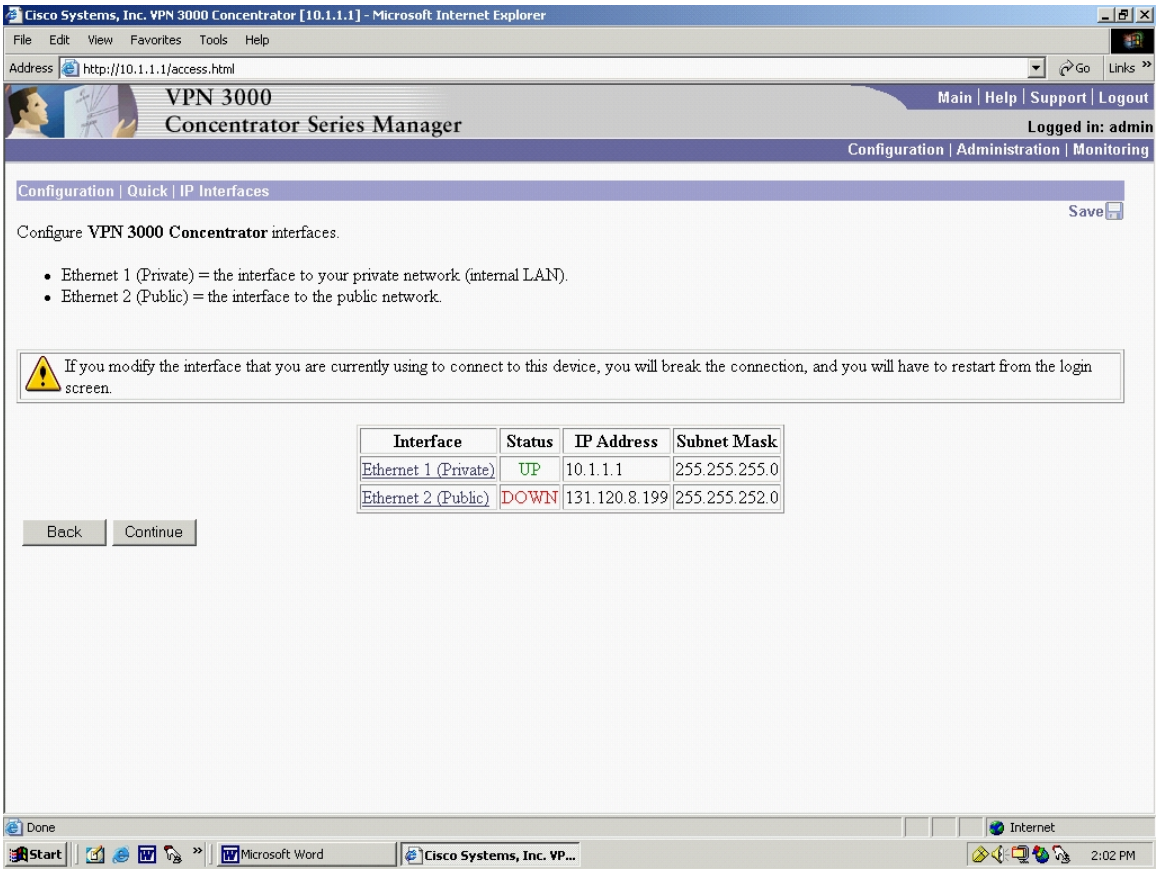

Figure 42. Concentrator Initial Configuration: Interfaces

Notice right away that at the top of the screen, the 3005 shows the user's location within the menu structure. Shown in Figure 42, it is "Configuration | Quick | IP Interfaces". Later, this hierarchical nomenclature that appears at the top of the screen will be echoed by a menu tree that will appear on the left side.

The status of the public port shows "DOWN" because the Ethernet cable was not connected to the Public port on the rear of the 3005. Note: It is possible to configure the 3005 without the public Ethernet cable connected.

Clicking "Continue" brings up the Ethernet Interface 1 (Private) screen, Figure 43.

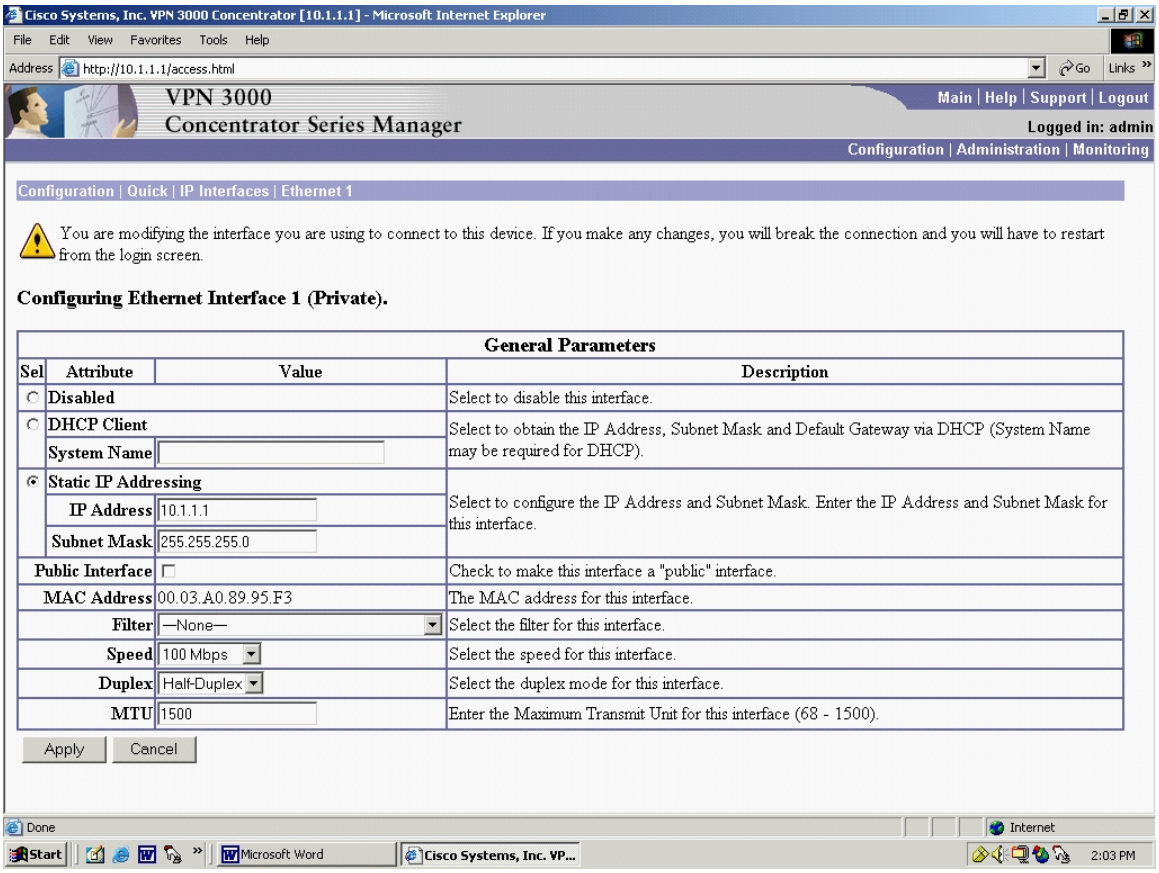

Figure 43. Concentrator Initial Configuration: Interface 1 (Private)

Notice that many of the options have already been configured. However, this screen gives the user a chance to make any changes.

Clicking “Apply” advances the Quick Configuration tour to the Configuring Ethernet Interface 2 (Public) screen, Figure 44.

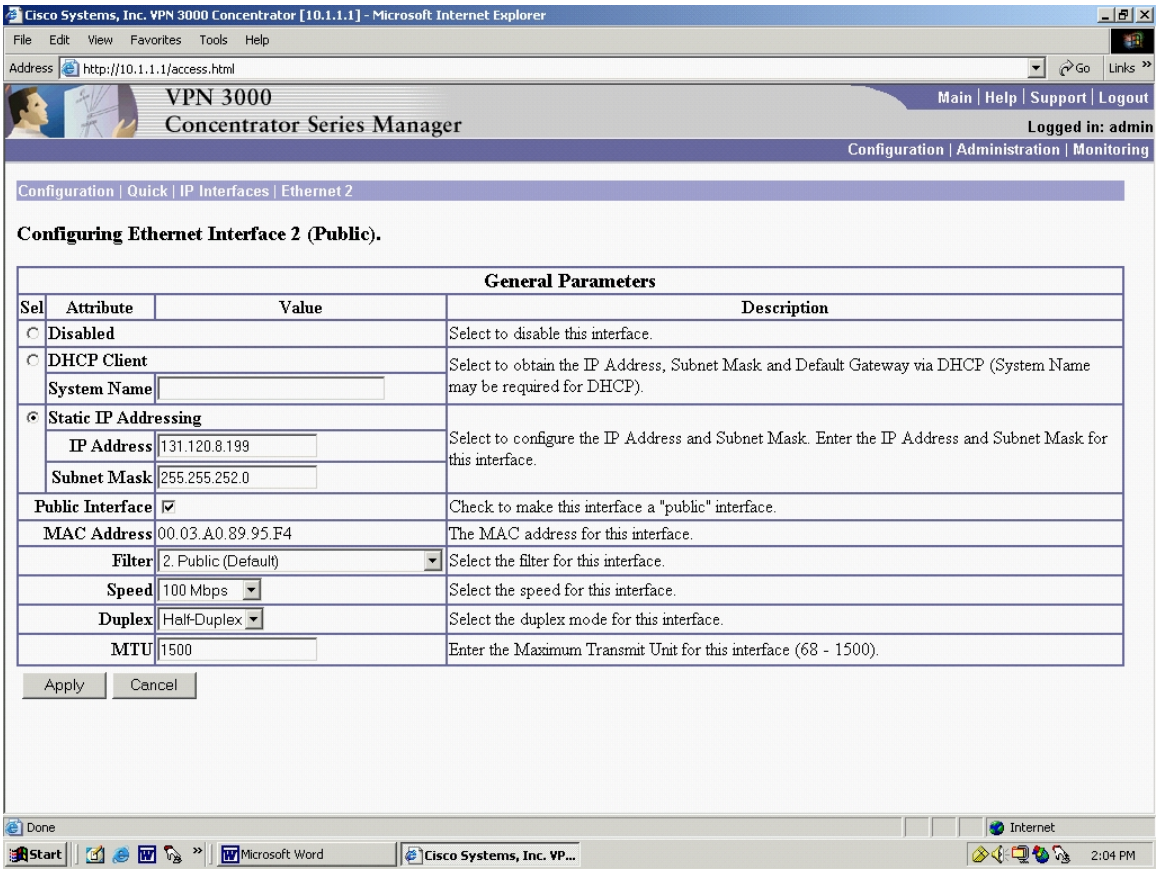

Figure 44. Concentrator Initial Configuration: Interface 2 (Public)

Similar to the router configuration, if the user intends to connect an inexpensive hub between the VPN 3005 Concentrator and the Internet, it is recommended that the port speed not be set to "Auto". Select either 100Mbps or 10Mbps. Inexpensive hubs are often not able to automatically negotiate port speed and this will cause loss of connectivity. Likewise, be sure to select half-duplex as inexpensive hubs cannot handle full-duplex traffic.

Clicking "Apply" brings the Configuration | Quick | System Info screen, Figure 45.

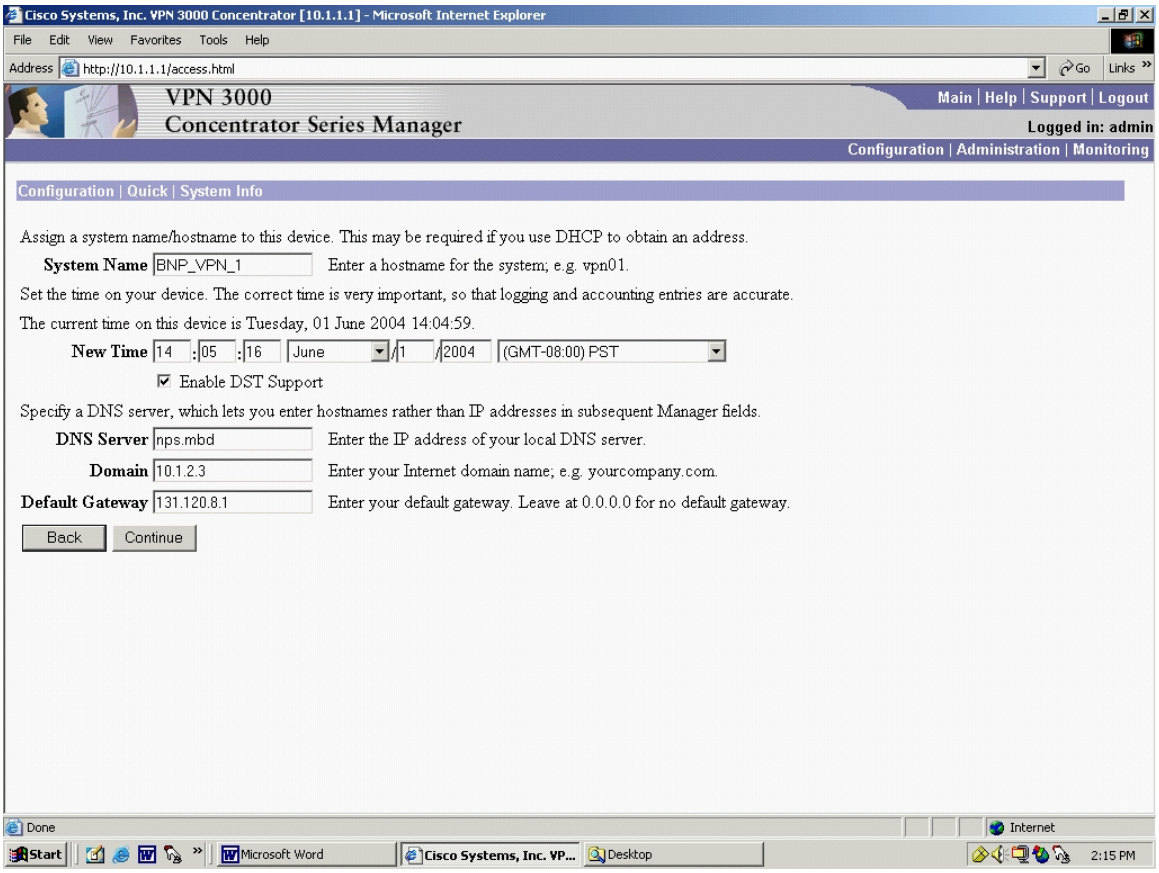

Figure 45. Concentrator Initial Configuration: System Info

This screen, Figure 45, allows the user to set several items that have not been able to be set before, namely the DNS Server, Domain, and Default Gateway. The System Name, Time, and Daylight Savings preference appear again if the user wants to make changes.

Clicking “Continue” brings the Configuration | Quick | Protocols screen, Figure 46.

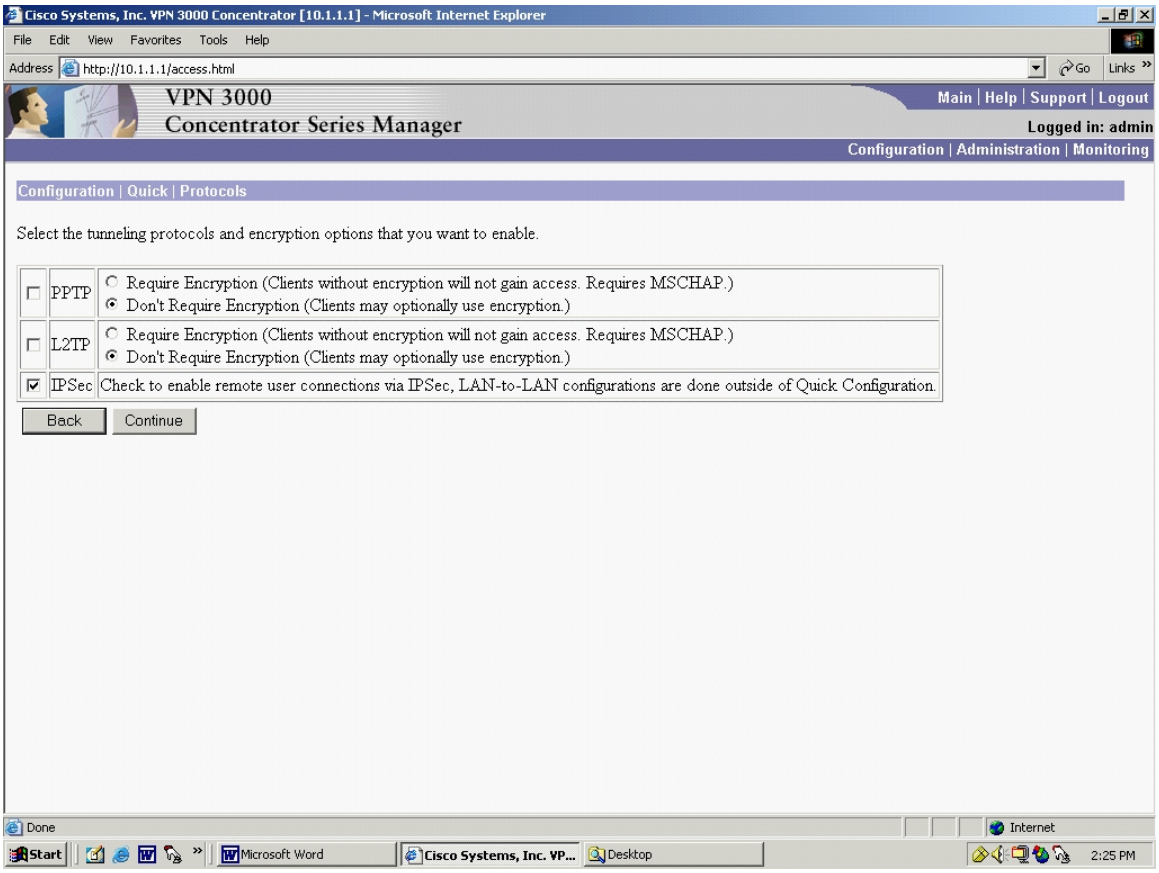

Figure 46. Concentrator Initial Configuration: Protocols

Clicking “Continue” brings Figure 47, the Configuration | Quick | Address Assignment screen:

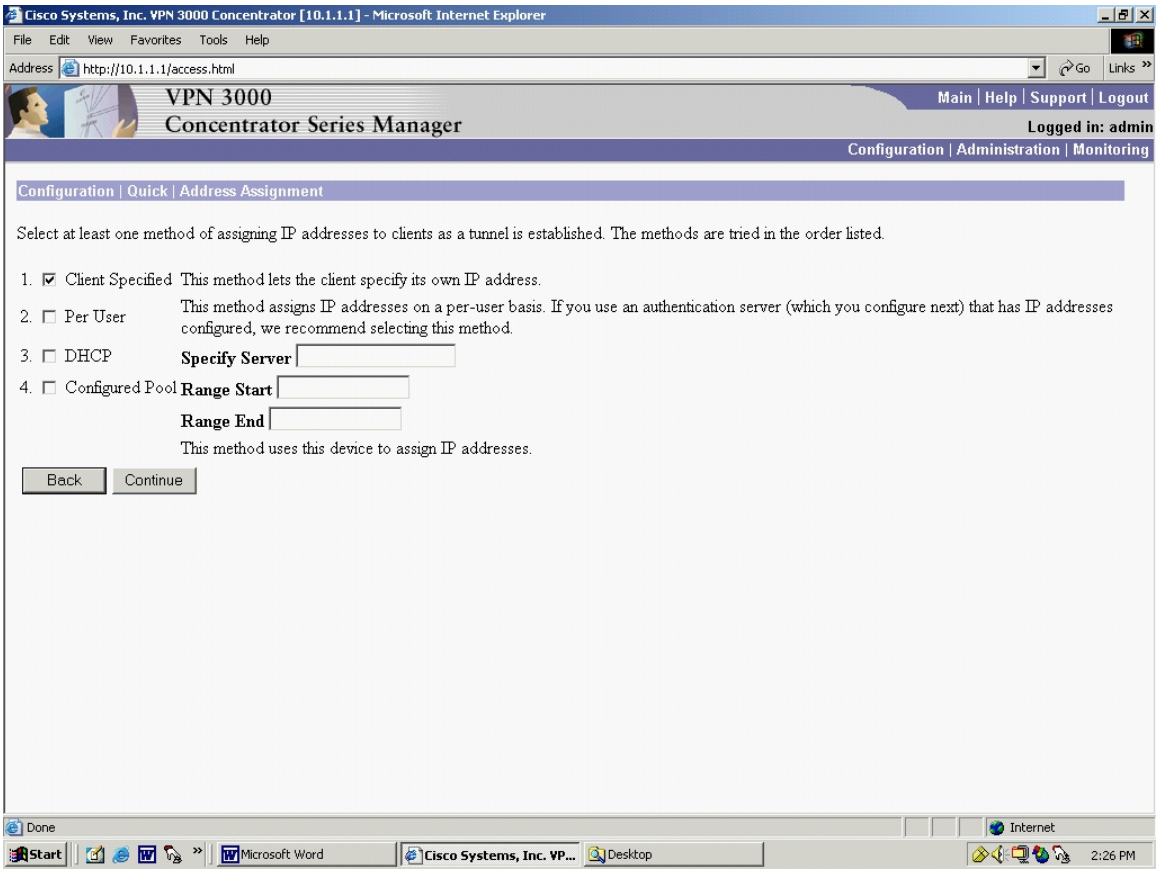

Figure 47. Concentrator Initial Configuration: Address Assignment

In this example, all computers on the private network already have their own IP addresses, so "Client Specified" is selected. However, if the 3005 system was needed to play the role of a DHCP Server, this screen would allow the user to enable that functionality.

Clicking "Continue" brings Figure 48, the Configuration | Quick | Authentication screen:

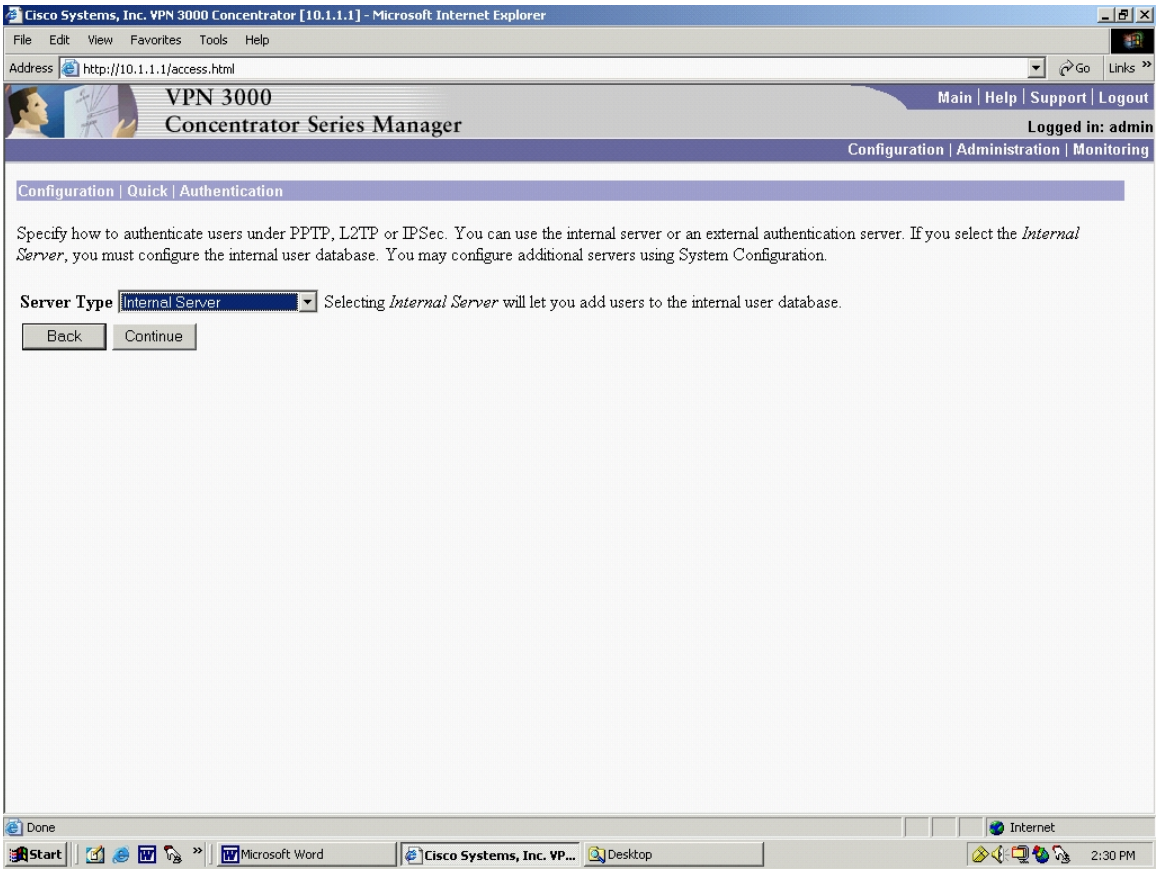

Figure 48. Concentrator Initial Configuration: Authentication

In this example, a dedicated authentication server is not being used, so the internal authentication provided by the 3005 will ultimately provide this functionality.

Clicking “Continue” to bring Figure 49, the Configuration | Quick | User Database

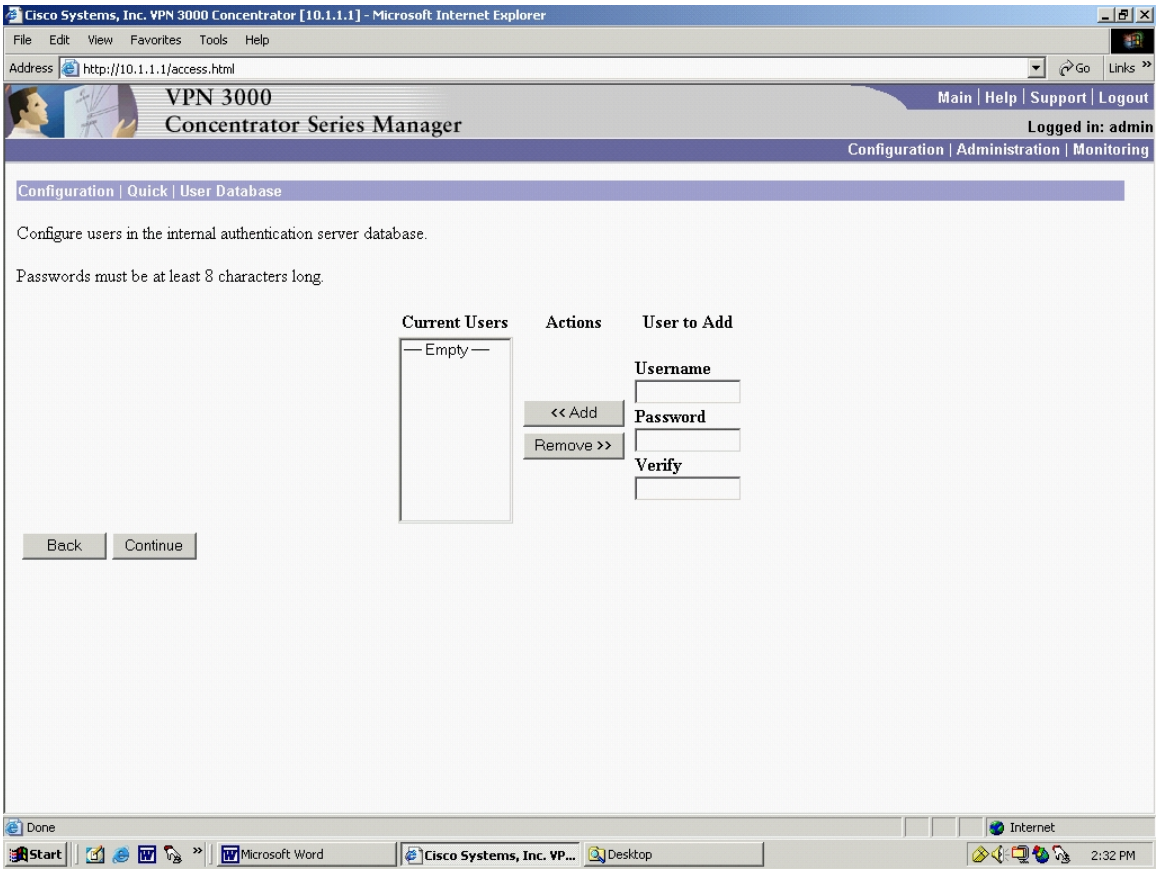

Figure 49. Concentrator Initial Configuration: Authentication Database

From the amount of documentation that is devoted to it, Cisco seems committed to using the 3005 for remote dial-up users. This is where the administrator would enter the users and passwords. For this thesis, however, no users are required.

Clicking “Continue” brings up the Configuration | Quick | IPSec Group screen, Figure 50.

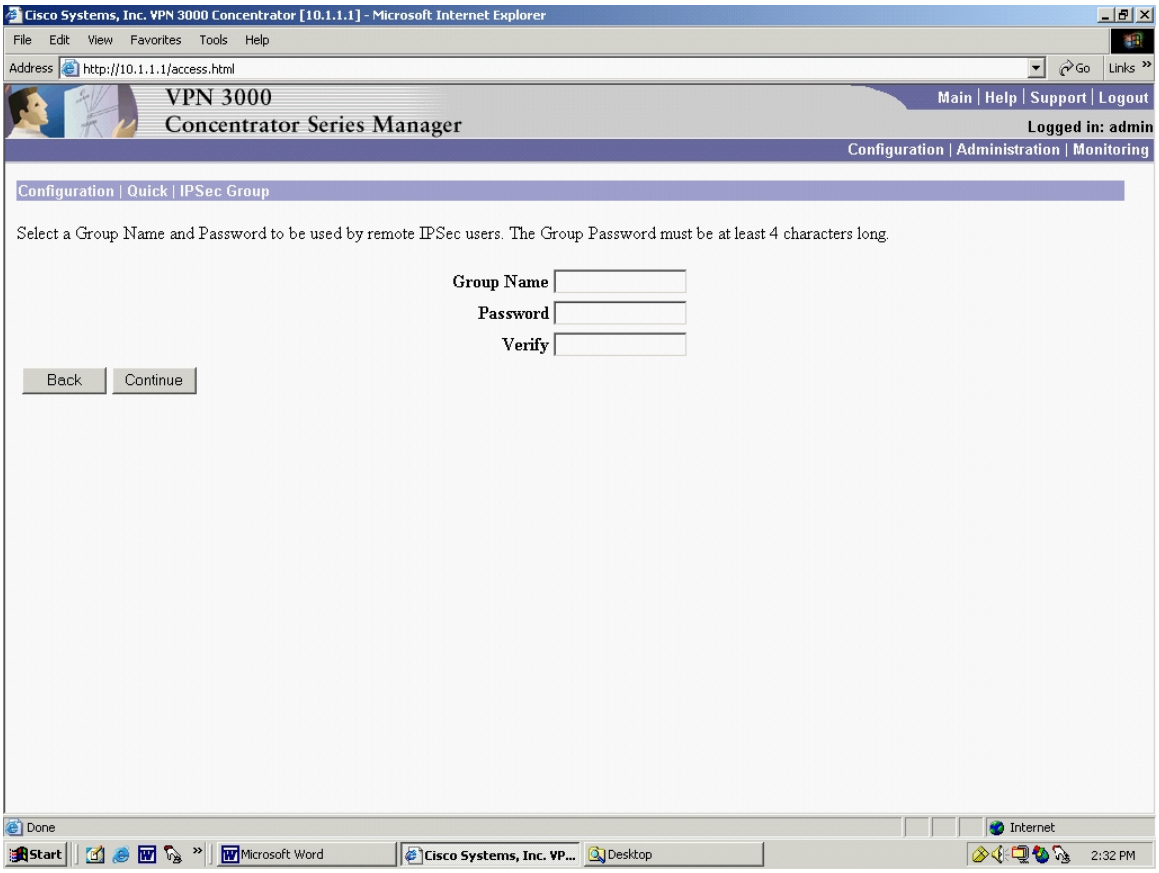

Figure 50. Concentrator Initial Configuration: IPSec Group

Groups are not required for a cyber-exercise LAN-to-LAN VPN. Clicking "Continue" brings the Configuration | Quick | Admin Password screen, Figure 51.

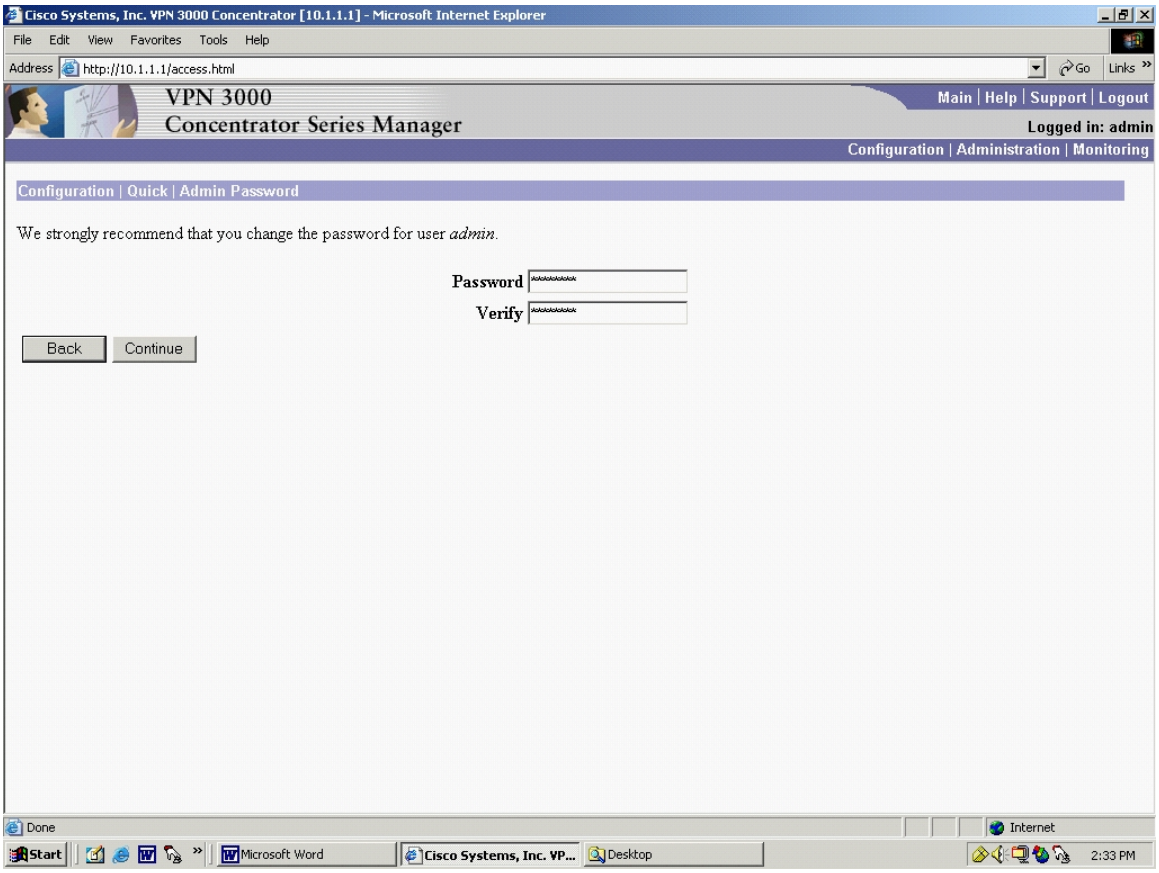

Figure 51. Concentrator Initial Configuration: Password Configuration

This final screen in the Quick Configuration tour allows the user to change the default login and password. Clicking "Continue" brings the last screen in the Quick Configuration tour, the Configuration | Quick | Done screen, Figure 52.

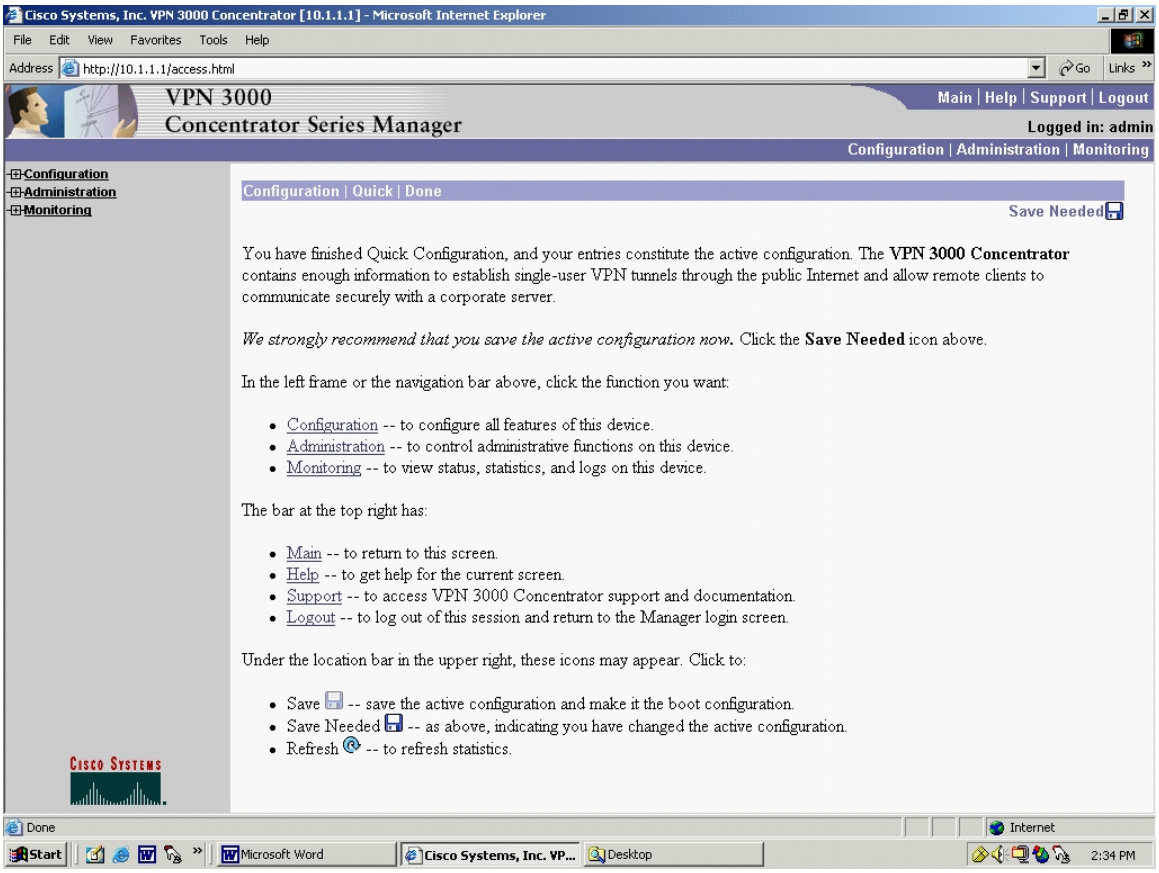

Figure 52. Concentrator Initial Configuration: Complete

There are many noteworthy items in Figure 52.

A directory structure on the left has appeared which includes Configuration, Administration, and Monitoring. Notice that these three are echoed by the Hotlinks near the middle of this window. Also, the "Save Needed" icon appears at the top left. Anytime a configuration change has been made, the icon, which normally is a grayed out "save", changes to an active "Save Needed". Clicking on it (recommended) saves the settings the user has input during the Quick Configuration tour.

Next is the process of setting up the cyber-exercise LAN-to-LAN VPN. Navigating via the left side menu tree, select Configuration | Interfaces. The resulting screen is shown in Figure 53.

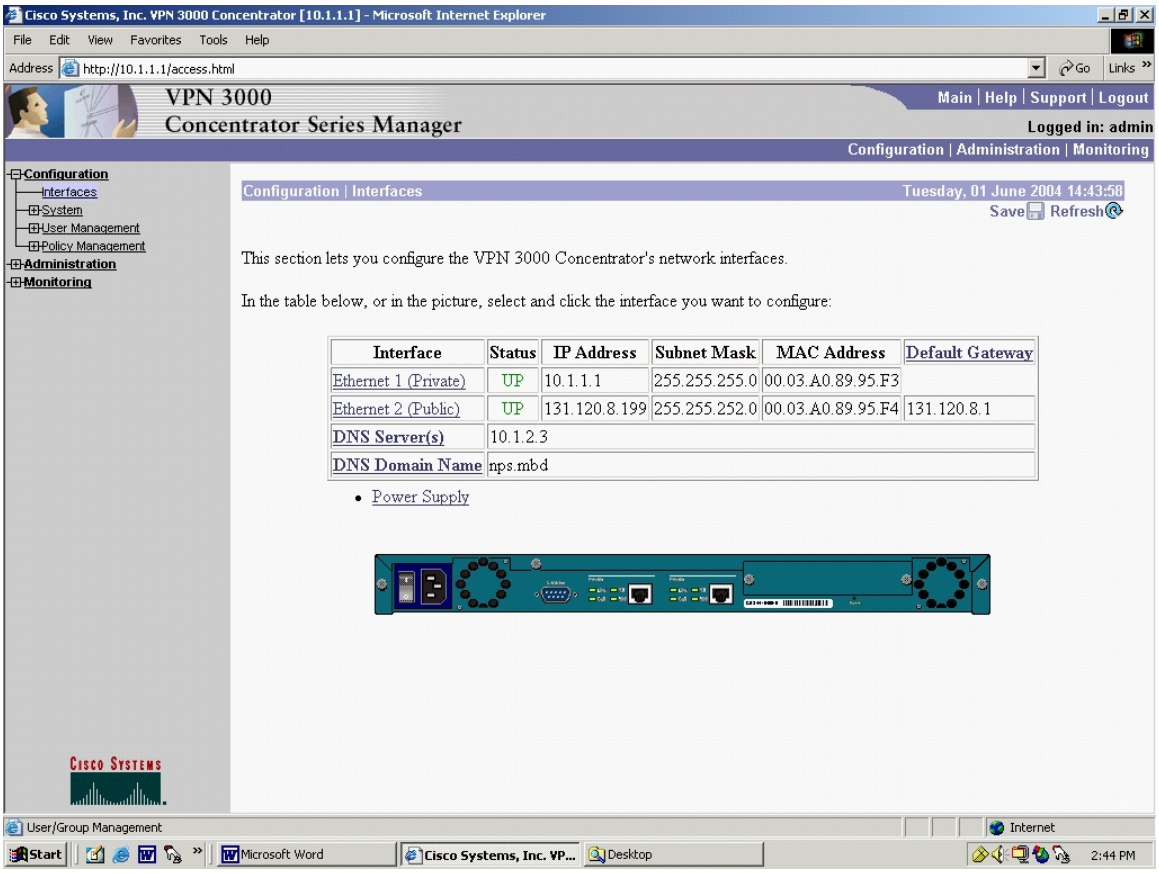

Figure 53. Concentrator Interfaces

The user can observe that the selections made during the Quick Configuration are displayed. If any settings needed to be adjusted, click on the hotlink. To continue setting up the cyber-exercise VPN, in Figure 53, click Ethernet 1 (Private). The resulting screen is shown in Figure 54.

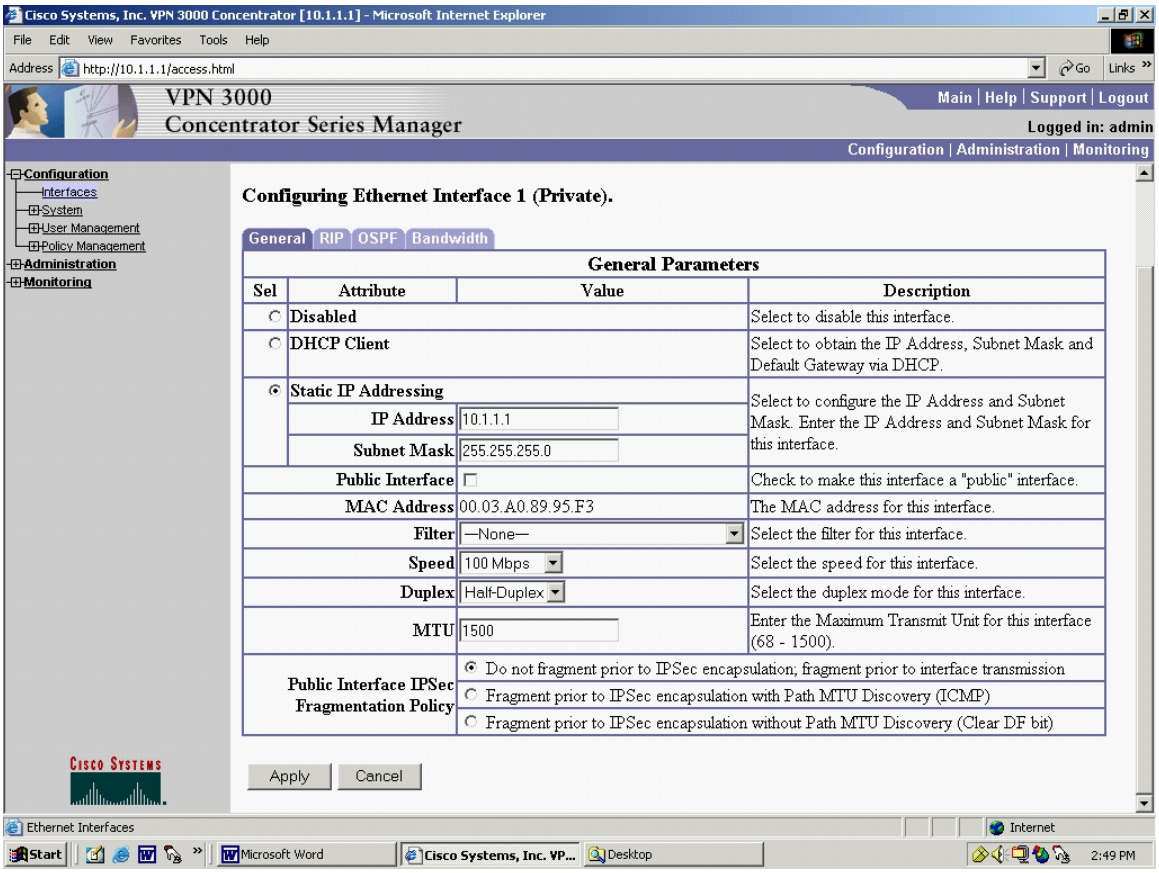

Figure 54. Concentrator Interface 1 (Private) General

Unlike the Quick Configuration, there are four TABs in Figure 54. The General TAB is the default view. Routing Internet Protocol (RIP) needs to be configured, so click on the RIP tab:

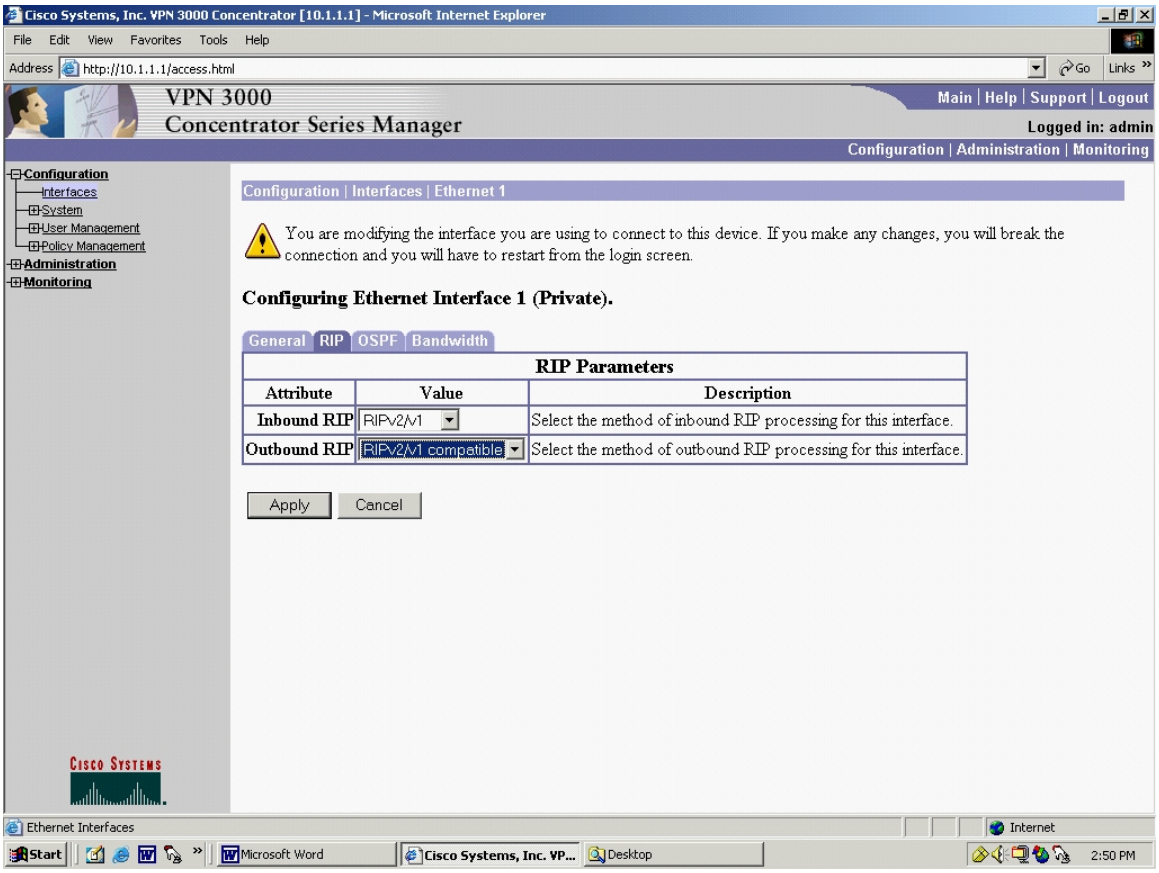

Figure 55. Concentrator Interface 1: Enabling RIP

Ensure that the selections shown in Figure 55 are selected. Click “Apply”, which brings up the “Interfaces” screen again, Figure 56. Click on the “Ethernet 2 (Public)” hotlink.

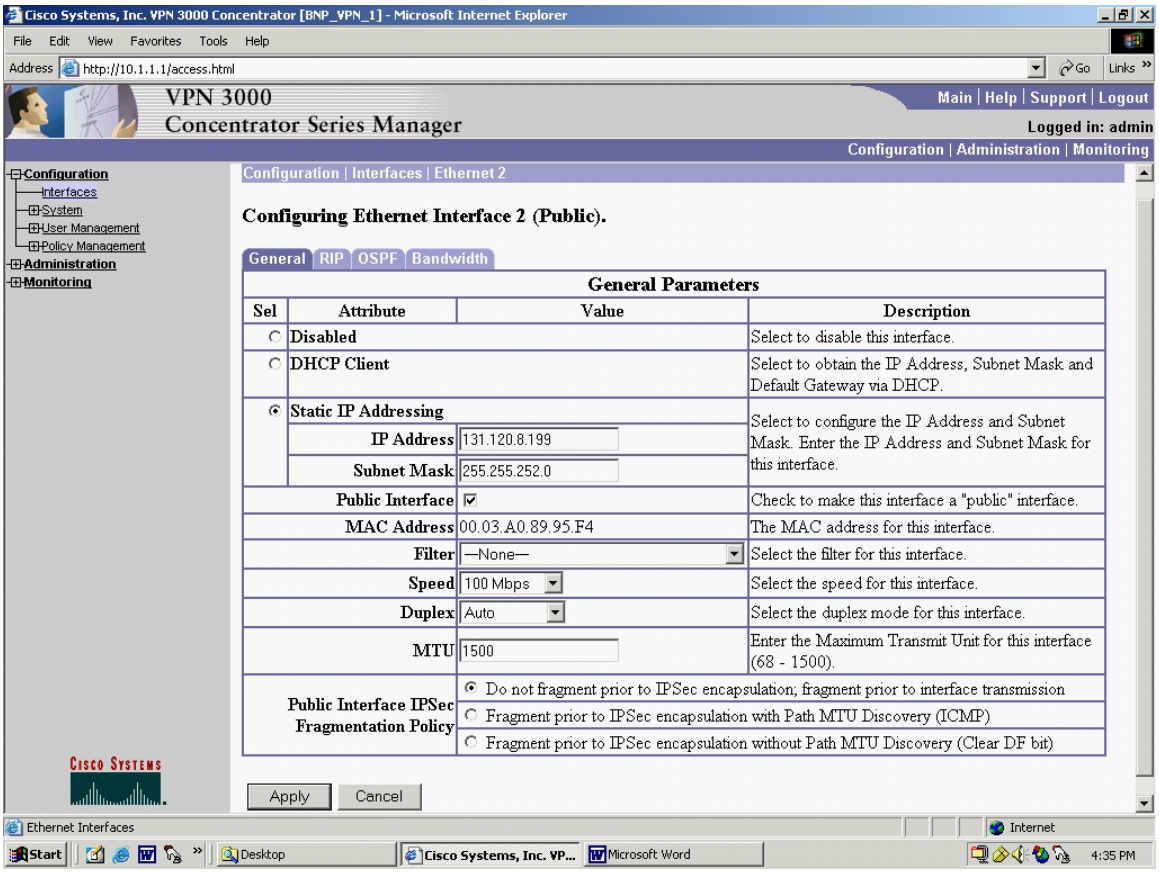

Figure 56. Concentrator Interface 2 (Public): General

Notice in Figure 56 there are a few items that are different from the Private screen.

Ensure the “Public Interface” box is checked. Before leaving this screen, select the “RIP” tab and configure its RIP exactly as the RIP tab was configured for Ethernet 1 (Private). Click “Apply”. Now select the Configuration | System | IP Routing | Default Gateways from the left side menu tree, Figure 57.

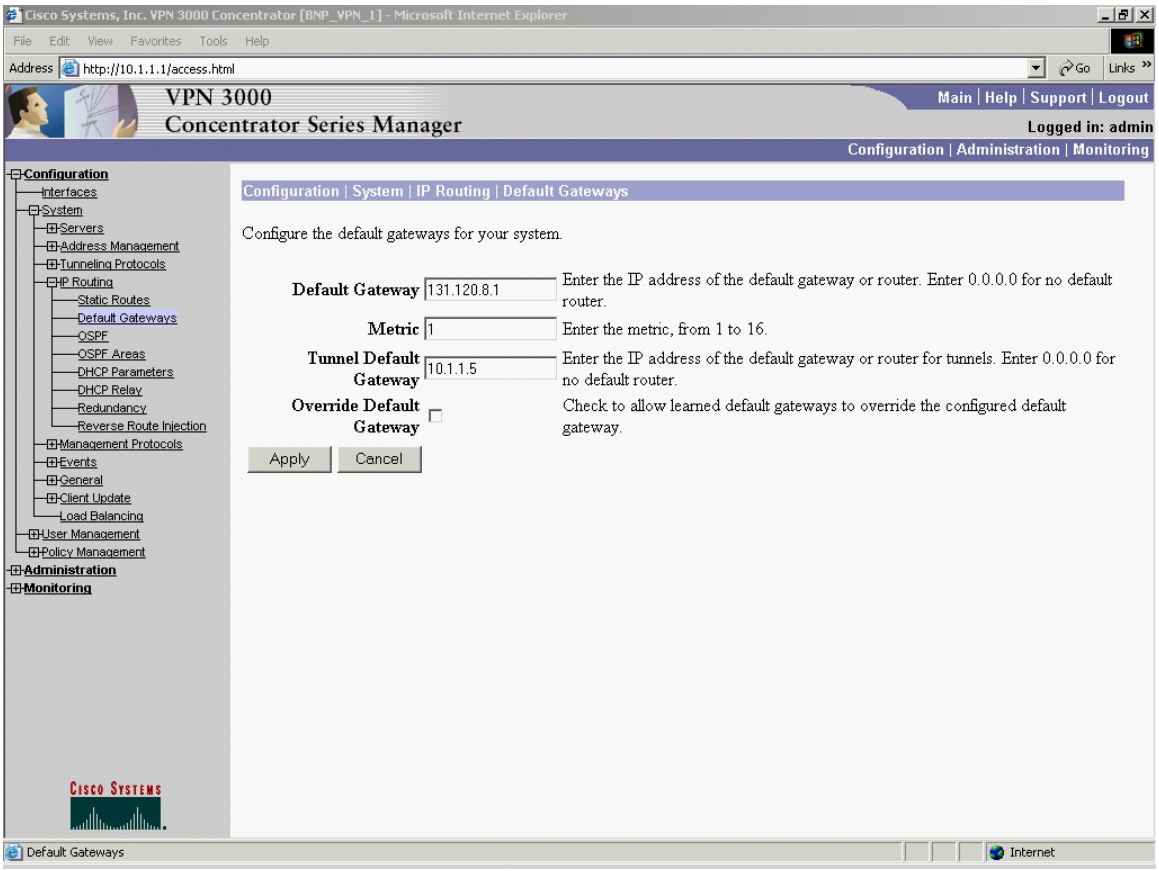

Figure 57. Concentrator Default Gateway

Figure 57 presents one of the most nonintuitive selections. The Default Gateway and metric are self-explanatory, but the "Tunnel Default Gateway" is misleading. The entry for "Tunnel Default Gateway" needs to be the network that is behind the *private port* of the 3005. In other words, this is the network where the traffic to be encrypted comes *from*, which in this example is 10.1.1.5. Click "Apply".

Navigating via the left side menu tree, select Configuration | Policy Management | Traffic Management | Network Lists and click "New". The resulting screen is shown, Figure 58.

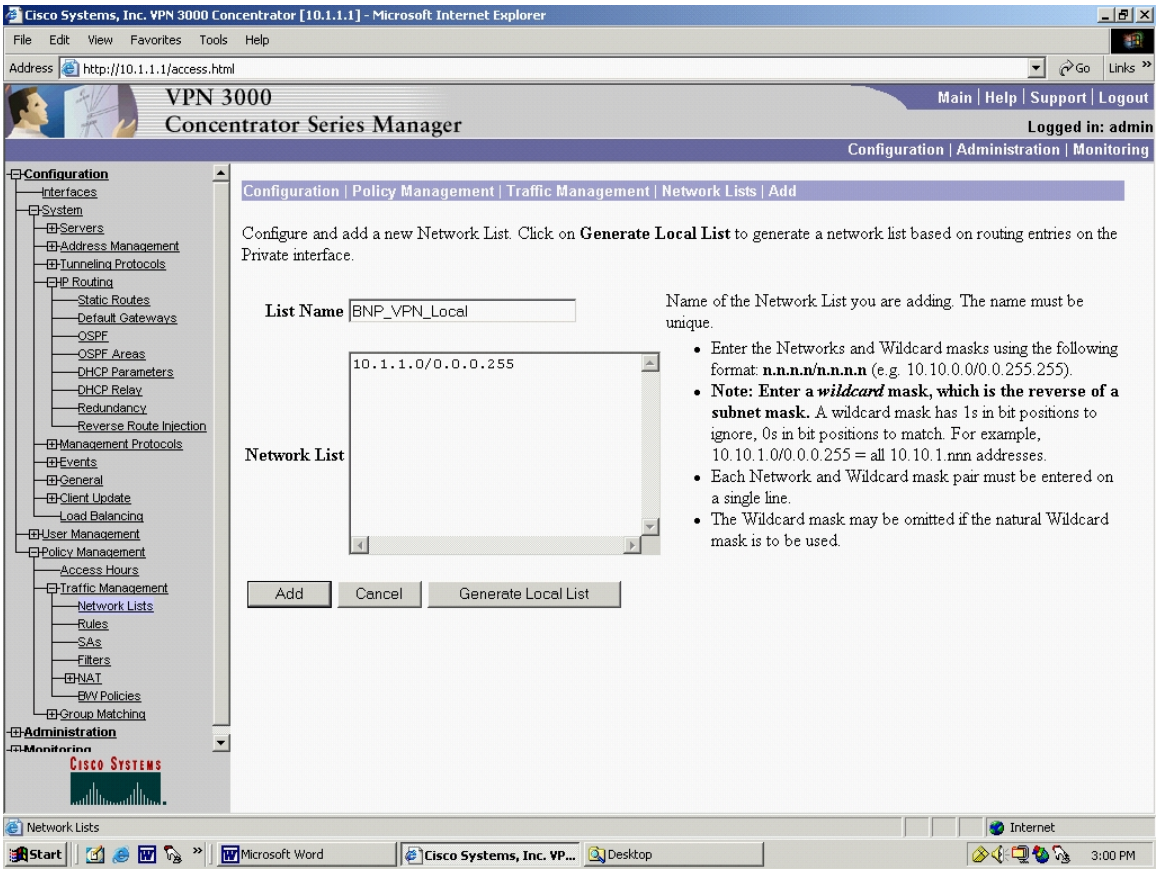

Figure 58. Concentrator Network List

Two network lists need to be added, one Local and one Remote. First add the Local network list. Similar to the Tunnel Default Gateway previously, enter the network where the encrypted traffic will originate from, in this case 10.1.1.0. Notice Cisco uses the wildcard notation, which is the one's compliment of the subnet notation (i.e., in wildcard notation, 0=match, and 1=ignore). The wildcard mask for /24 is 0.0.0.255. Click "Add" and the screen will return to the Network Lists screen, Figure 60. Click "New" and "Add" in the remote Network List. The resulting screen is hown, Figure 59.

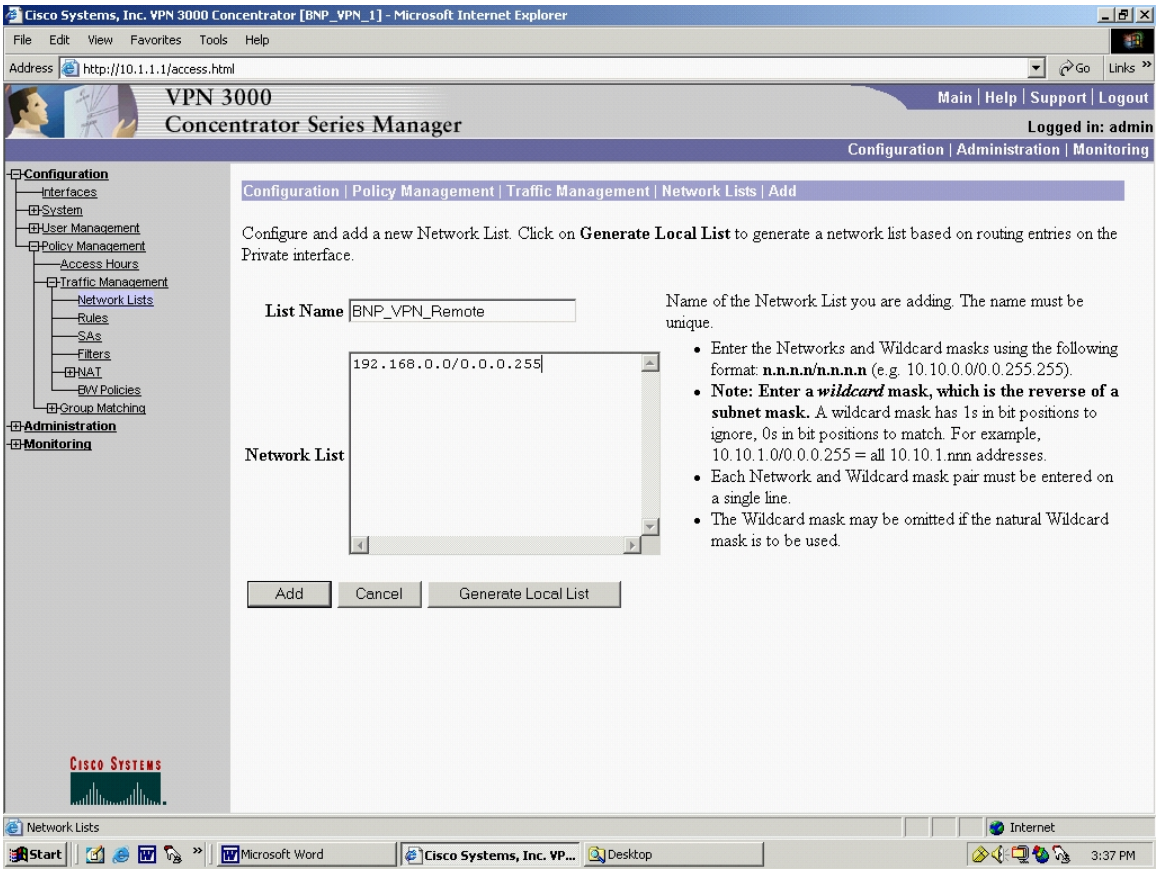

Figure 59. Concentrator Network List: Add

A final click on “Add” and the network will be added to the list, resulting in a the main Network Lists screen, where both Remote, Local, and Cisco generated default list exist, as shown in Figure 60.

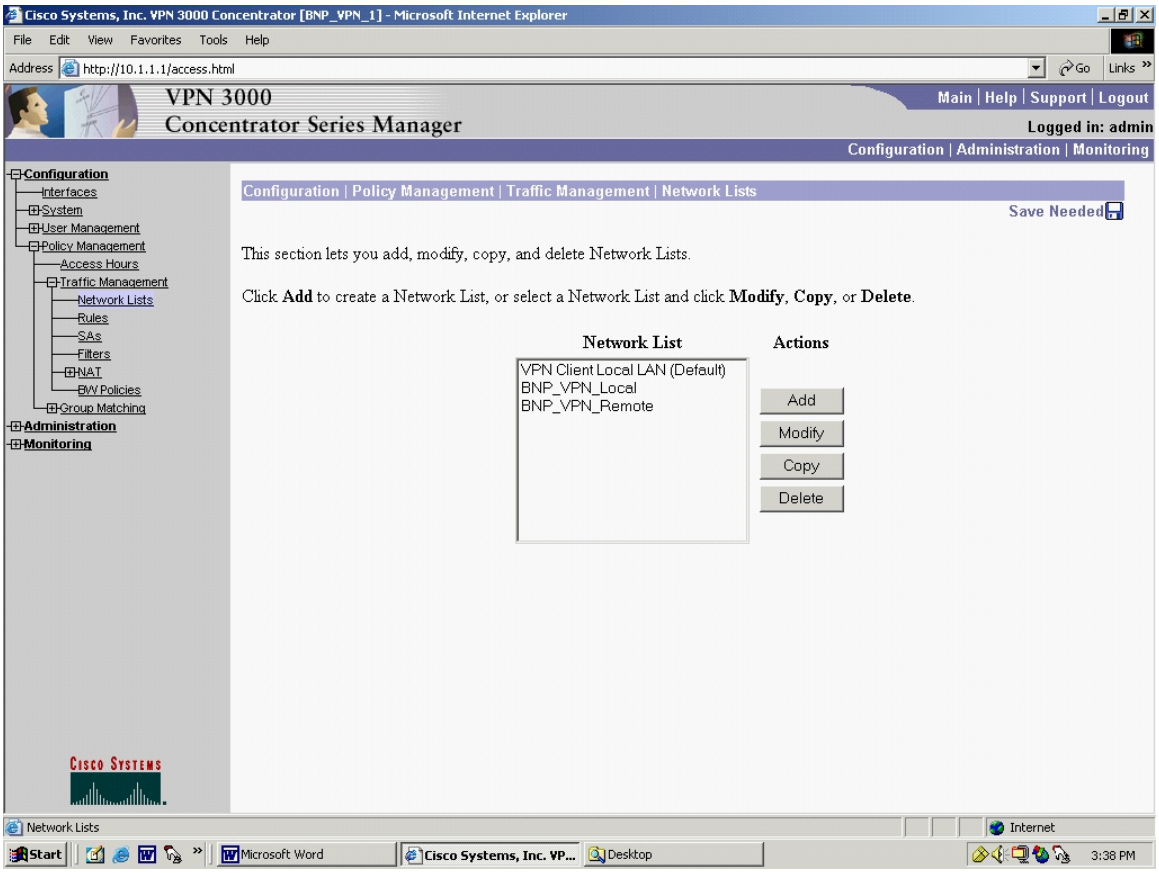

Figure 60. Concentrator Network List Added

Navigating via the left side menu tree, select Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN and click “Add”. The resulting screen is shown in Figure 61.

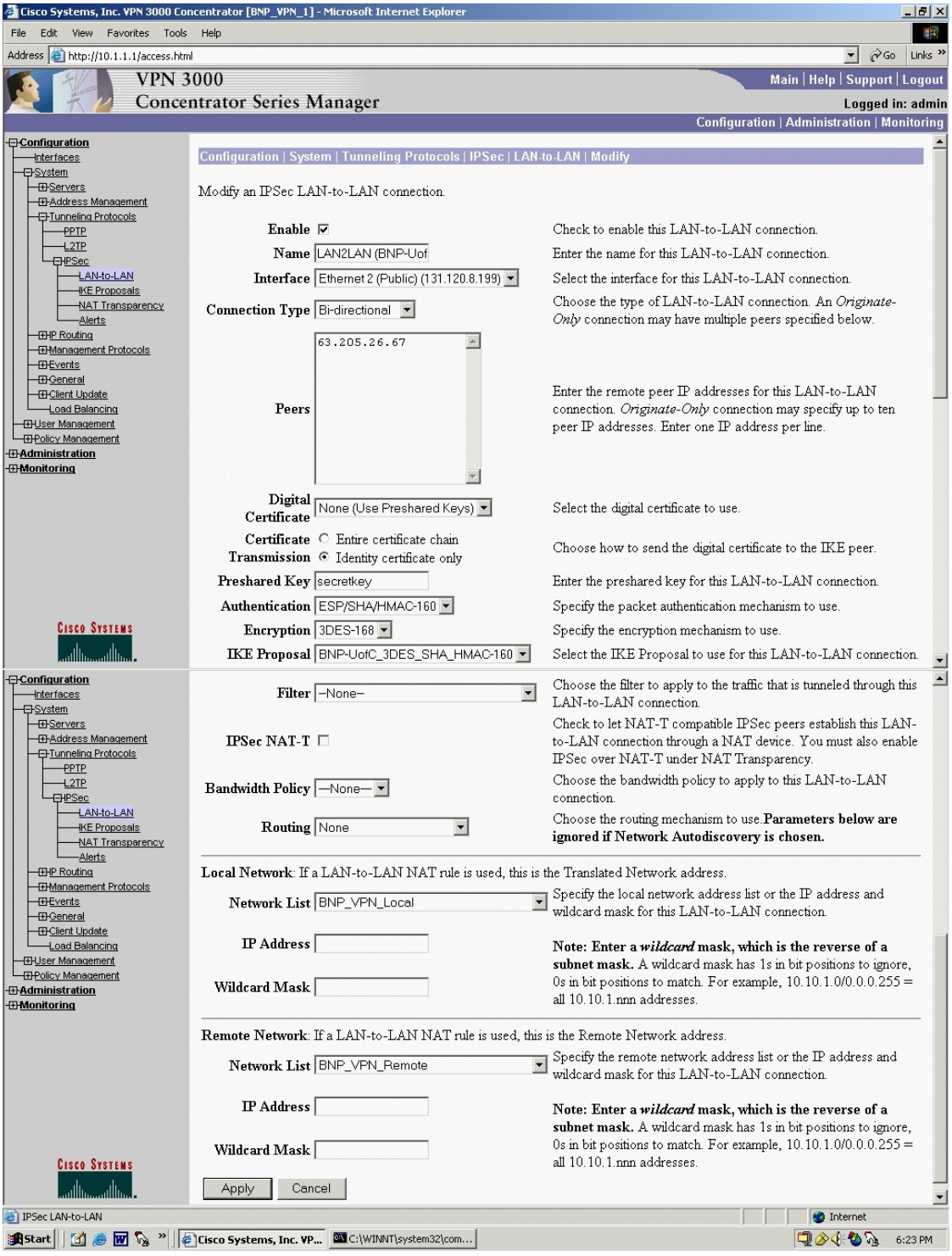

Figure 61. Concentrator IPSec LAN-to-LAN Add

Ensure that the appropriate entries are made. Entries are shown for the example network being built. Near the bottom of Figure 61, the two Network Lists

that were built in the previous step can be selected. Clicking “Add” results in the information screen being presented, as depicted in Figure 62.

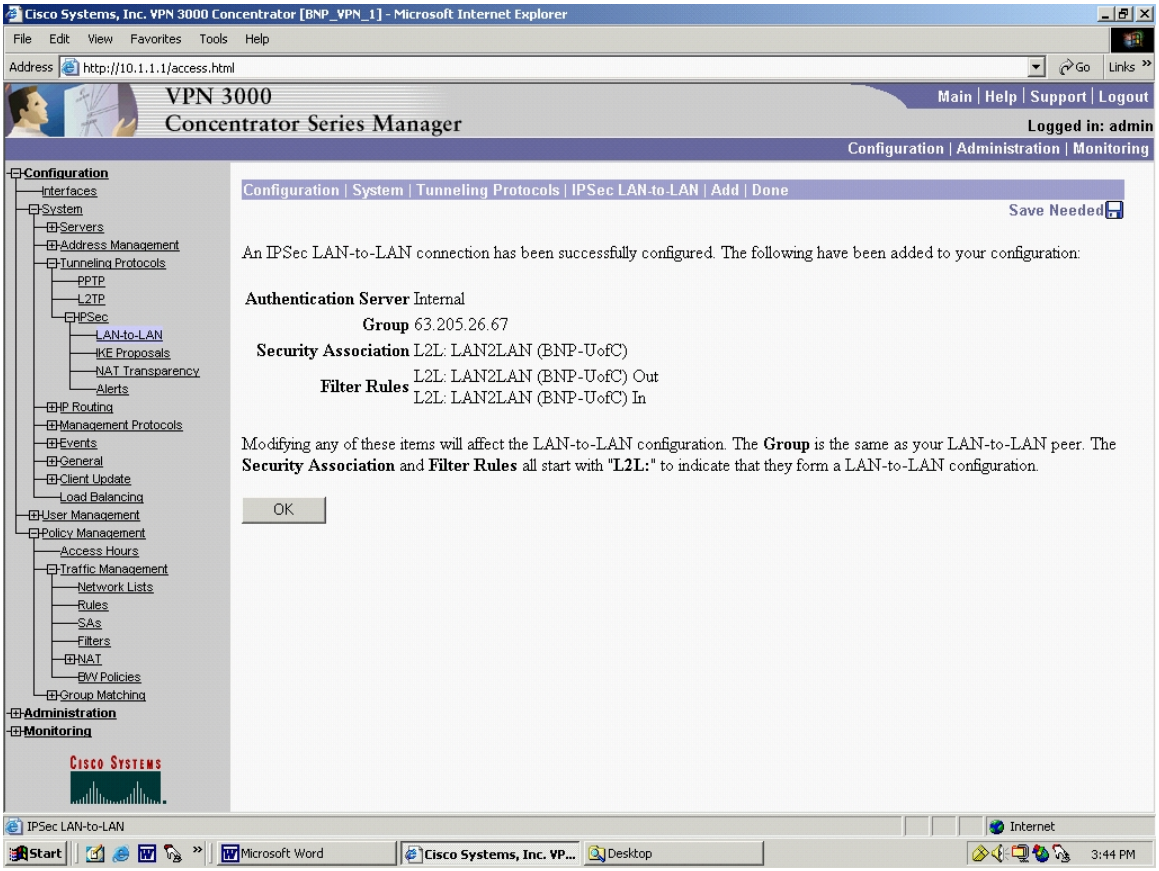

Figure 62. Concentrator IPSec LAN-to-LAN Configuration

Clicking “OK” results in the LAN-to-LAN connection that was just created being shown, Figure 63.

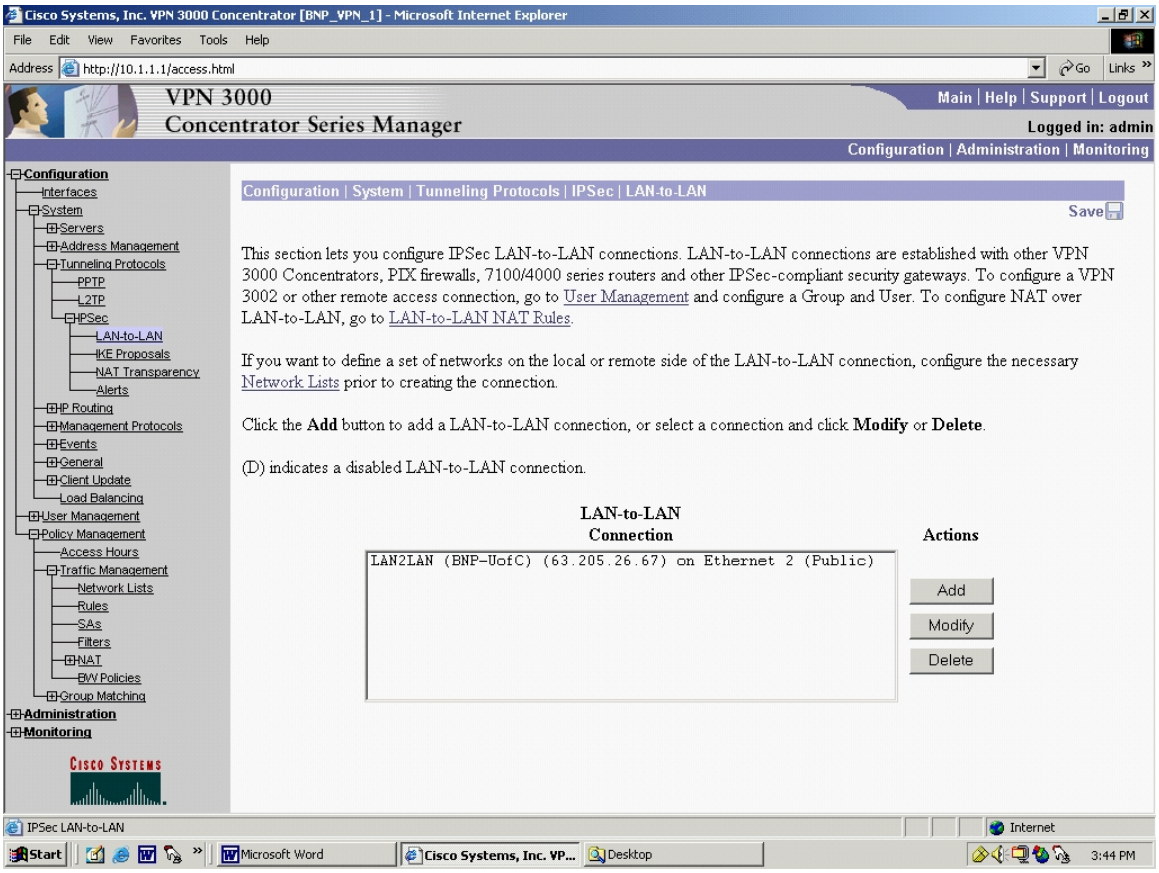

Figure 63. Concentrator IPSec LAN-to-LAN Added

Navigating via the left side menu tree, select Configuration | System | Tunneling Protocols | IPSec | IKE Proposals. The result is shown in Figure 64.

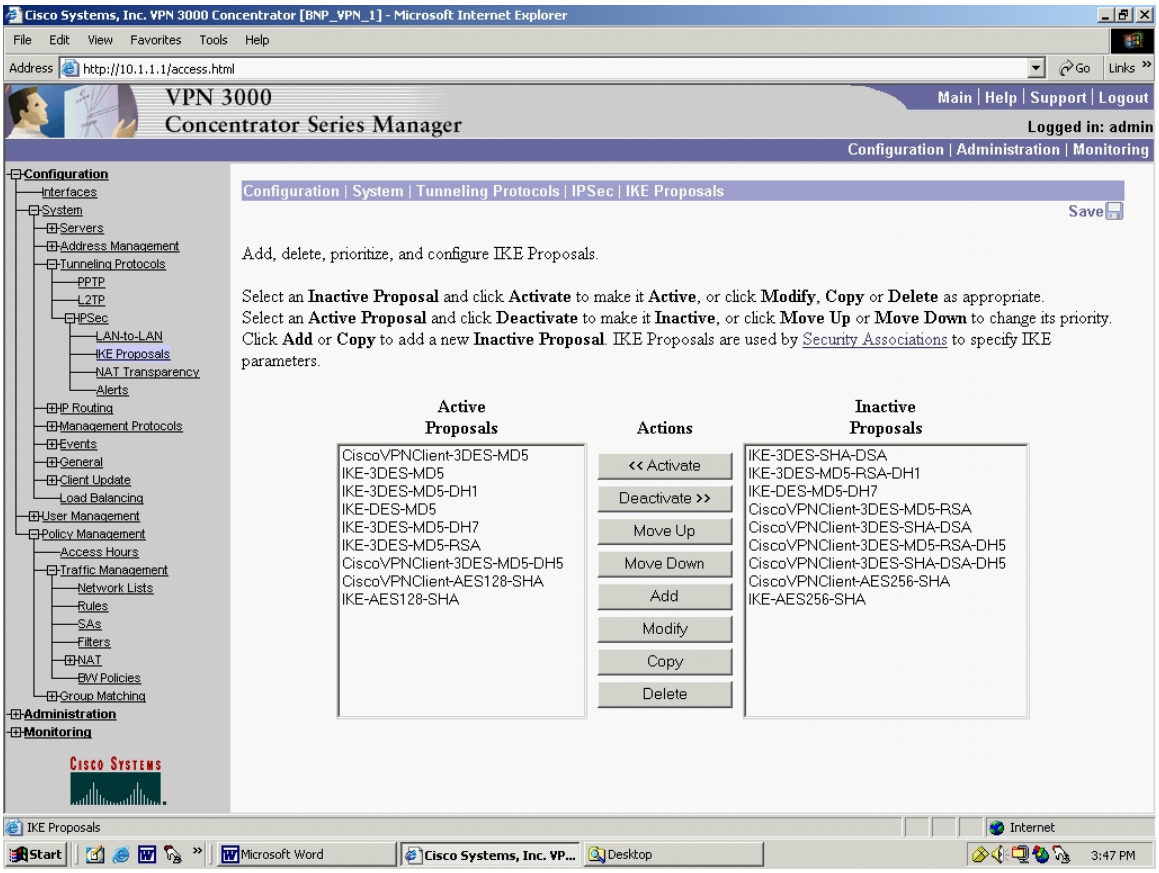

Figure 64. Concentrator IKE Proposals: Active/Inactive

Notice none of the Cisco preloaded selections offer the IKE Proposal that is needed, i.e. 3DES, SHA_1_HMAC_160, Group-2. Click "Add" to build an IKE proposal. The resulting screen is shown in Figure 65.

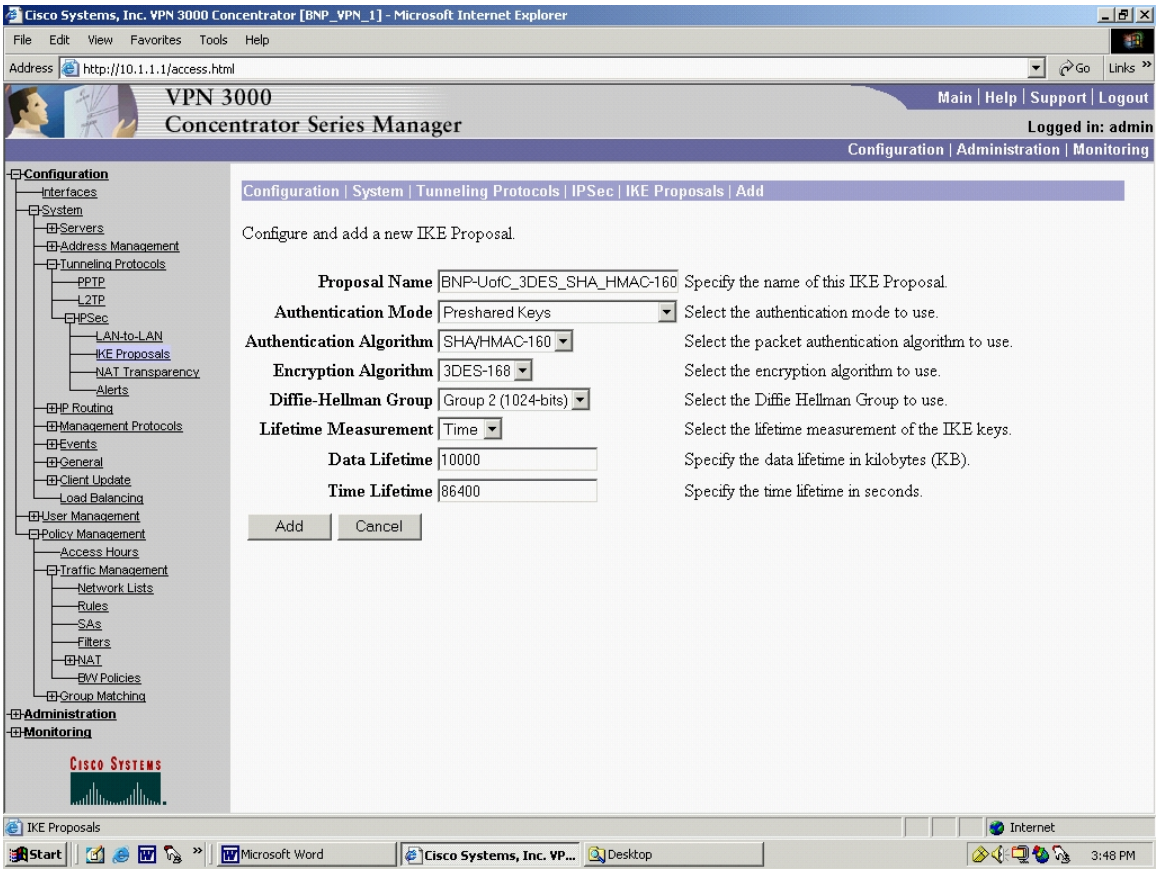

Figure 65. Concentrator IKE Proposals Add

Build the IKE proposal that is required, giving it a descriptive title. Click "Add". This will go back to the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen, Figure 66. The newly created IKE proposal is not active.

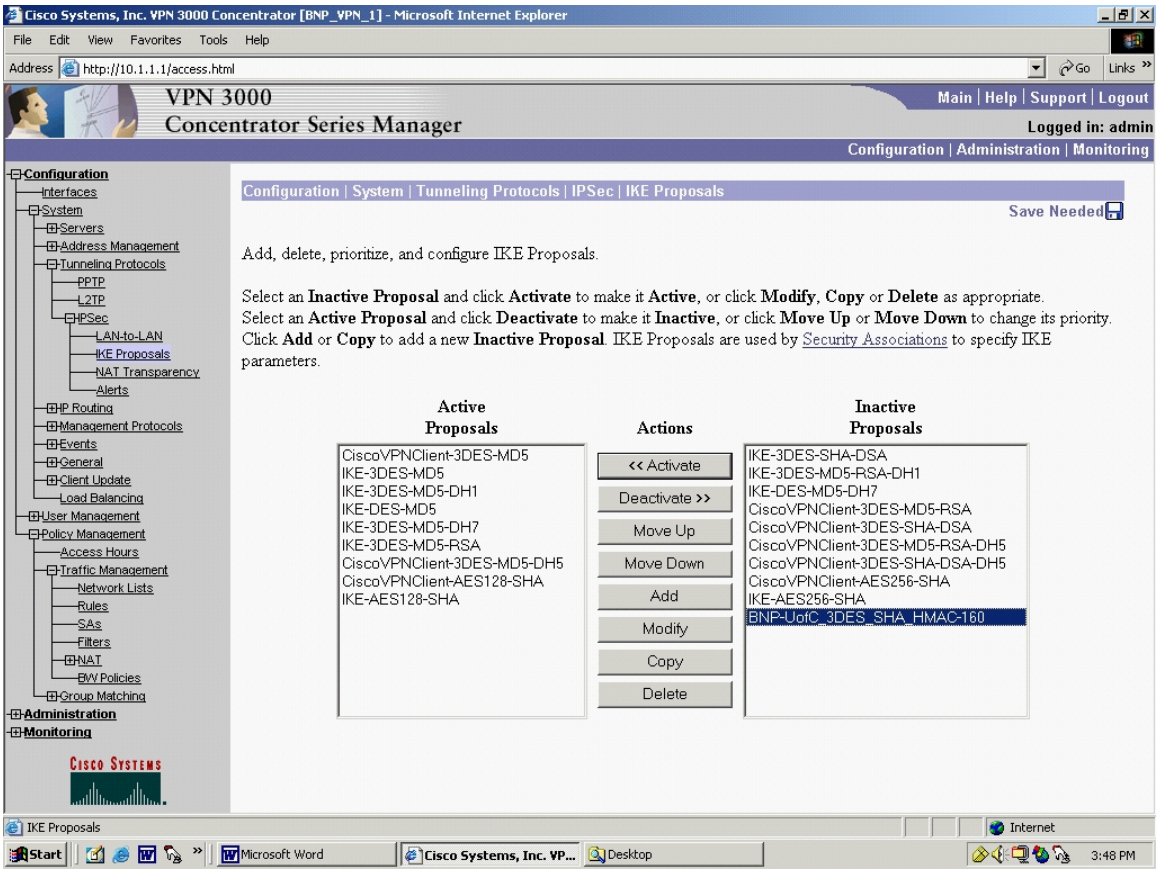

Figure 66. Concentrator IKE Proposal: Selected

To activate the newly created IKE proposal, highlight it and click "<<Activate" to move it to the Active Proposals. Move it to the top of the Active Proposals column by highlighting it again in the left pane and clicking "Move Up". The result is shown in Figure 67.

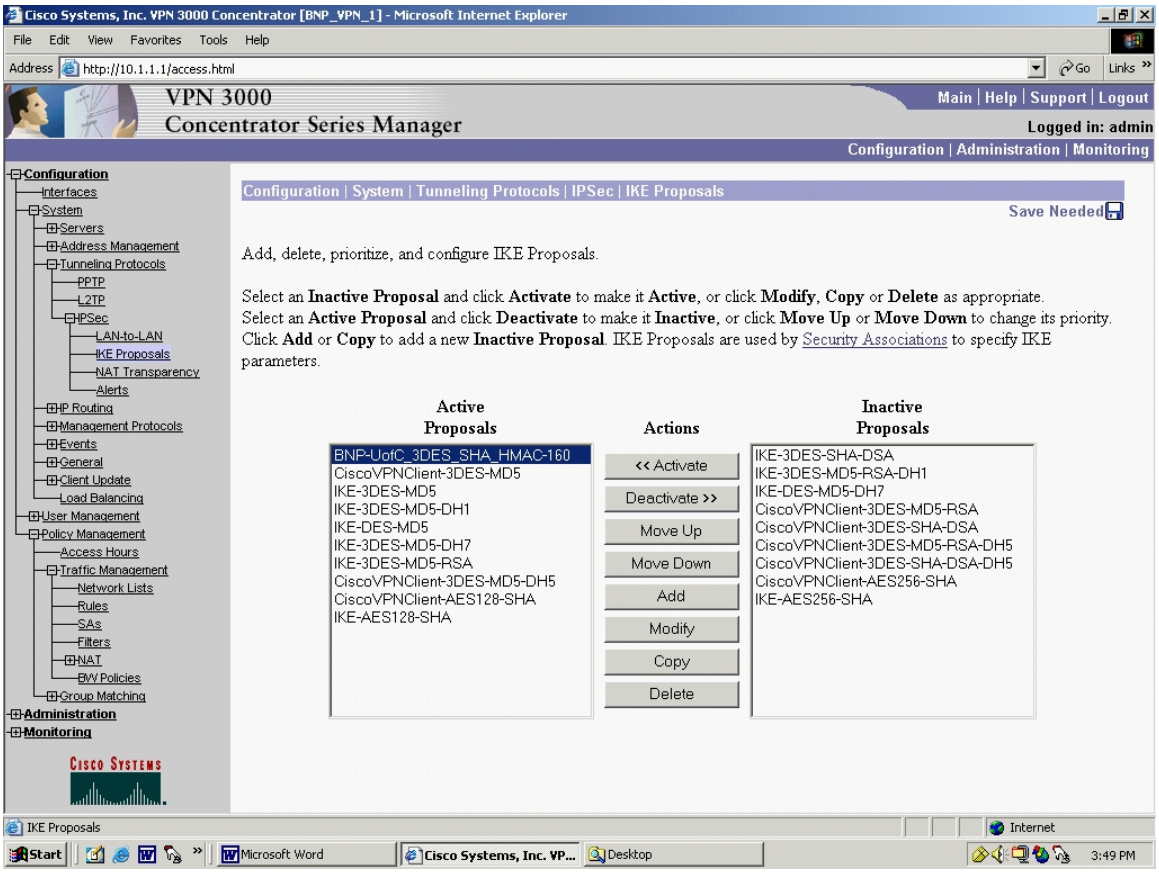

Figure 67. Concentrator IKE Proposal: Prioritized

Now, verify the IPSec Security Association.

An IPSec SA has already been automatically built from the information that has been entered. It is a good idea to verify that this automatically built SA meets the planned network's needs. Navigating via the left side menu tree, select Configuration | Policy Management | Traffic Management | Security Associations. Highlight the SA with the same name as the IKE proposal, and click "Modify". The result is shown in Figure 68.

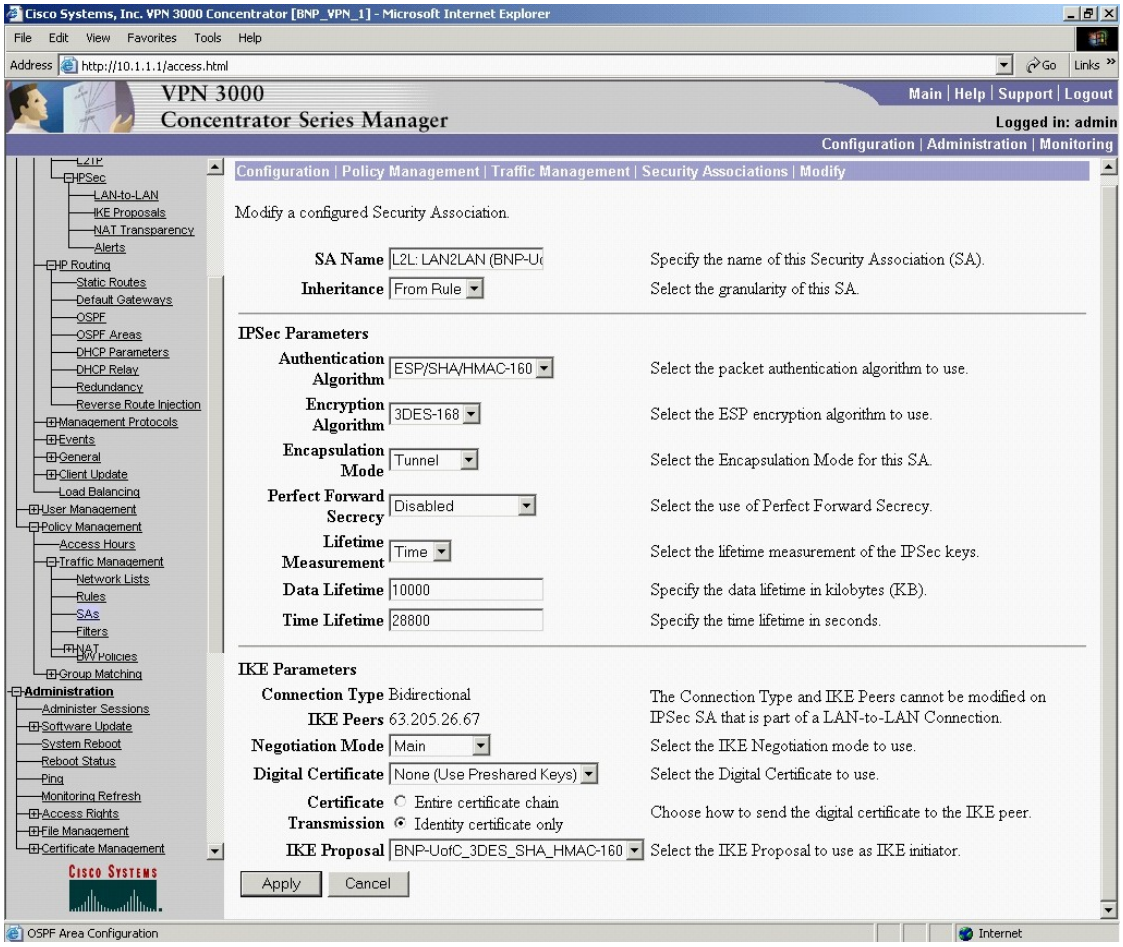

Figure 68. Concentrator Security Association Modify

Click “Add”. Observe that the SA has been added, Figure 69.

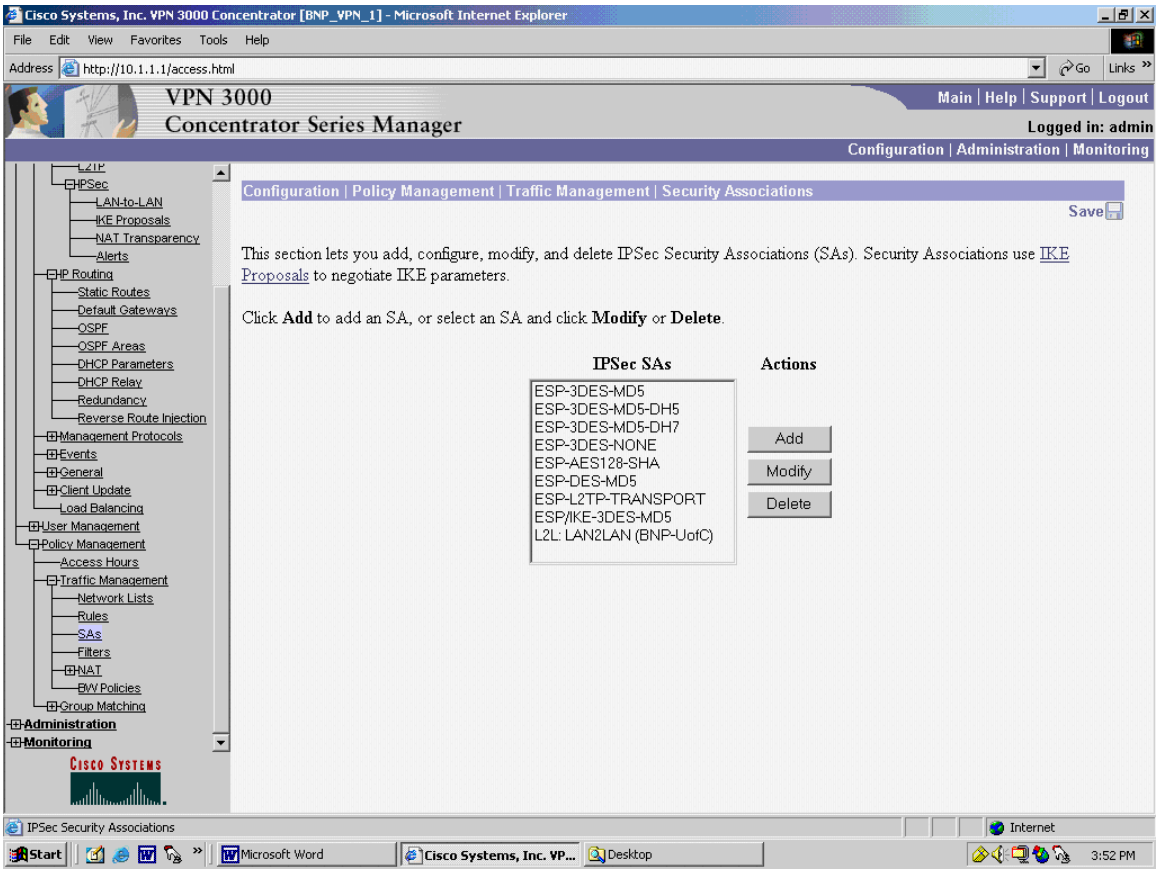

Figure 69. Concentrator Security Associations

D. DIGITAL CERTIFICATES

Digital certificates are an alternate way to provide authentication during IKE phase I. For the BNP, the NS Certificate Management System (NCMS) is used. Within the BNP, the NCMS information is listed in Table 23.

Type of CA server:	NCMS
IP address of the CA server:	10.1.13.2
Host Name:	MAAT.SILVERDRAGONS.BNP
URL (same as IP?)	https://maat.silverdragons.bnp:1027
CA administrator contact information:	ca@silverdragons.bnp

Table 23. NMCS Data Summary

1. Router to Router Use of Certificates Using CLI

To implement digital certificates in the router using the CLI, the commands listed Table 24 are used. Instead of using a pre-shared secret, a certificate is used in its place. The numbers on the left in Table 24 are the step numbers that correspond to the

step numbers in Table 14. In other words, where Table 14 has step one, additional steps are required, numbered in Table 24.

Step	NPS BNP_VPN Router Commands	Purpose
1a	BNP_VPN(config)#**crypto ca certificate query**	This is an optional step. This command tells the router not to store certificates and CRLs on the router, but to retrieve them from the CA. This will prevent the router's non-volatile random access memory (NVRAM) from filling up with certificates and CRLs.
1b	BNP_VPN(config)#**clock timezone pst -8** **clock set hh:mm:ss dd month yyyy**	Since certificates are time sensitive, it is essential that the router date, timezone, and time be set accurately. Cisco routers use military time, and month by name (e.g. January).
1c	BNP_VPN(config)#**ip domain-name silverdragons.bnp**	Tells the Cisco IOS how to complete unqualified host names.
4a	BNP_VPN(config)#**crypto key generate rsa** How many bits in the modulus [512]: **512**	Generates a general purpose key consisting of one pair of RSA keys. After the prompt, the desired modulus is entered. The default is 512 bits. According to Cisco documentation, it will take a 2500 Series router 20 seconds to generate RSA keys using 512 bit modulus. A larger modulus will result in longer key generation times. The NCMS is capable of generating certificates for keys up to 2048 bits long.
4a	BNP_VPN(config)#**Crypto ca identity LocalNameYouChoose**	Declares what CA the router will use. This is only used locally. It does not have to match the CA identity used by the VPN peer. Notice this enters the crypto CA identity mode.
4b	BNP_VPN(ca-identity)#**enrollment url https://maat.silverdragons.bnp:1027**	Specifies the URL of the CA and tells the router where to go to enroll the VPN endpoint.
4c	BNP_VPN(config)# **Crypto ca crl request LocalNameYouChoose**	Tells the router the location where the CRL will be downloaded. Use the same name for the CA as was used in step 1c above.
4d	BNP_VPN(ca-identity)#**crl optional**	An optional command. Allows router to accept other peers' certificates if the CRL is not accessible.

Step	NPS BNP_VPN Router Commands	Purpose
4e	BNP_VPN(config)#**crypto ca authenticate LocalNameYouChoose** Fingerprint: (example) 3D:9C:E1:BB:34:5F:8H:9G:4C:7G:3S:7G:3E: 9B:6C:4N % Do you accept this certificate? [yes/no]: **Y**	This command allows the router to authenticate the CA to ensure the CA is valid. Use the same name for the CA as was used in step 1c above. The router was already told where the CA is located (above). Since the CA certificate is self-signed, the CA's public key should be obtained out of band and manually compared to the fingerprint generated.
4f	BNP_VPN(config)#**crypto ca enroll LocalNameYouChoose**	This command requests certificates from the CA for all the router's RSA key pairs that were generated in line 4a. In Cisco, the two events of enrolling and obtaining certificates are both set in motion with the "crypto ca enroll" command. A password prompt will occur. This password will be used by the CA administrator to authenticate this router in the future.

Table 24. Router CLI Commands for Certificates

2. Using the Certificate

These commands have requested, generated, and installed the certificate(s). Now, instead of using pre-shared secret, the router can use certificates.

In the BNP router table, Table 14, two steps in the sequence of commands to configure IKE change. In step four, instead of "pre-share", use rsa-sig, i.e. the line

```
BNP_VPN(config-isakmp)#authentication pre-share
```

becomes

```
BNP_VPN(config-isakmp)#authentication rsa-sig
```

In step seven, the following line is not needed:

```
BNP_VPN(config)#crypto isakmp key 12345 address 63.205.26.67
```

Revoke that step using the "no" command, i.e.

```
BNP_VPN(config)#no crypto isakmp key 12345 address 63.205.26.67
```

At this point, the VPN endpoint routers will use the certificates for authentication instead of the pre-shared secret.

3. Router to Router Use of Certificates using SDM

Unfortunately, the Cisco SDM does not provide CA support.

4. VPN 3005 Concentrator Use of Digital Certificates

Very similar steps are followed to utilize certificates with the 3005 Concentrator so no further details are provided here. During its initial setup, the router already had the clock and time zone set and the IP domain name has been given. This was shown earlier in this Chapter.

5. Identify a Certificate Authority (CA)

Certificate usage with the 3005 begins with the Certificate Management page. From the left side menu tree, select Administration | Certificate Management:

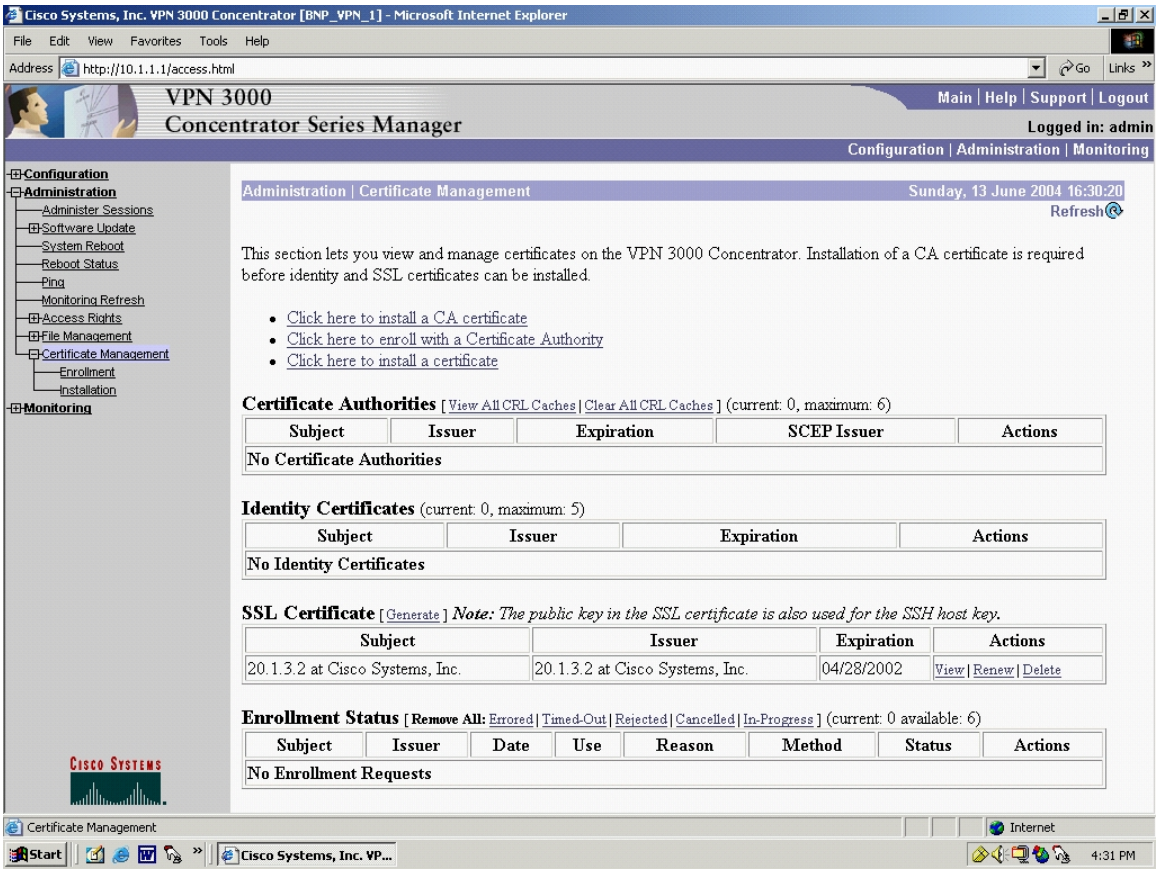

Figure 70. Concentrator Certificate Management

Options to install certificates and enroll the 3005 with a CA are shown, Figure 70. The 3005 supports both manual and automatic certificate installation. The manual method will be discussed first. This discussion will continue and will include the use

of the certificate in the example VPN. Once the reader has a good idea of this process and how it works, the automatic registration and installation of certificates, via SCEP, will be covered.

6. Generate Keys and Enrollment

The first step the 3005 needs to have completed is the installation of the CA certificate. To do this manually, click on the "Click here to install CA certificate" in Figure 70. This brings up the Administration | Certificate Management | Install | CA Certificate screen, shown in Figure 71.

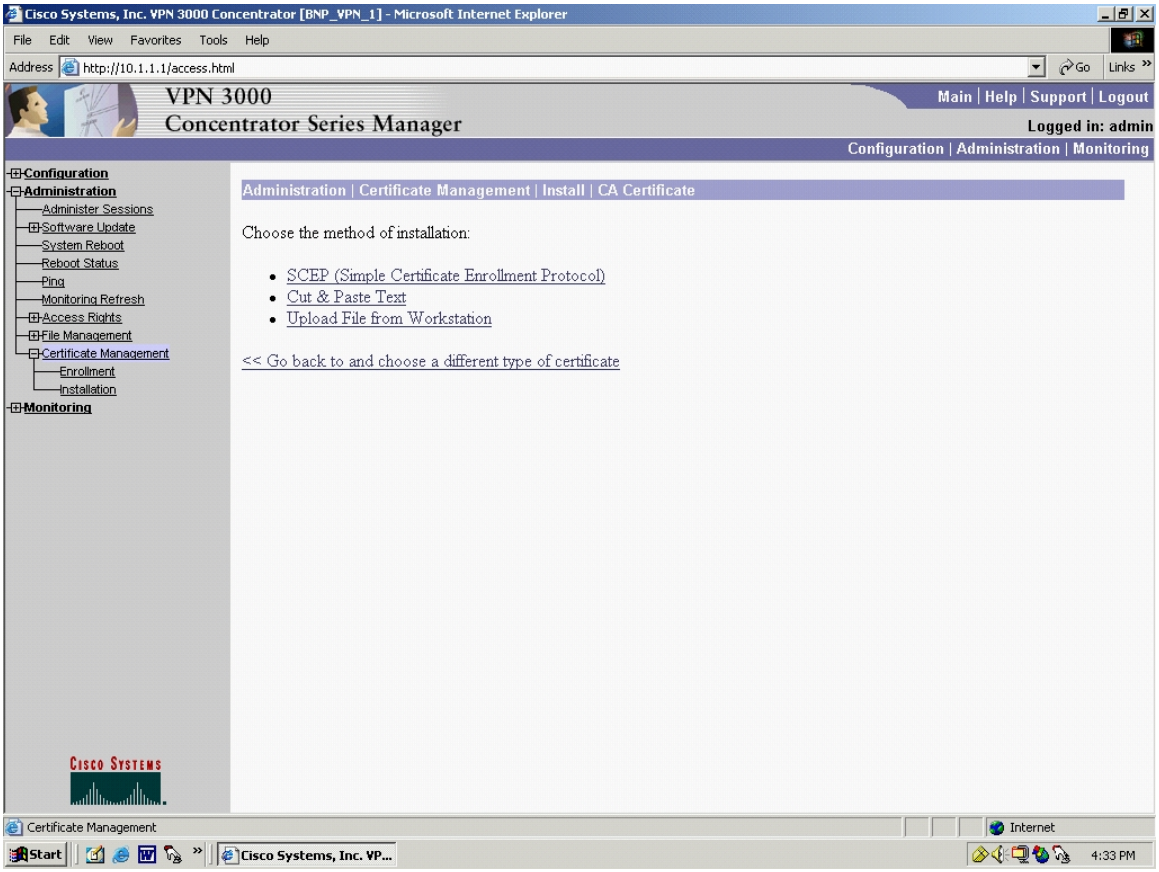

Figure 71. Concentrator CA Certificate: Install

This screen allows 3 methods of installing the CA certificate.

The first way to install a CA certificate would be automatically. Click "SCEP (Simple Certificate Enrollment Process)". This brings up the Administration | Certificate Management | Install | CA Certificate | SCEP, Figure 72.

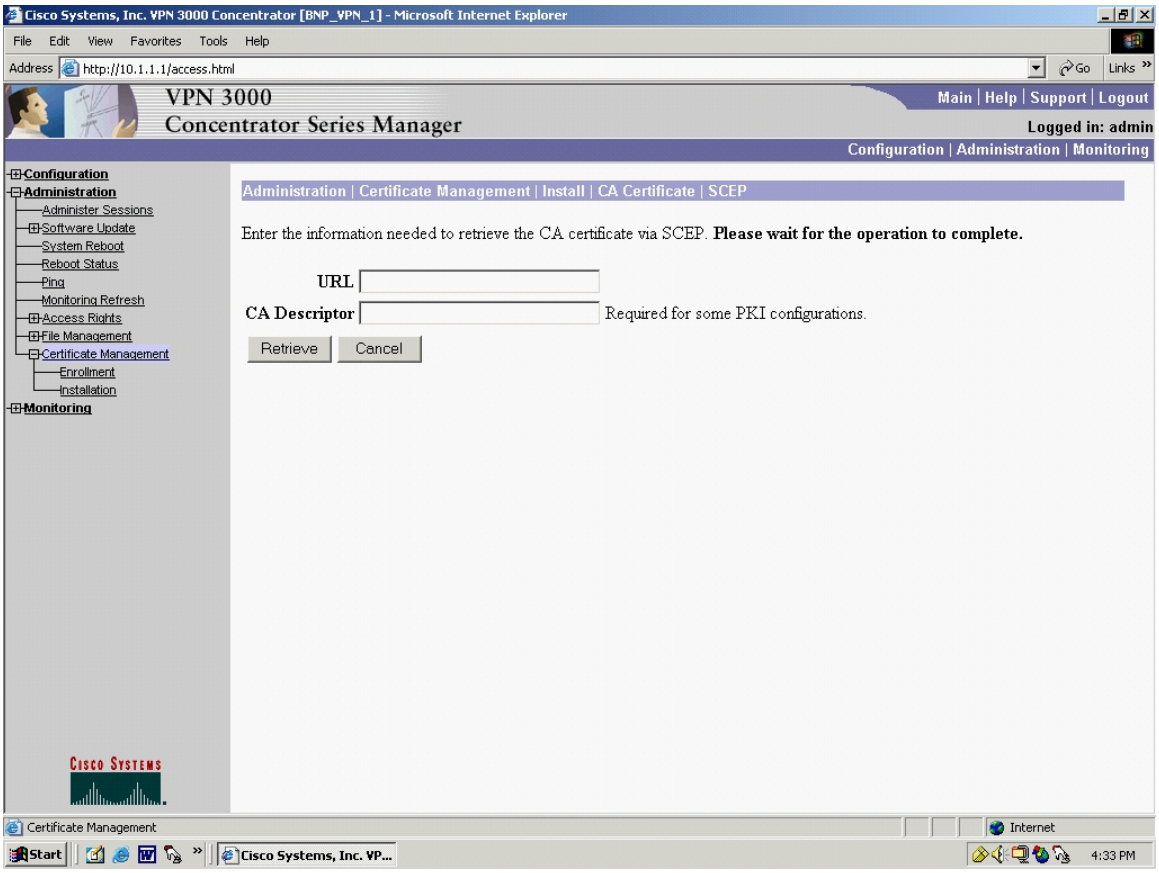

Figure 72. Concentrator CA Certificate SCEP

Enter the URL and CA Descriptor and hit “Retrieve”. Via SCEP, this will retrieve and install the CA certificate. It is important that this step be accomplished in order to access the rest of the SCEP process.

Currently in this thesis, the automated process of integrating a VPN with a CA server is not implemented. The follow-on SCEP screens can not be illustrated. However, manual CA certificate generation via the BNP Netscape Certificate Management System (NCMS) was accomplished, and the manual process will be shown. The reader will realize that the automatic SCEP screens are very similar to the manual screens shown in Figures 73 through Figure 85.

A CA certificate was generated manually via NCMS. This CA certificate was then passed out of band, via a floppy disc, to be used by the 3005. This CA certificate allows certificate functionality with the Cisco 3005 VPN Concentrator.

To take a look at the manual process, the user would first need to go out of band and obtain the CA certificate, either as a *.cer file, or in the form of text. A CA certificate ca.cer file was generated by the BNP NCMS.

For the manual process, go to the Administration | Certificate Management | Install | CA Certificate screen, Figure 71. There are two options.

If Cut and Past Test is selected, this brings up the Administration | Certificate Management | Install | CA Certificate | Cut & Paste Text screen, Figure 73.

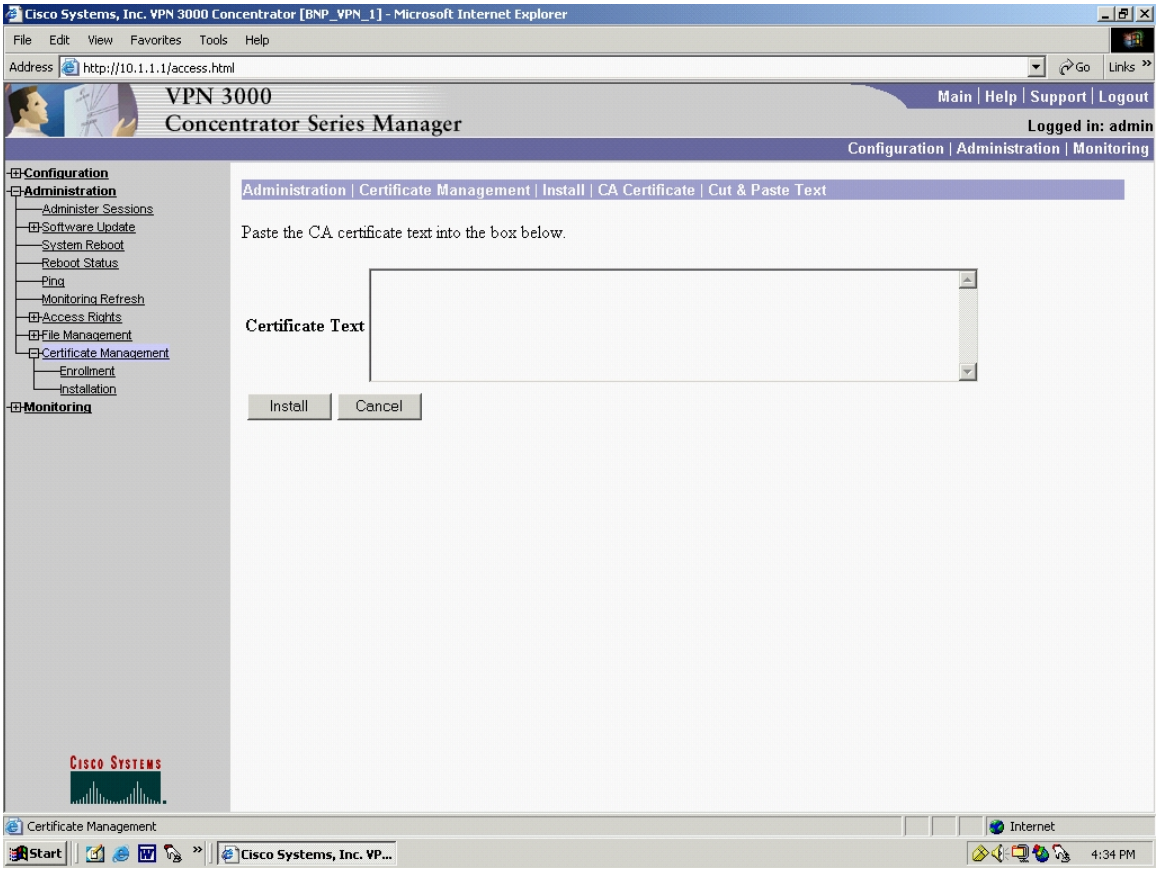

Figure 73. Concentrator CA Certificate Text: Cut and Paste

The user would enter the certificate information here, preferably by cut and paste to avoid typographical errors, and click “Install”.

The other option is to access the out of band CA certificate via the ca.cer file that is generated by the NCMS. Access the Administration | Certificate Management | Install | CA Certificate | Upload File From Workstation screen, Figure 74.

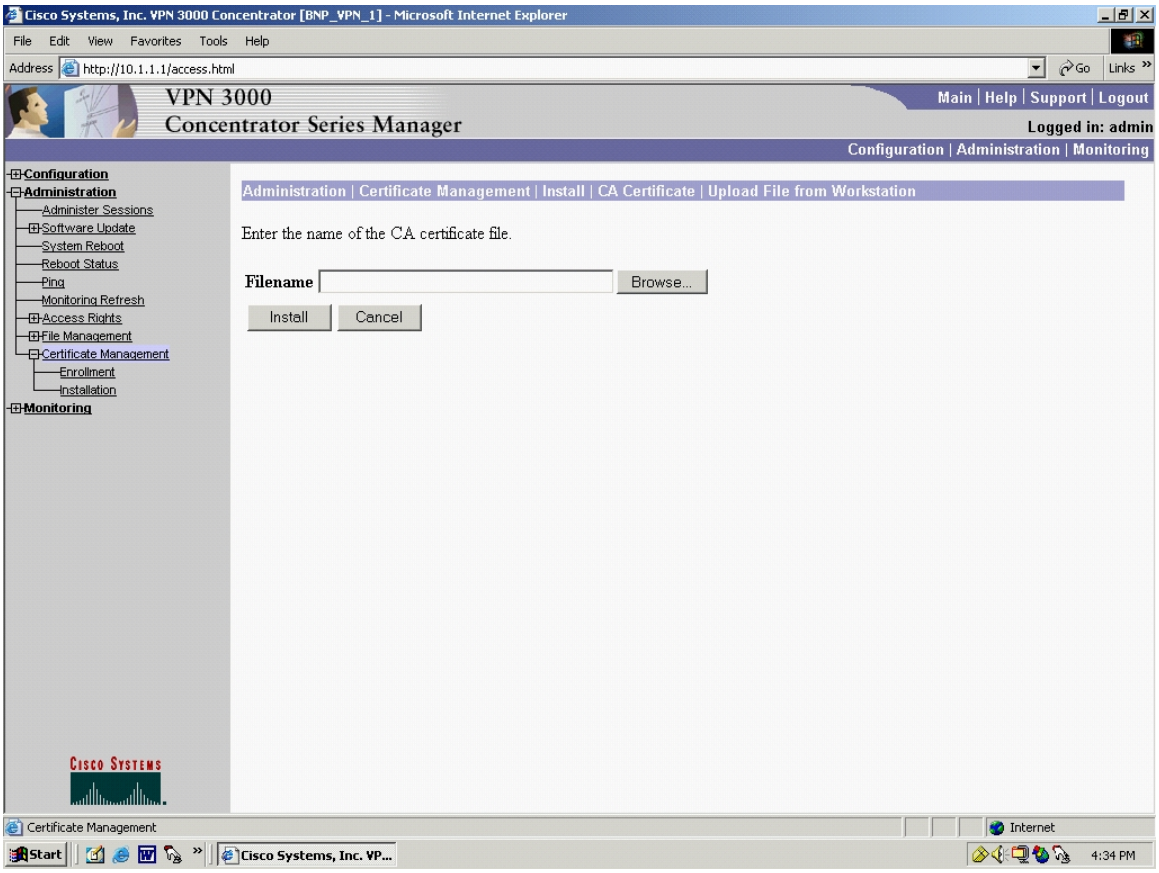

Figure 74. Concentrator CA Certificate: Load from File

Click Browse and find the filename on the floppy drive of the host computer being used to configure the 3005. The pop-up window is shown in Figure 75.

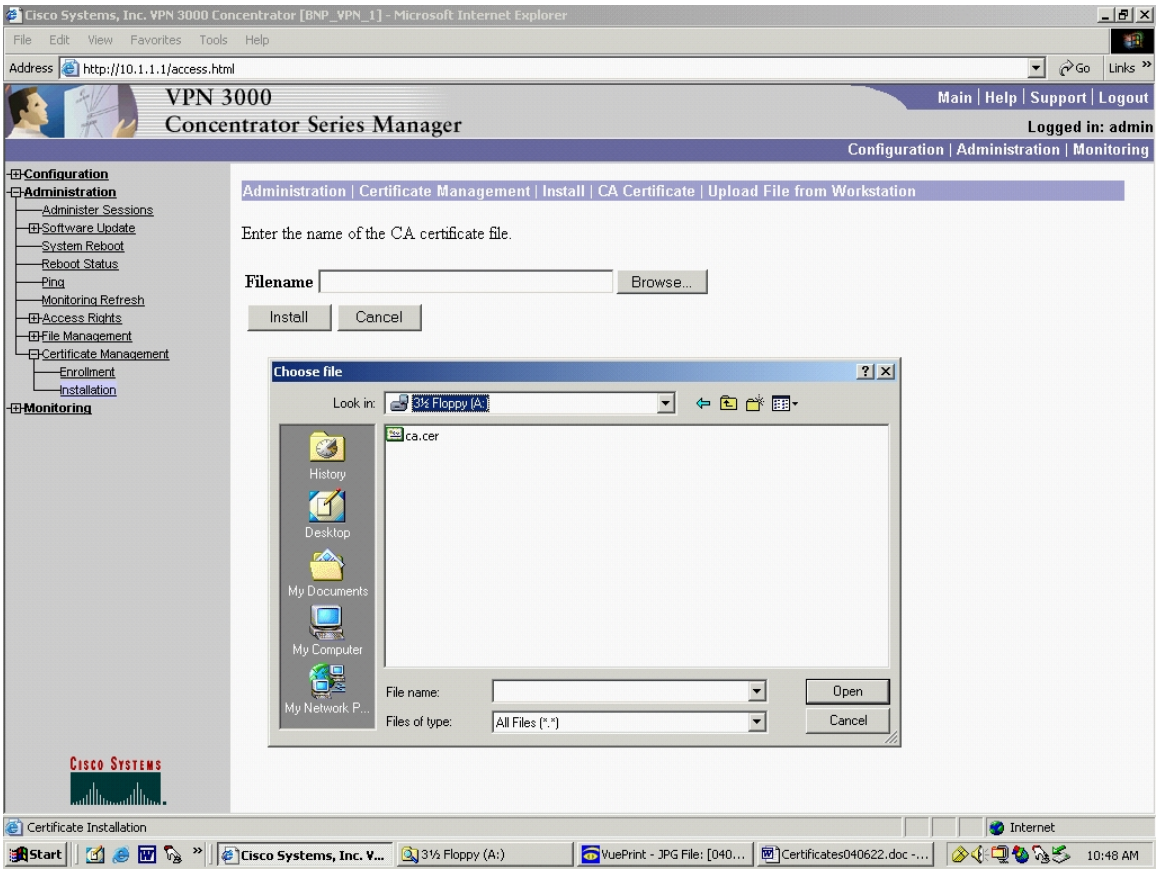

Figure 75. Concentrator CA Certificate: Upload

In Figure 75, select the certificate and click “Open”. This loads the file path of the ca.cer into the 3005. Then click “Install”. This installs the CA Certificate and automatically brings up the Administration | Certificate Management screen, Figure 76, which unlike the previous Figure 70, now shows the CA Certificate installed:

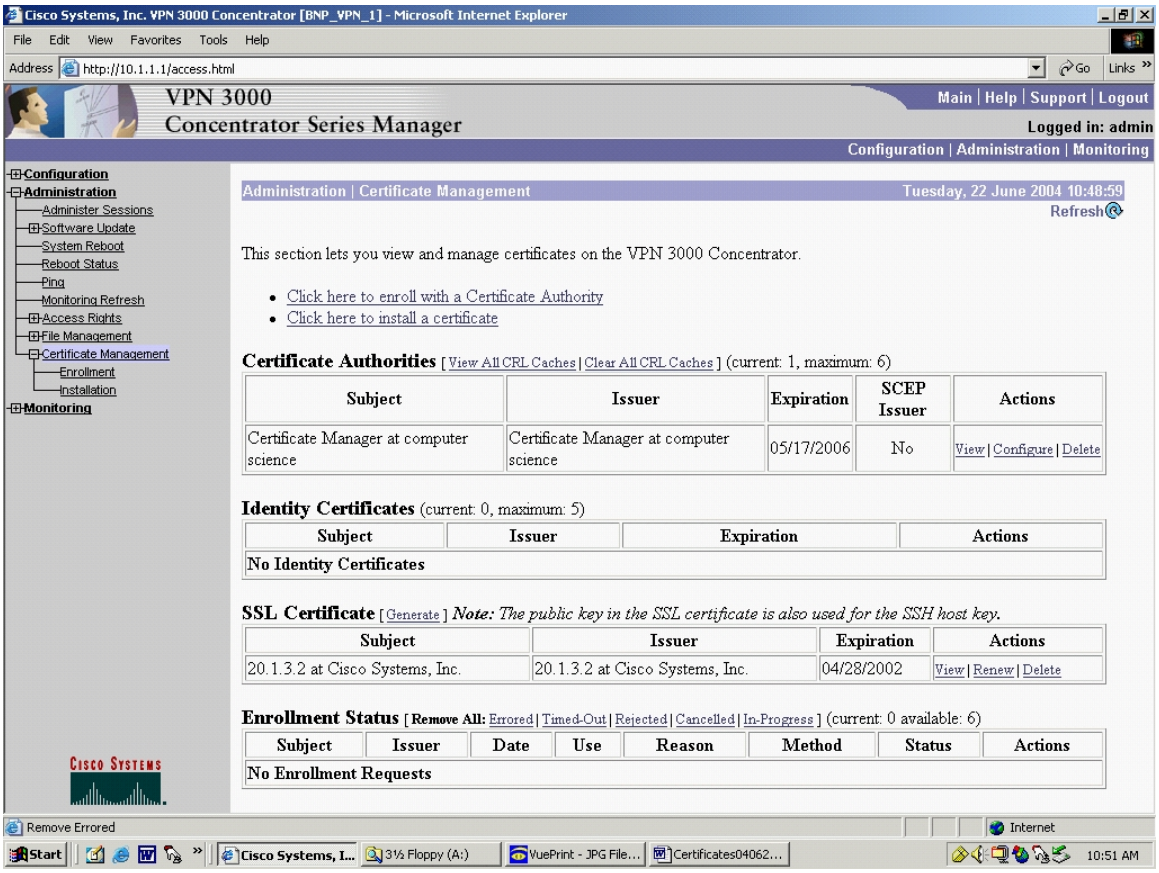

Figure 76. Concentrator Certificate Management

Clicking on the hotlink “view” allows the user to view the certificate as shown in Figure 77.

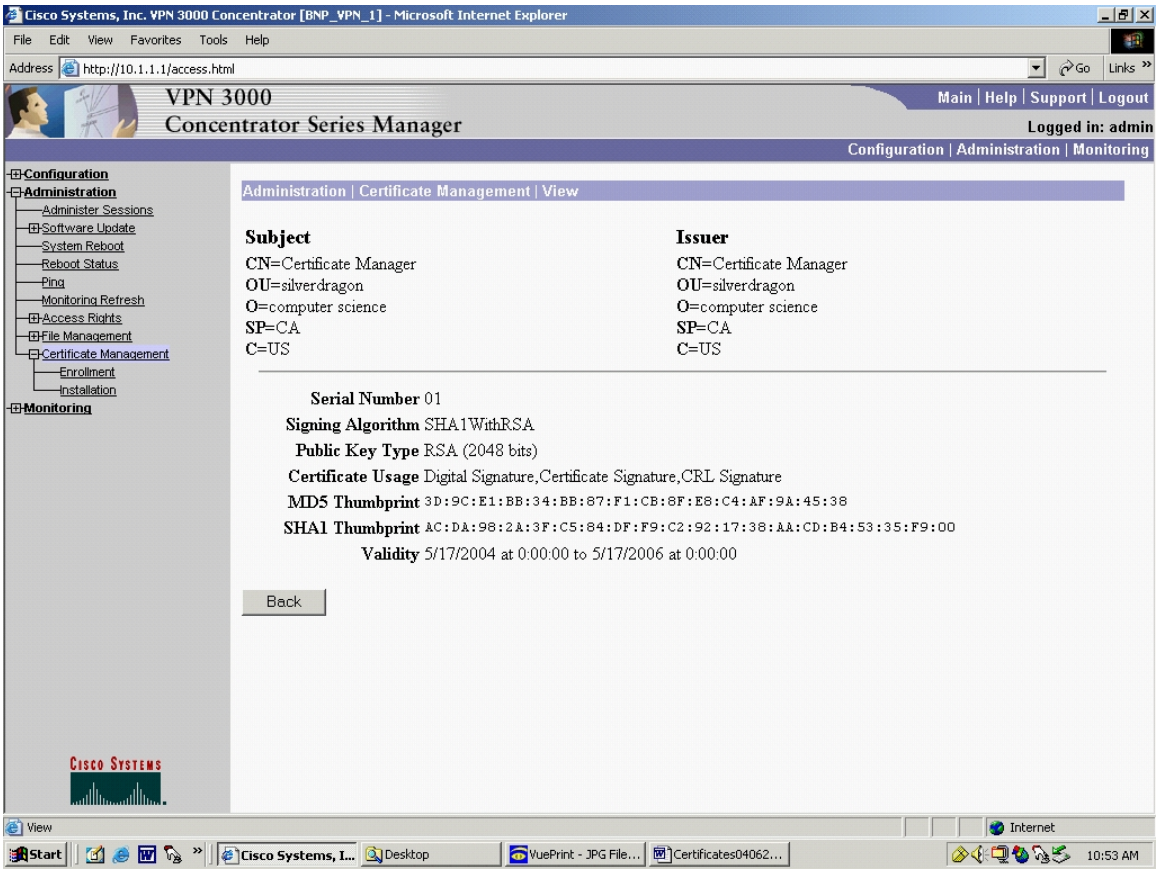

Figure 77. Concentrator Certificate Management View

Now, generate the identity certificate PKCS10 request. Cisco has chosen to combine the execution of the next two steps of the six-step certificate process, Generation of Keys and the Enrollment Process. Access the Administration | Certificate Management | Enrollment screen, Figure 78.

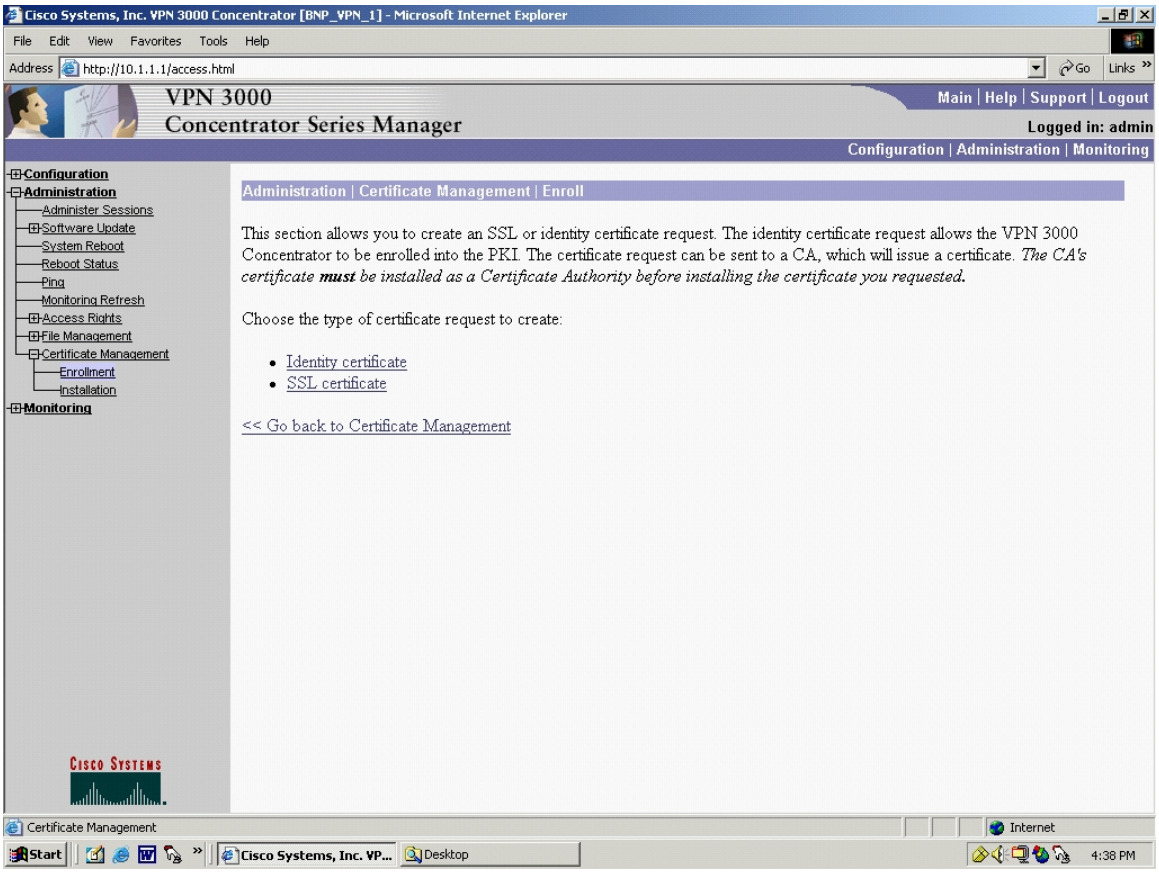

Figure 78. Concentrator Certificate Management Enroll

Click "Identity Certificate" to access the Administration | Certificate Management | Enroll | identity certificate screen, Figure 79. Note the options available in Figure 79. Figure 79 shows the user that to automatically generate an identity certificate with SCEP, the CA certificate must have also been installed with SCEP. In this example, the CA certificate was not installed with SCEP. Recall the CA certificate was installed manually. Hence, in Figure 79, only the following manual option is shown.

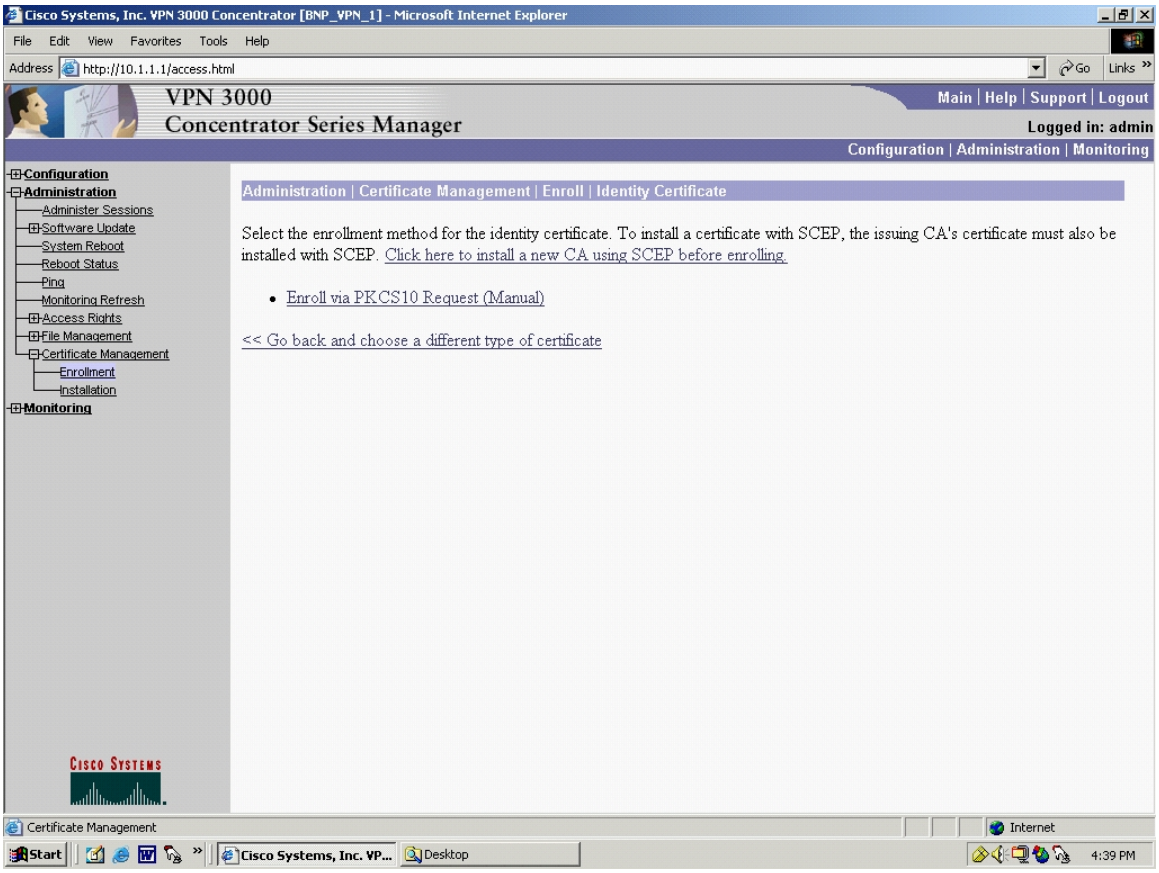

Figure 79. Concentrator Certificate Management Identity Certificate

If a CA certificate had been installed via SCEP, Cisco manuals show there are two additional hotlink options that appear:

Enroll via SCEP at MSCAsvr02

Enroll via SCEP at MSCAsvr05

In order to see these options, the user would have to install the CA certificate via SCEP, i.e. follow the “Click here to install a new CA using SCEP before enrolling” hotlink in Figure 79 and end up on the Administration | Certificate Management | Install | CA Certificate | SCEP screen, Figure 72, where the URL is entered.

However, to continue with the manual process, click the hotlink “Enroll via PKCS10 Request (Manual)” in Figure 79 and access the Administration | Certificate Management | Enroll | identity certificate | PKCS10 screen, depicted in Figure 80.

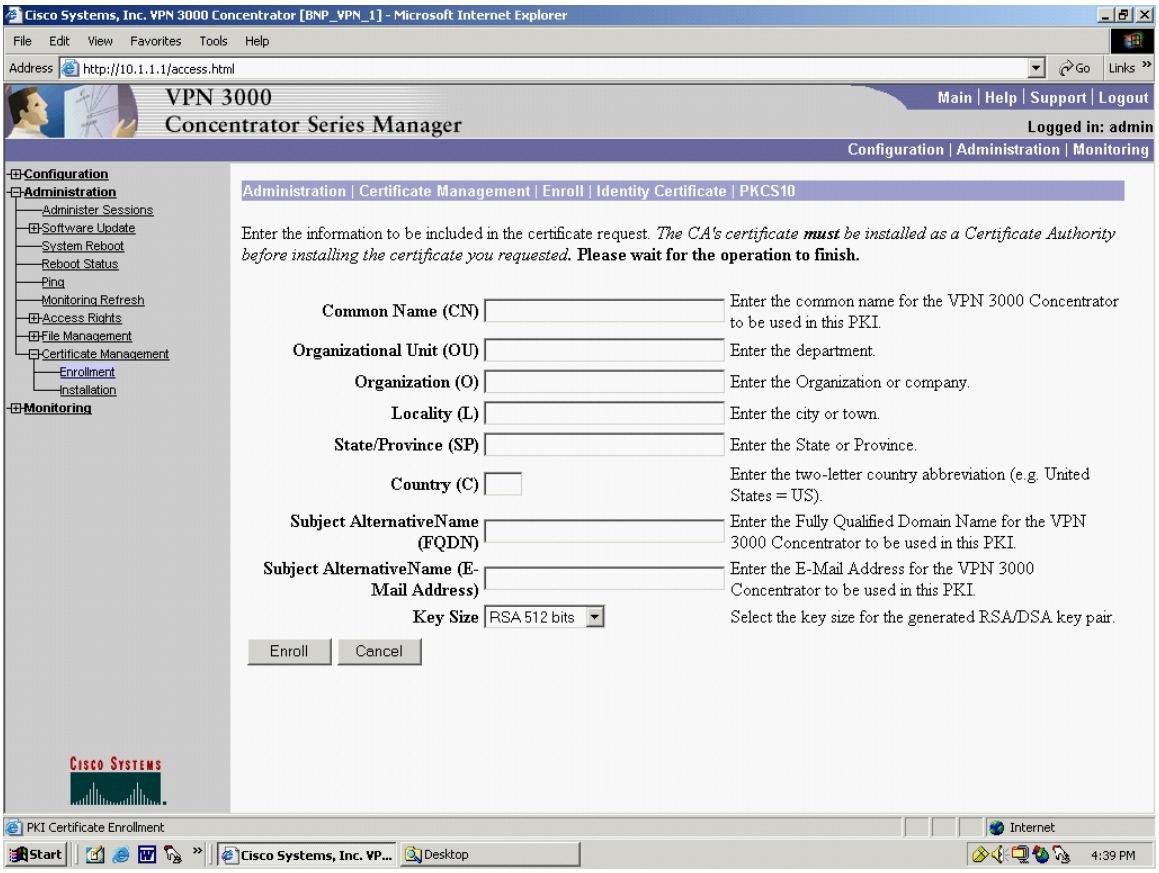

Figure 80. Concentrator Certificate Management Enroll via PKCS#10

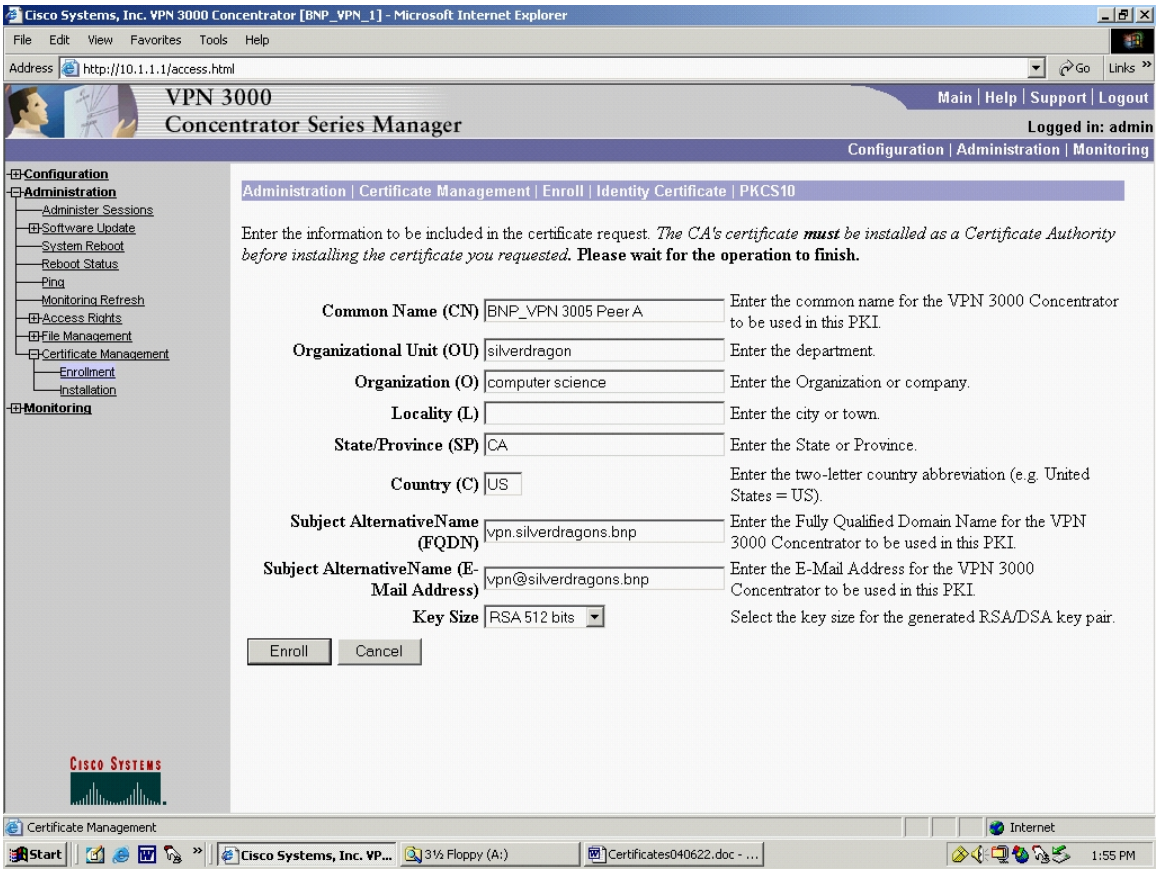

Figure 81. Concentrator Certificate Management PKCS#10

Figure 81 is the PKCS #10 request form and combines the Key Generation step and the Enrollment step into one. Enter all required information, including the Key Size. When "Enroll" is pressed, the 3005 will generate public-private RSA keys and, since this is a manual process, the 3005 will generate the PKCS#10 request, shown in Figure 82.

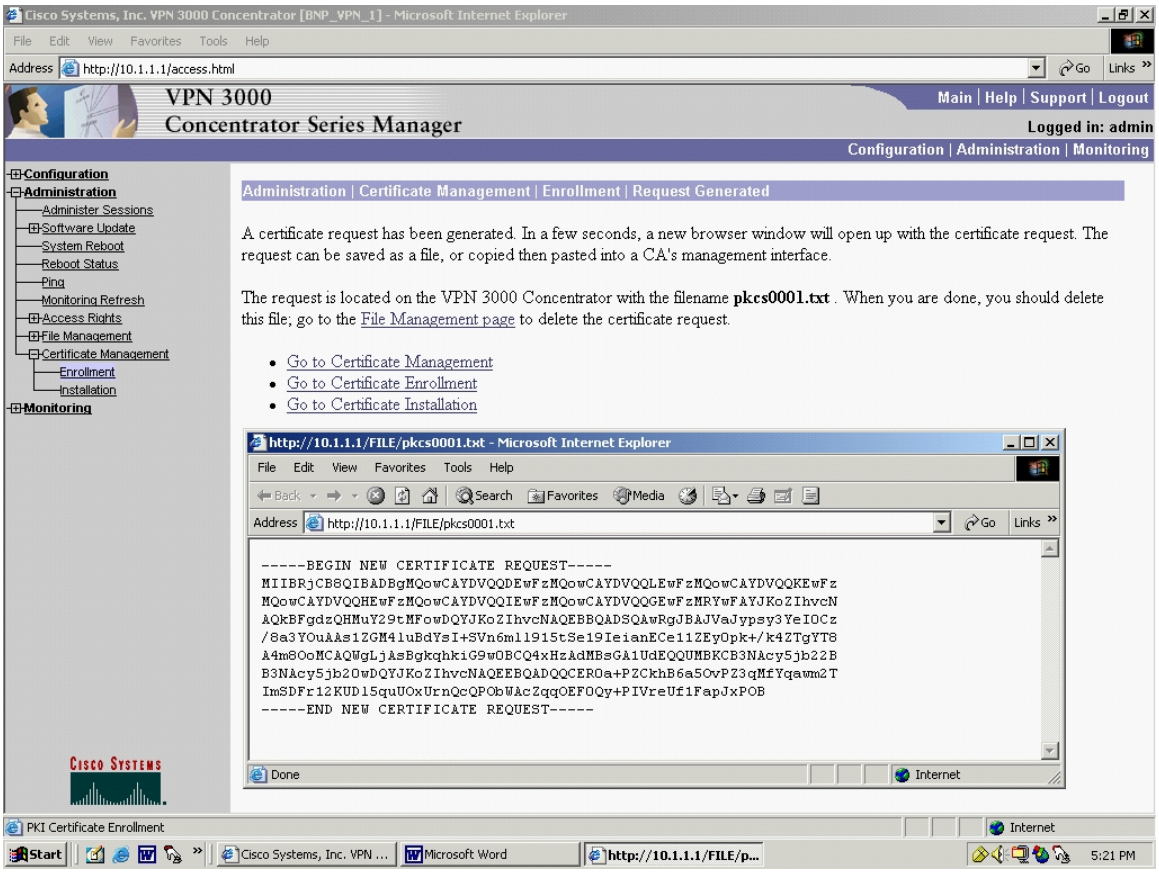

Figure 82. Concentrator Certificate Management Enrollment Request Generated

Using the browser "Save As" function within the inner pop-up window, the user can save the certificate to the host computer and ultimately to a floppy drive. The certificate can be sent out of band to the CA so an identity certificate can be generated.

At this point, the user can go back to the Administration | Certificate Management screen, Figure 83, and see the enrollment status of the identity certificate.

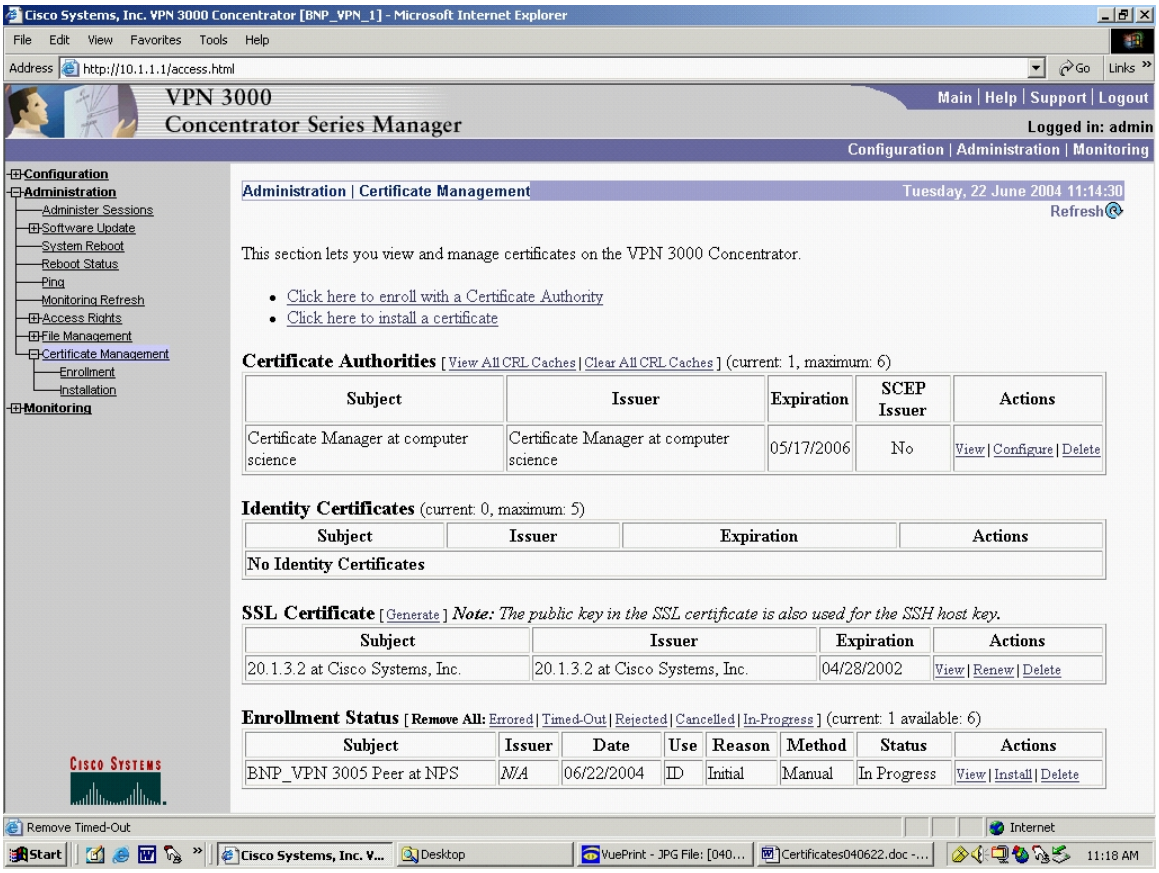

Figure 83. Concentrator Certificate Management View

Unfortunately, the NPS NCMS was unable to generate an identity certificate using the pkcs0001.txt output file from the 3005. Troubleshooting with the NCMS system administrator showed that a plug-in was needed by the NCMS in order to manually generate the identity certificate.

However, once an identity certificate has been generated and the 3005 has been enrolled, its identity certificate would reside in the 3005. To install this certificate that has been obtained via the enrollment process, go to the Administration | Certificate Management, Figure 76, and select the hotlink “Click here to install certificate”. This provides access to the Administration | Certificate Management | Install certificate obtained via enrollment screen, Figure 84.

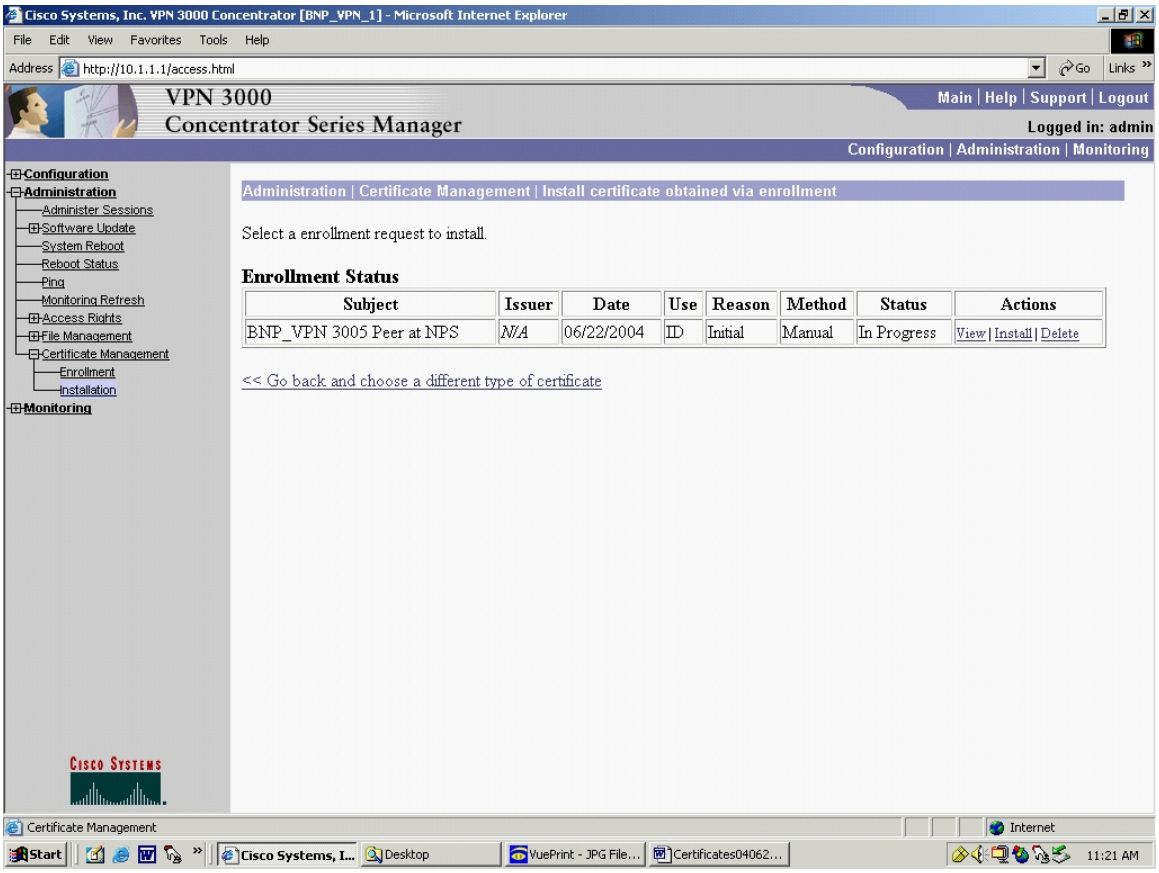

Figure 84. Concentrator Certificate Management Install Certificate

Clicking on the “view” hotlink under “Actions”, the user can see that the status of the certificate shows “In Progress”, Figure 85. Note that the identity certificate has not been installed yet. It is in the middle of the enrollment process.

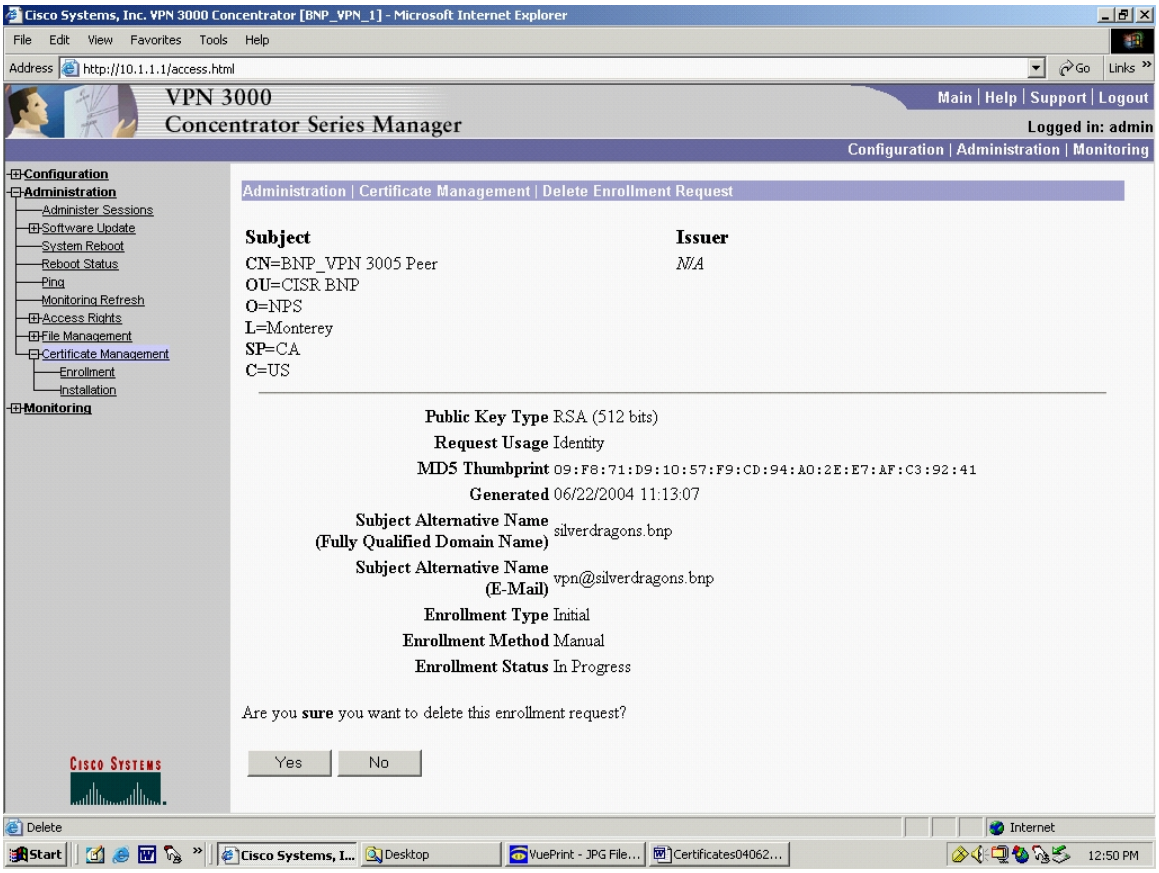

Figure 85. Concentrator Certificate Management Delete Enrollment Request

Once an identity certificate was generated and put on a floppy disc by the NCMS the user would need to upload the identity certificate. This is similar to how the CA certificate was uploaded. Under actions, click "Install" and the 3005 will require input. The user can cut and paste in information, or can get the information from a file. However, instead of doing this for a CA certificate as was done previously, the user is now doing it for the identity certificate, i.e. using the Administration | Certificate Management | Install | Identity Certificate screen, shown in Figure 86.

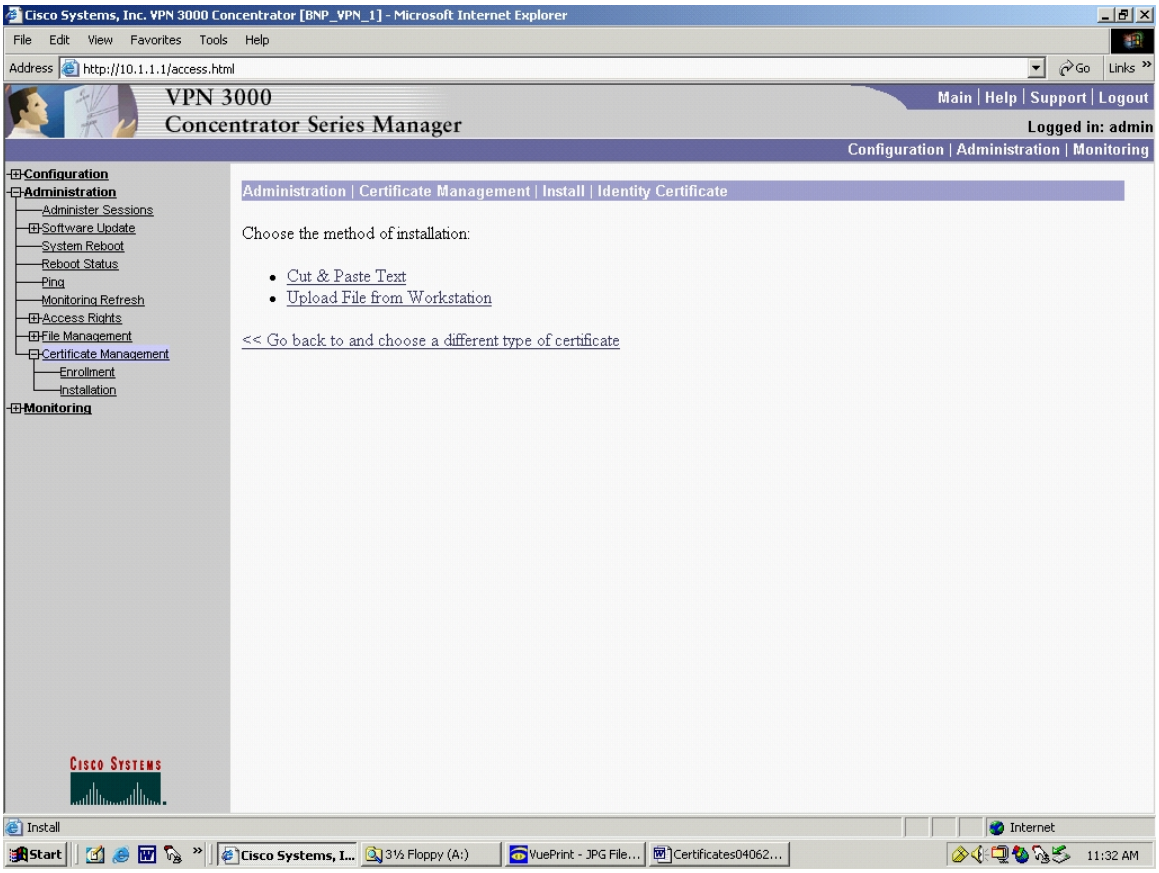

Figure 86. Concentrator Certificate Management Install Identity Certificate

In Figure 86, select “Upload File From Workstation” and similar to what was accomplished in the CA Certificate screen, Figure 75, find the id.cer certificate and install it.

Going back to the Administration | Certificate Management screen, Figure 70, both the CA Certificate and the identity certificate would now show installed.

The 3005 is now configured to using Certificates.

Using the Certificates in the VPN 3005 Concentrator

There are two places in the 3005 that require adjustments in order to switch from the use of pre-shared secret authentication to the use of certificates. The first is the Configuration | Policy Management | Traffic Management | Security Associations | Modify screen, Figure 87.

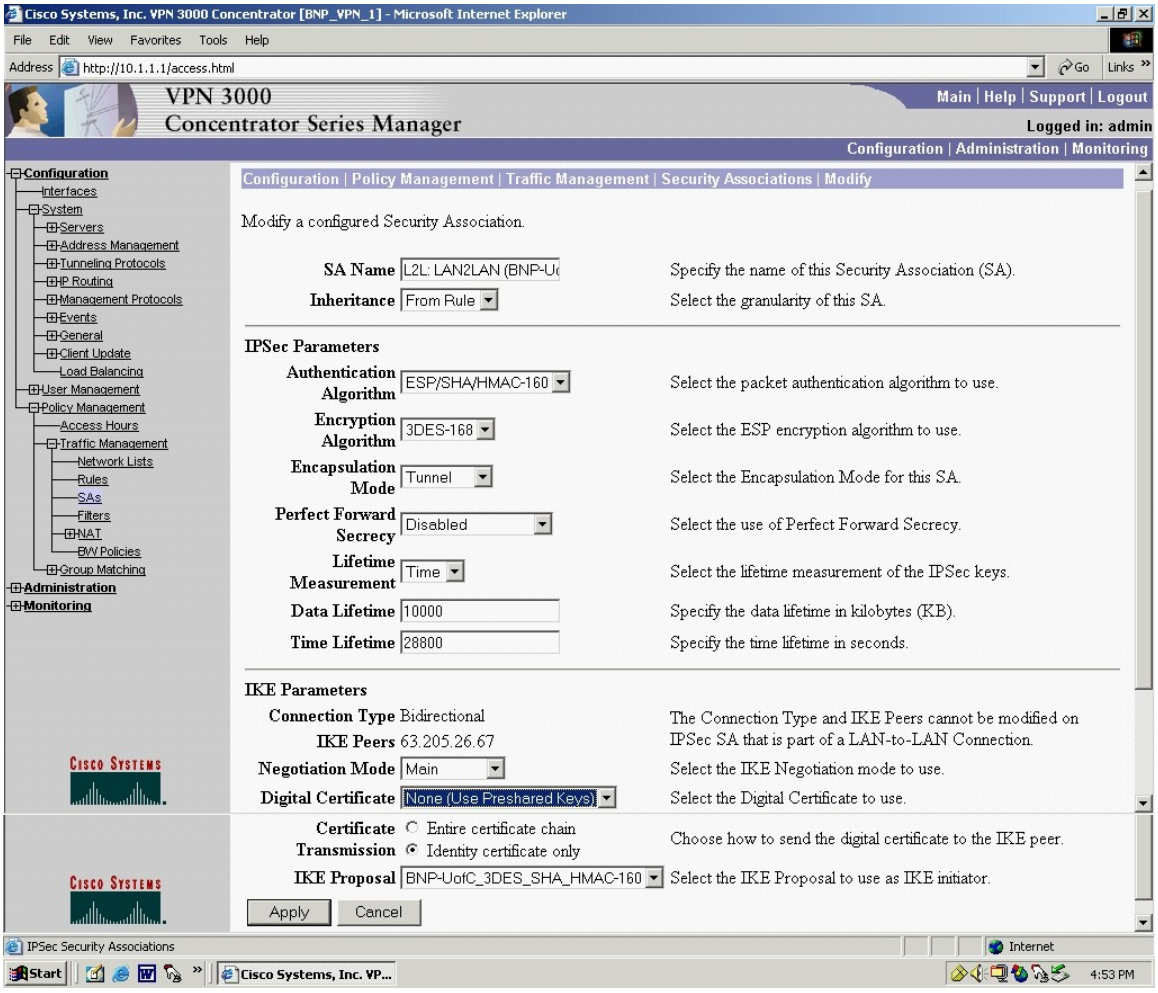

Figure 87. Concentrator Certificate Usage: IKE Security Association

In Figure 87, under IKE Parameters, Digital Certificates, instead of selecting "None - Use Pre-Shared Key" as was done in Figure 68, select the identity certificate which was created and will now be present in the drop down list.

The second screen that requires changes is the Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify screen, Figure 88.

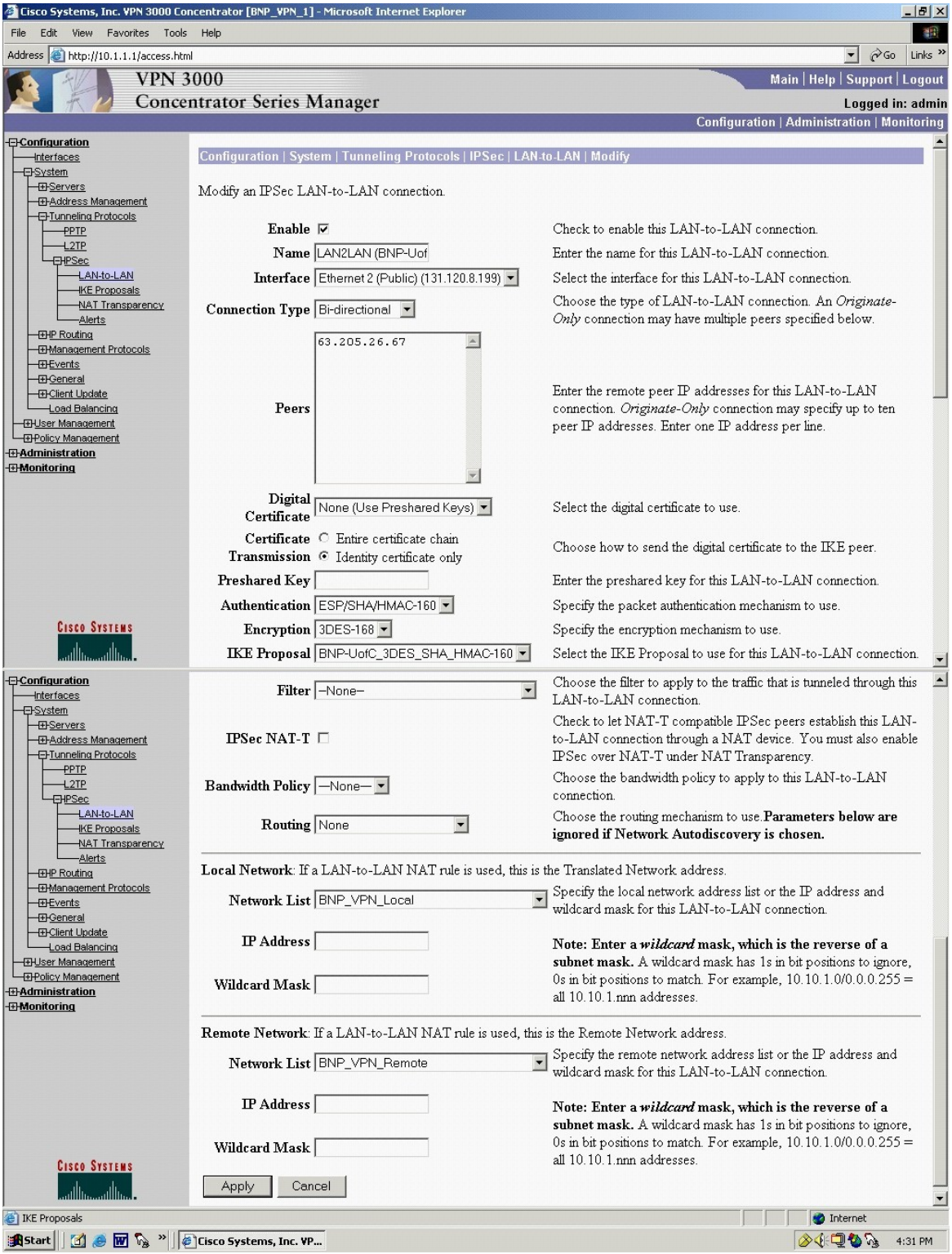

Figure 88. Concentrator Certificate Usage: IPSec Security Association

In the upper portion Figure 88, there is another reference to Digital Certificates. The user would select the identity certificate from the drop down list.

E. SPLIT TUNNELING

Split tunneling is a configuration of a VPN where traffic to the VPN peer is sent encrypted through the tunnel, yet traffic that is not destined for the VPN peer is sent in the clear outside of the tunnel.

Before the exercise, split tunneling needs to be enabled. Traffic destined for the cyber-exercise opponent's network goes through the VPN tunnel, yet other traffic is left alone to reach its destination as if the VPN was not in place. This allows cyber-exercise participants to send and receive e-mail, and access the Internet outside the tunnel in order to update drivers and continue to patch their systems. Split tunneling also allows traffic to flow through the tunnel in order to test VPN connectivity prior to the start of the exercise.

During the exercise, split tunneling must be disabled. Traffic from the network behind the cyber-exercise VPN gateway that is not destined for the VPN peer is blocked. This will ensure that non participating network nodes are not exposed to any of the exercise traffic.

In the split tunneling examples that follow, private address space is used on this sample network. Instructions using both the CLI and the SDM demonstrate the commands to enable and disable split tunneling. The reader may realize that, in the example that follows, the cyber-exercise network uses private address space (identified in the IETF's RFC1918, e.g.10.1.1.5 or 192.168.0.251). Though private address space would allow exercise participants to send traffic to the Internet, return traffic will not routed back, as routers will not forward to a private address space. In order to ensure that the cyber-exercise private address space is able to communicate with the Internet, the VPN gateway router would need to implement network address translation (NAT). NAT provides one or more public IP addresses to be mapped to private/internal IP addresses as packets traverse the NAT device (usually a router) going to/from the private and public networks that are on either side. This allows the network of private IP space addresses behind the VPN gateway to access the Internet, so long as split

tunneling is enabled. Using the commands below would allow the enabling and disabling of split tunneling on the cyber-exercise network that is using NAT. [TAN02]

1. Split Tunneling Router to Router Using CLI

Per the instructions in Table 14, the VPN tunnel is already in place. In effect, a split tunnel condition exists. This is the pre-cyber-exercise state. However for the cyber-exercise state, all other traffic must be blocked. This is done via an Access Control List (ACL).

The following commands in Table 25 must be executed.

BNP_VPN(config)#**access-list 120 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.0.255**	Creates the first rule in ACL 120. Permits IP traffic from the BNP network to the U of C network.
BNP_VPN(config)#**int f0/0**	Switched to the interface configuration mode.
BNP_VPN(config-if)#**ip access-group 120 in**	Applies ACL 120 to the FastEthernet 0/0 interface for traffic traveling inbound to the router, i.e. traffic coming from the BNP network (10.1.1.0)

Table 25. Router CLI: Disabling the Split Tunnel via ACL

To implement a split tunnel condition, it is necessary to disassociate ACL 120 with the Interface using the commands shown in Table 26.

BNP_VPN(config)#**int f0/0**	Switched to the interface configuration mode.
BNP_VPN(config-if)#**no ip access-group 120 in**	The “no” command disassociates the ACL.

Table 26. Router CLI: Enabling the Split Tunnel

2. Split Tunneling Router to Router using SDM

Similar to the CLI steps in Tables 25 and 26, in order to take the router from a pre-cyber-exercise (split tunnel enabled) state where it is now to block all other traffic, the user needs to create an Access List.

Using the SDM, go to Advanced Mode | Rules. This screen is shown in Figure 89.

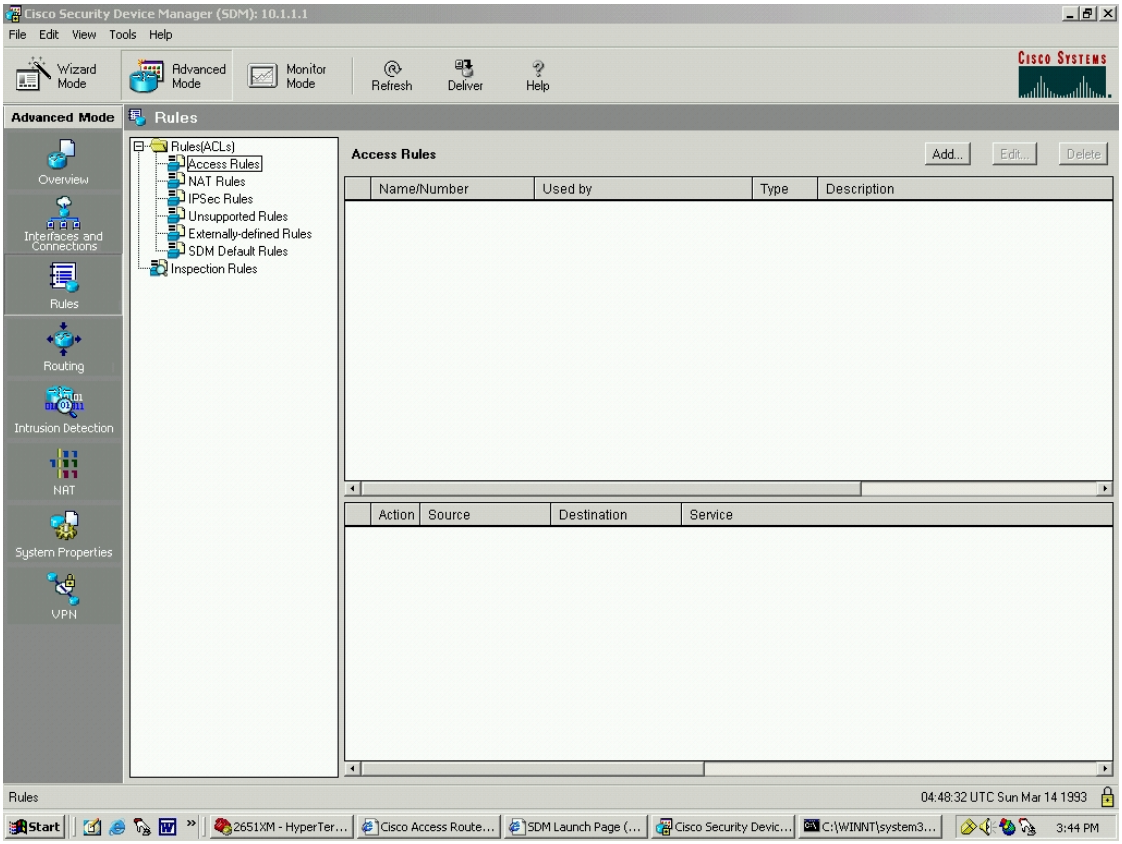

Figure 89. Router SDM: Access Rules

Click “Add”

In Figure 90, enter the Name, Type, and Rule Description:

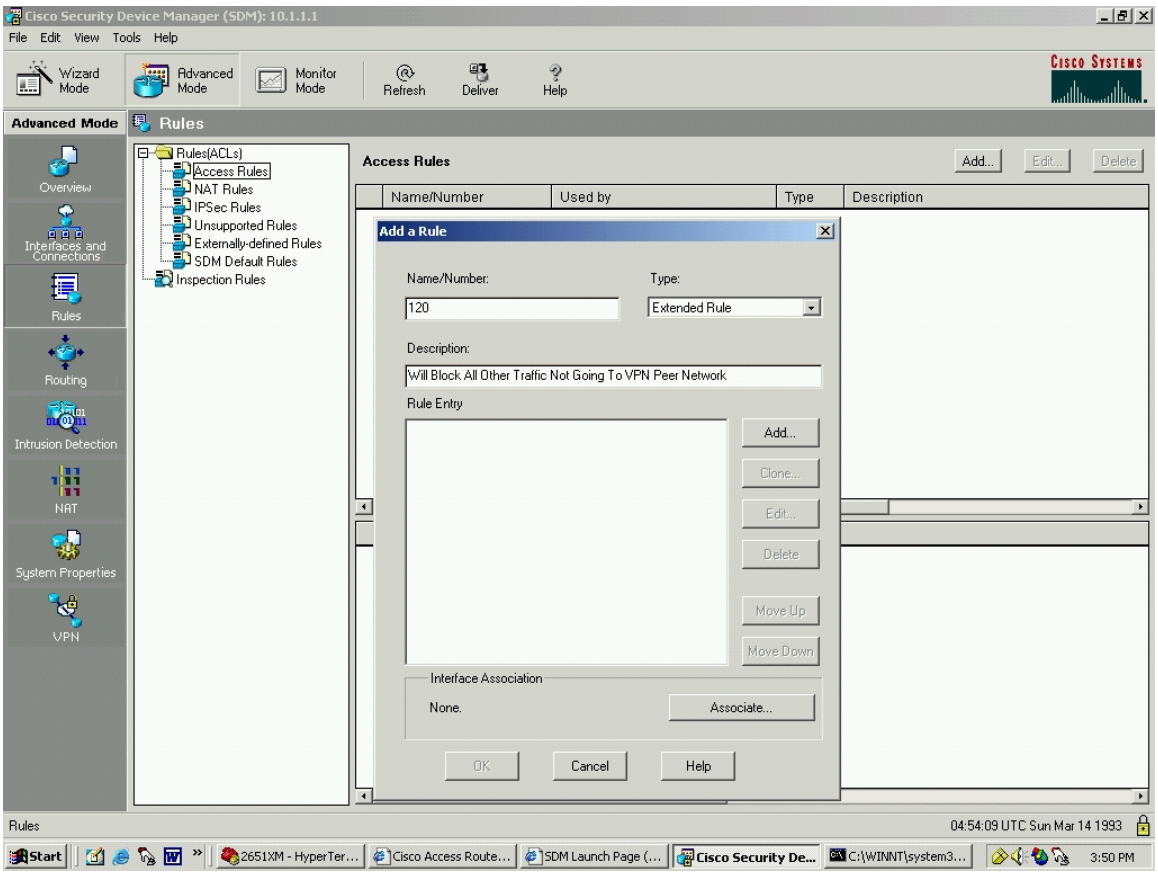

Figure 90. Router SDM ACL: Add a Rule

Click “Add”. Set up this first part of the rule to allow traffic from the local network to the peer network. This can be noted in the description:

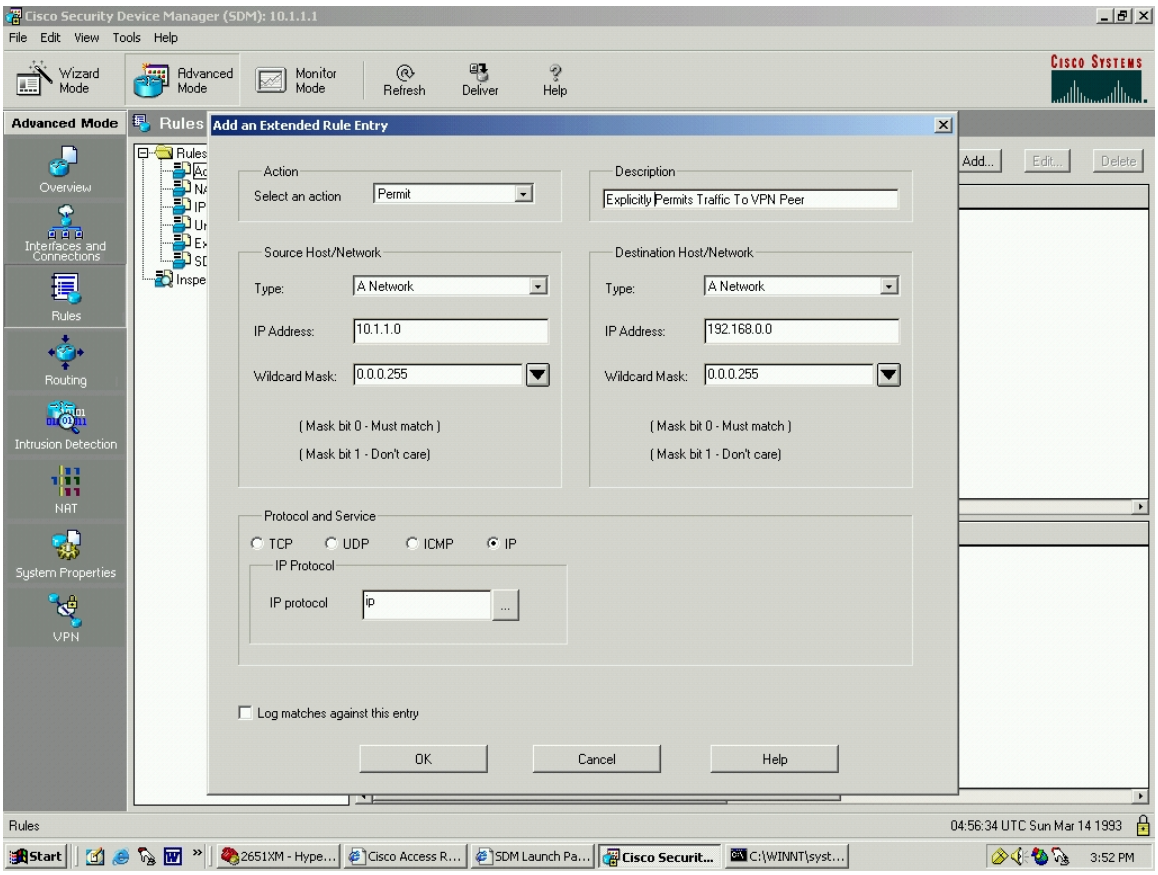

Figure 91. Router SDM ACL: Extended Rule Entry

In Figure 91, click “OK”. The first part of the rule has been added. Similar to the CLI, there is another part to the rule, consisting of blocking all other traffic.

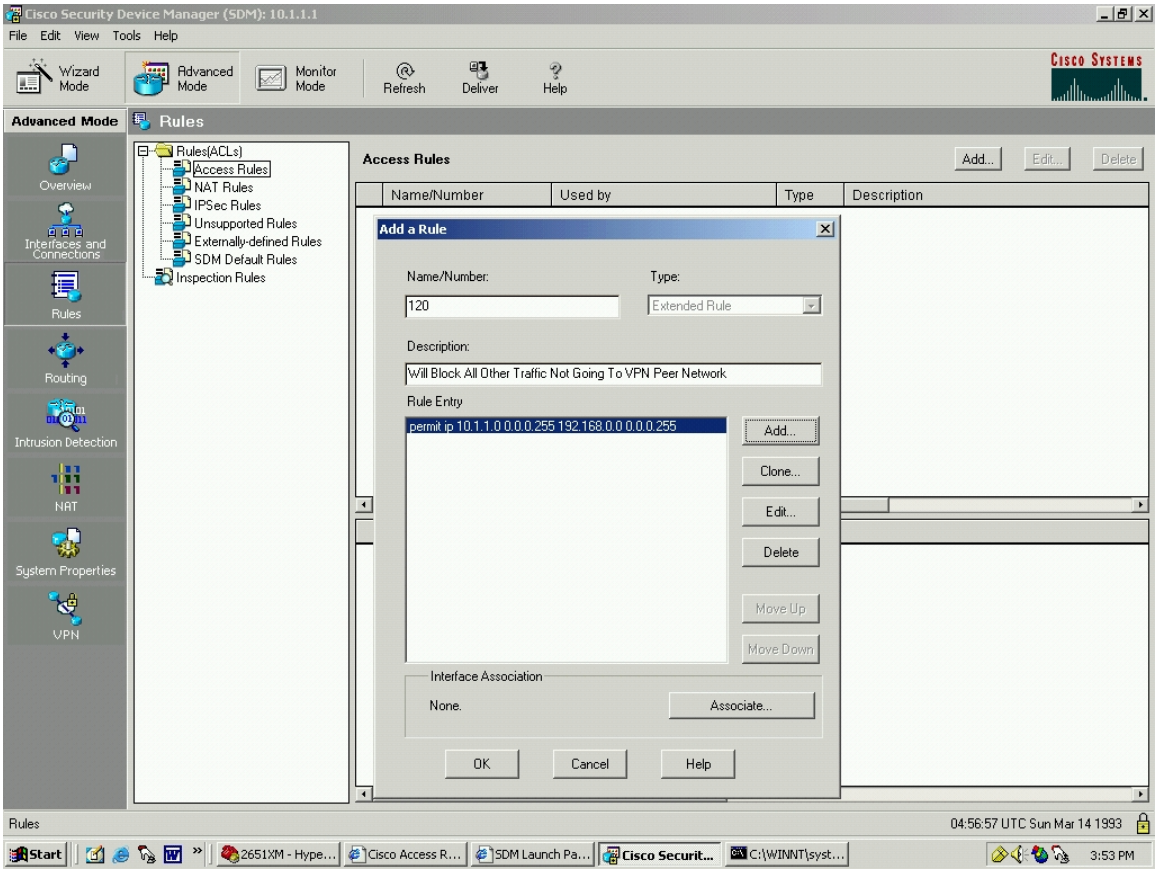

Figure 92. Router SDM ACL: Rule Added

In Figure 92, click “Add”. Set up this second part of the rule to block all other traffic. This can be noted in the description. Notice that “Any IP Address” is a Cisco default selection under “Type” in Figure 93.

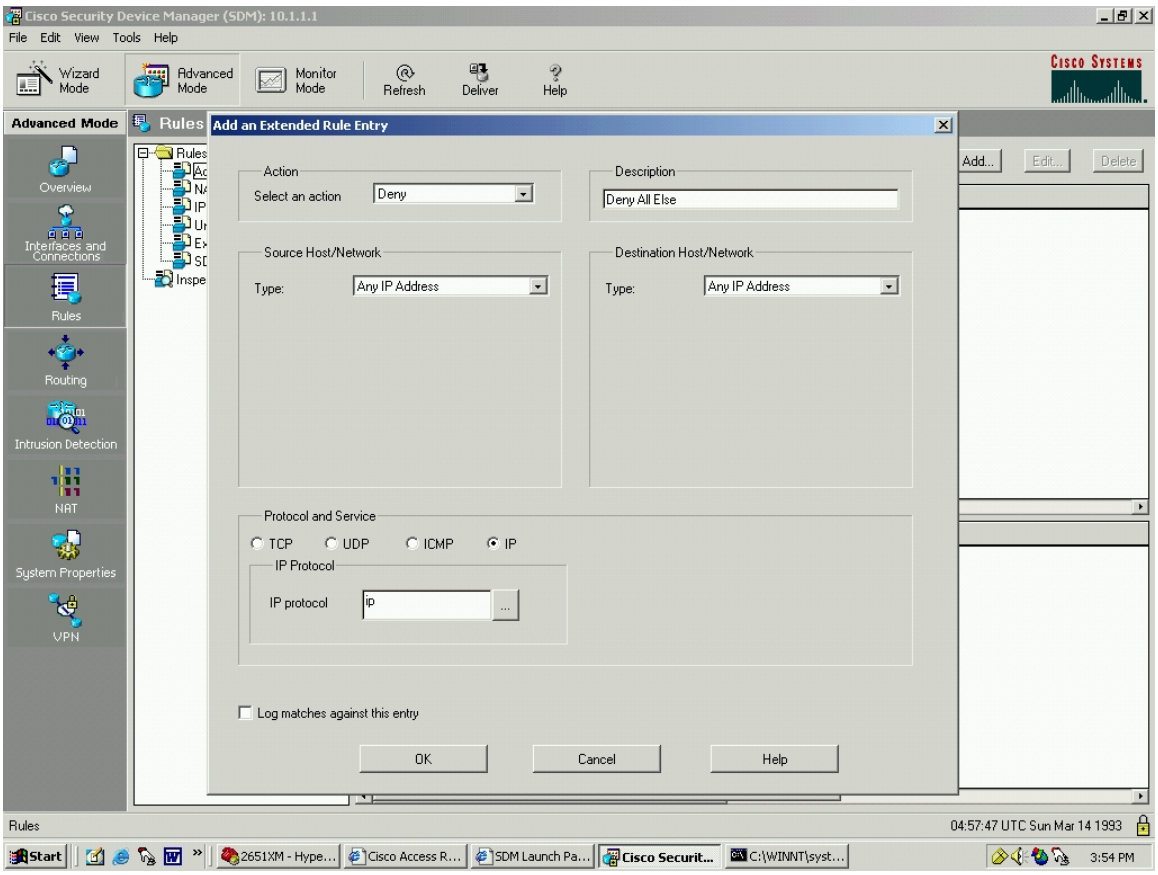

Figure 93. Router SDM ACL: Add an Extended Rule Entry

Click “OK”. Now the second part of the rule has been added, as shown in Figure 94.

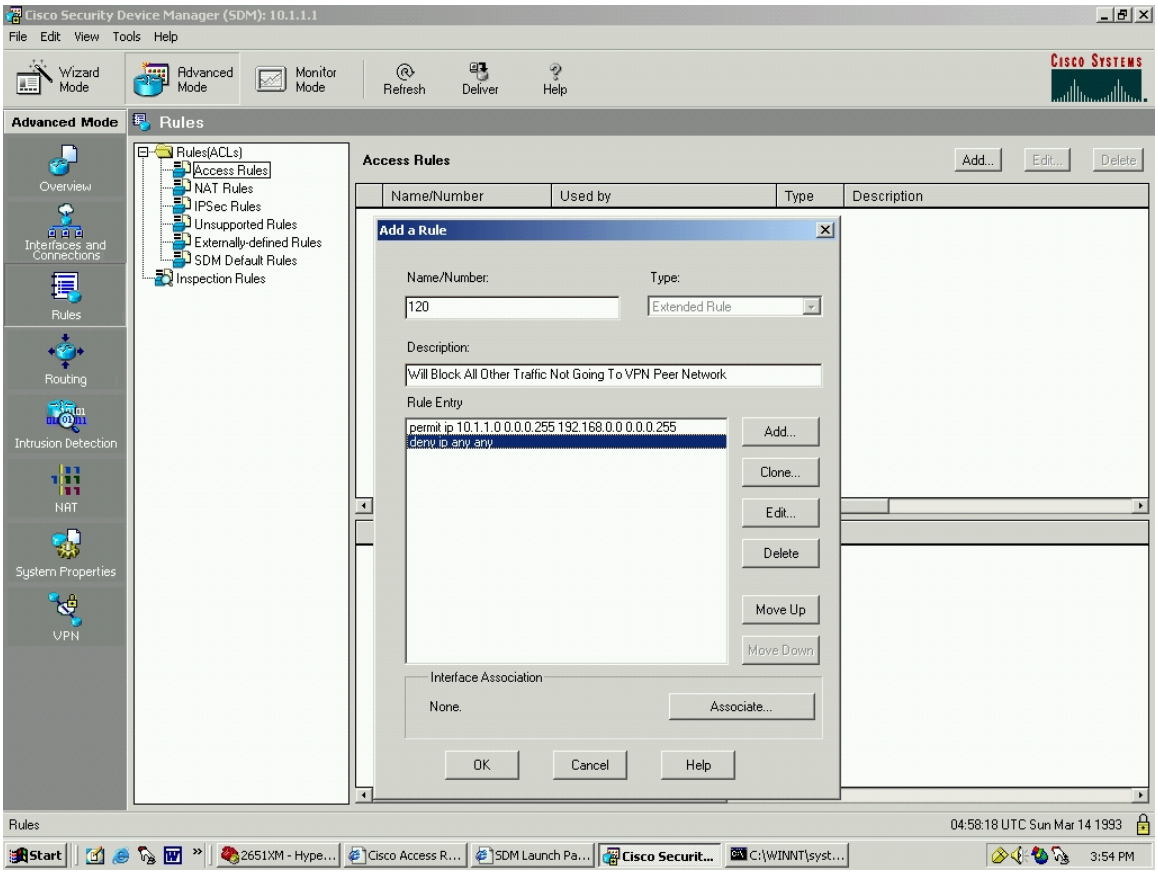

Figure 94. Router SDM ACL: Rule Added

ACL 120 still must be associated with an interface. In Figure 95, click “Associate”.

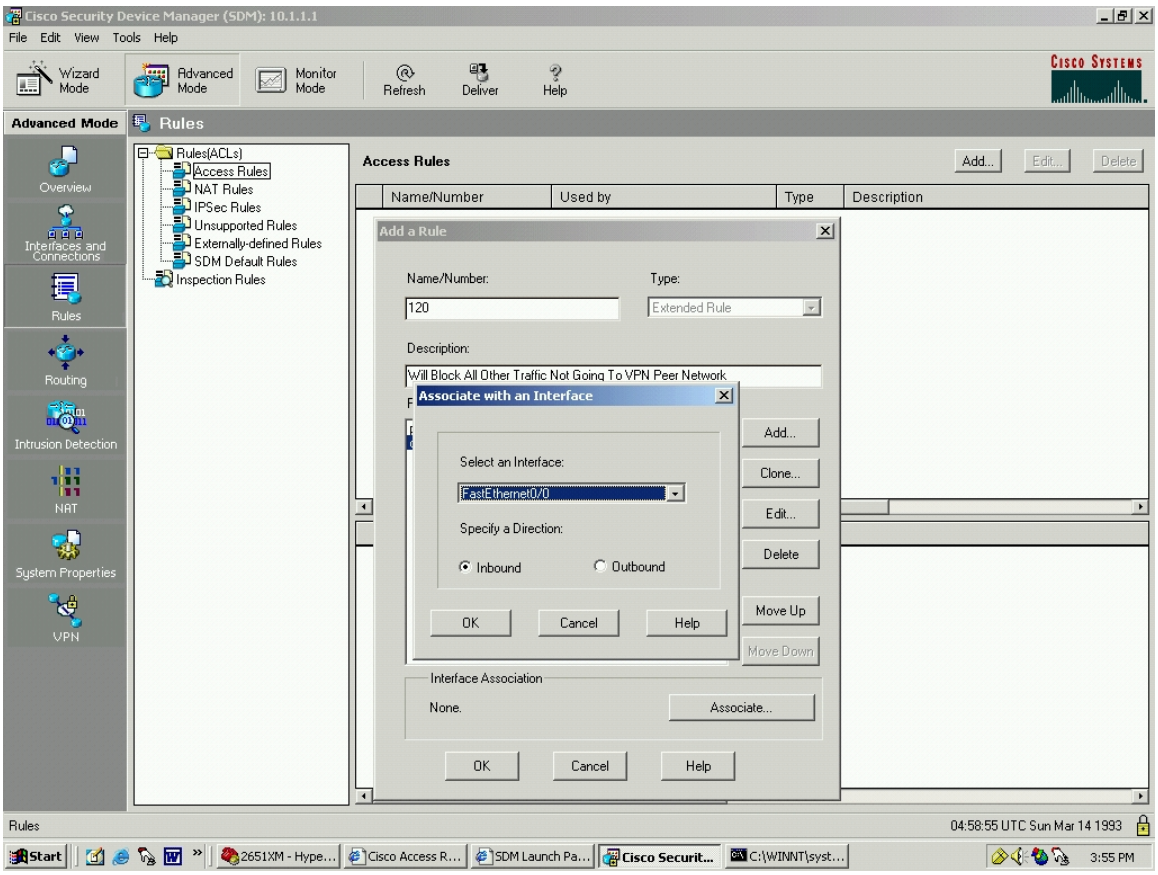

Figure 95. Router SDM ACL: Associate Rule with Interface

In Figure 95, select an Interface, in this case f0/0, and the direction, “Inbound” (i.e. inbound to the router). Click “OK”.

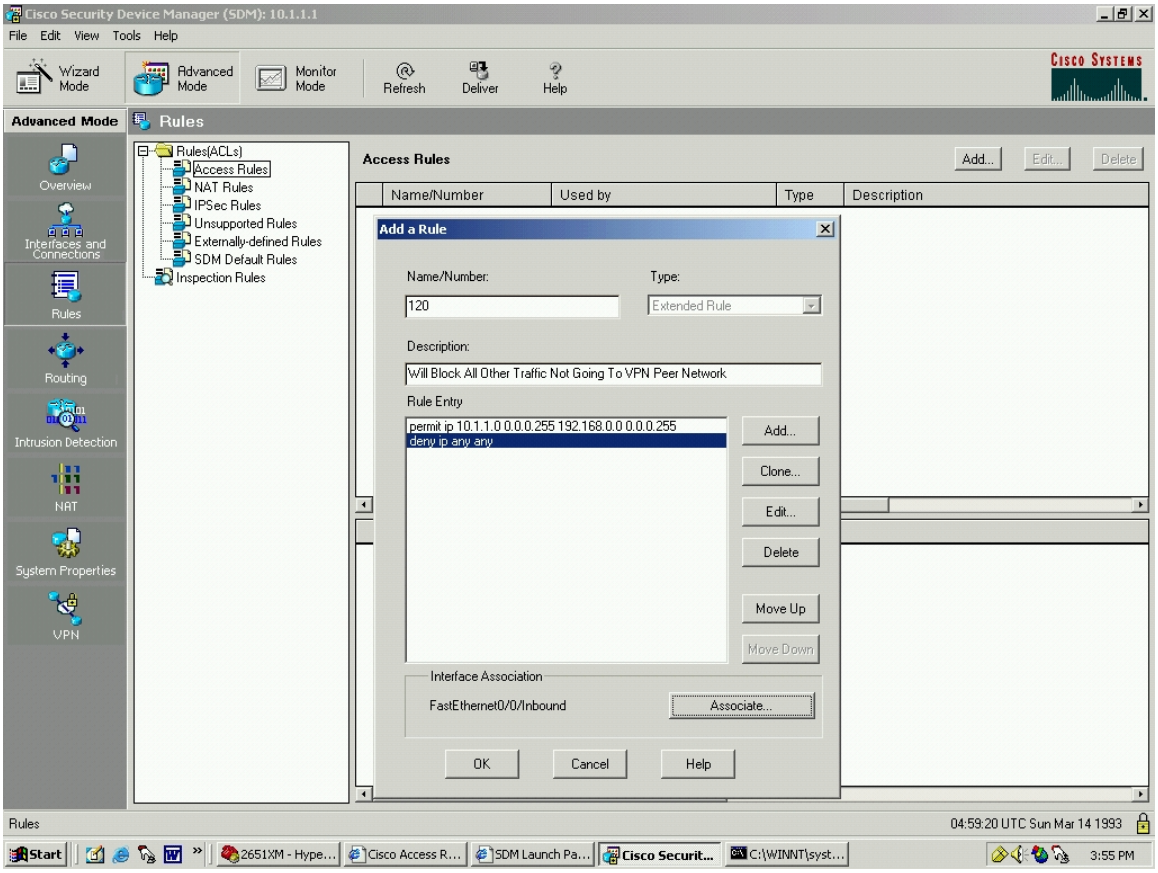

Figure 96. Router SDM ACL: Rule Added

Click “OK”.

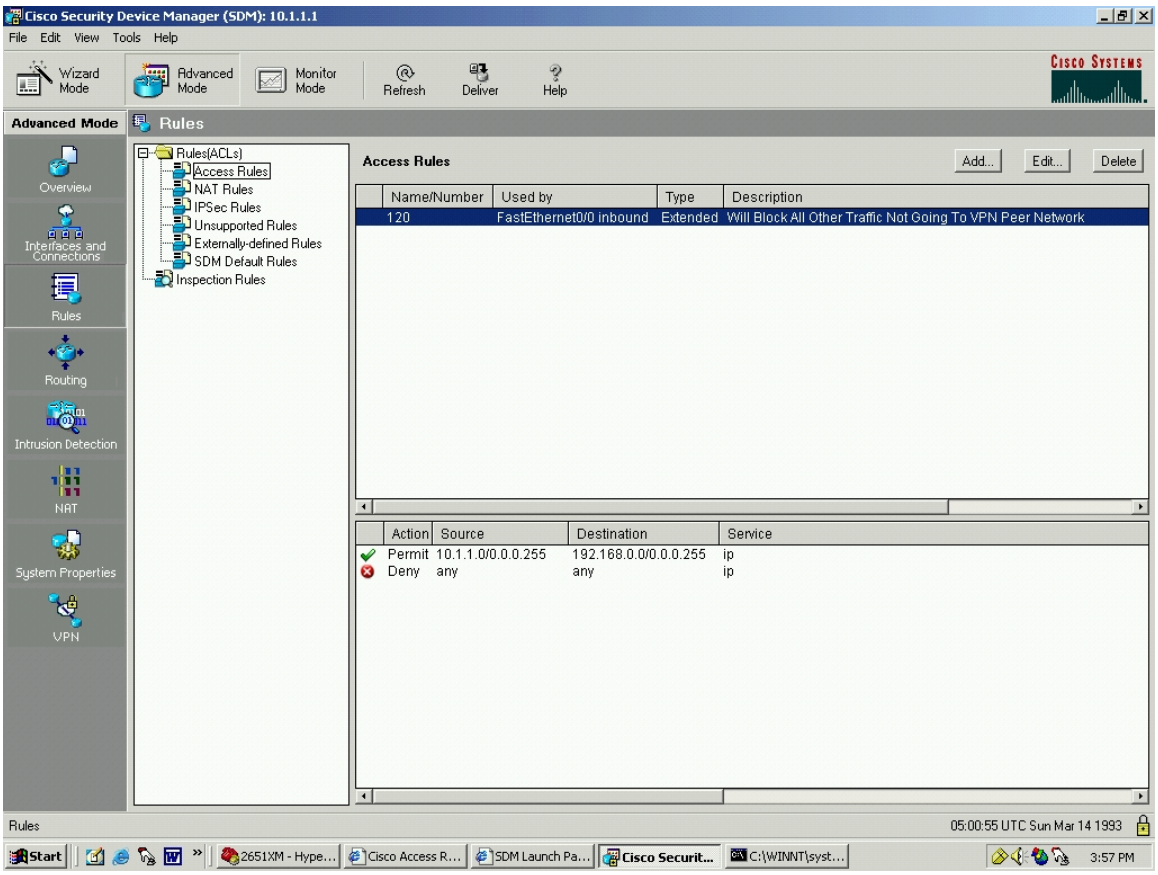

Figure 97. Router SDM ACL: Rule Added

The rule is in place. In Figure 97, click the "Deliver" icon in the top menu bar to send the commands to the router.

3. Split Tunneling with Cisco 3005 Concentrator

The two primary applications of VPNs are using the technology to securely connect two or more LANs, and using the technology to allow a secure remote extension of a LAN to remote dial-in users. After much research into the capabilities of the 3005, it becomes apparent why Cisco decided to name the device a "VPN Concentrator".

Previously, if a corporation needed many users to connect from remote locations to its headquarters, the standard solution was to use a bank of modems. However, with the advent of VPN technology, this same corporation can "concentrate" the access point of all users via one Cisco VPN "Concentrator".

It naturally follows that the remote dial-in capabilities of the Cisco VPN concentrator are very robust. In fact, the 3005 can service up to 100 users at once via separate tunnels. [CIS04] Since the 3005 is specialized particularly to support the remote user dial-in VPN model, it would follow that the concentrator's support for LAN-to-LAN VPN functionality is less robust. Research within two separate Cisco books [MAS99, MAS02] dealing with the LAN-to-LAN and the dial-up configuration of the Cisco VPN concentrator revealed split tunneling instructions for dial-up users. However neither book had examples or instructions for LAN-to-LAN split tunneling using the VPN Concentrator.

F. CHAPTER SUMMARY

This chapter has examined three VPN alternatives. Detailed steps to build a functioning VPN have been shown, as well as the use of digital certificates and the implementation of split tunneling. In Chapter VI, a close look will be taken at all theoretical and practical topics discussed so far, resulting in the recommendation of an optimum VPN to be used to link cyber-exercises.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY AND CONCLUSIONS

A. VIRTUAL PRIVATE NETWORKS

This thesis has examined the complex technology that goes into building a virtual private network (VPN). Realizing the need to hone cyber-attack and defend skills, frequent cyber-exercises between universities is one the best ways to accomplish this goal. The creation of a VPN is the preferred method to link the networks that participate in these cyber-exercises. VPN creation has been the subject of this thesis.

1. Technology

The technology that goes into the understanding and building of a VPN is complex. All aspects of internet protocol security (IPSec) must be carefully considered. The internet key exchange (IKE) parameters, the authentication header (AH) and encapsulating security payload (ESP) security protocols, the tunnel and transport security modes, encryption and hash algorithms, and proper selection of the VPN endpoint devices methods must be understood, evaluated, and carefully chosen in order to ensure that all user requirements are met.

2. Benefits

If carefully selected and properly implemented, a VPN is the preferred method to provide a secure and reliable link between participating networks. Depending on the needs of the users, VPNs can be tailored to run from gateway to gateway, or from host to host. VPNs can be created on almost any budget. VPNs can be designed to provide confidentiality, and/or integrity and authenticity. VPNs can be integrated with public key infrastructure (PKI) digital certificates if needed, or can operate using pre-shared secret keys. Finally, VPNs can be custom configured to balance security strength against efficiency and speed. The ultimate result of careful configuration, selection, and implementation of a VPN is that cyber-warriors can effectively isolate their exercise traffic from the public Internet infrastructure that it traverses.

B. CYBER-EXERCISE REQUIREMENTS

Ideally, cyber-warriors require a VPN that provides a balance of security and efficiency, can be easily set up and maintained, and whose hardware falls within their budget. All aspects discussed so far, including VPN layer choice, security mode and protocol, encryption and hash algorithms, key management, and endpoint devices must be considered. Each of these items are addressed below.

1. Layer

After careful consideration of all possibilities, the ideal location for a VPN to link LAN-to-LAN cyber-exercise participants is Open Systems Interconnection (OSI) layer 3, the network layer. As examined in Chapter II, a layer 2 (data link layer) VPN exacts an overhead in header processing that is unnecessary for networks that are directly connected to the Internet, and a layer 5 (application layer) VPN is inadequate because it cannot encapsulate every application that may be utilized in a cyber-exercise. Building an internet protocol security (IPSec) layer 3 VPN allows a cyber-exercise to take advantage of the potential broadband speed of a LAN-to-LAN connection over the Internet, as well as to take advantage of the many security choices that can be tailored within the IPSec protocol.

2. Security Mode

After consideration of the two modes, tunnel and transport, the only logical choice is the tunnel mode. Tunnel mode allows cyber-exercises to be conducted gateway-to-gateway, also referred to as LAN-to-LAN. If transport mode were utilized, the cyber-exercise could only be conducted from one host to one host. This host-to-host connection would not meet the multi-host needs of a realistic cyber-exercise.

3. Security Protocol

After consideration of the two protocols, encapsulating security payload (ESP) and authentication header (AH), the only logical choice is the ESP. ESP supports encryption which will provide the required confidentiality. If AH were used, only integrity, authentication, and replay protection would be provided for traffic. As was

demonstrated with Ethereal, without encryption, exercise traffic would traverse public network infrastructure in the clear.

4. Encryption Algorithm

The advantages and disadvantages of the data encryption standard (DES) and the advanced encryption standard (AES) encryption algorithms were considered. Potentially, a cyber-exercise participant may only be able to afford a low end device as a VPN gateway. This device may not be very efficient when conducting encryption. Coupled with the knowledge that cyber-exercises do not require extremely robust encryption to provide confidentiality for the exercise traffic, the optimal algorithm to use for a cyber-exercise would be AES128. More secure and faster than DES, AES128 provides a good balance between the security desired for a cyber-exercise and algorithm performance.

5. Hash Algorithm

The advantages and disadvantages of the Secure Hash Algorithm-1 (SHA-1) and Message Digest 5 (MD5) hash algorithms were considered. In a similar thought process as used in choosing the encryption algorithm, a cyber-exercise participant's VPN gateway may not be very capable. Coupled with the knowledge that cyber-exercises do not require the most robust hash algorithm, the optimal hash algorithm to use for a cyber-exercise would be MD5. MD5, generating a 128-bit hash, will provide a good balance between sufficient packet integrity and system performance.

6. Key Management

After considering the pros and cons of key management, to include use of pre-shared secrets versus digital certificates, and the choice between a static key and dynamic re-keying, a static key exchanged out of band was deemed the preferred choice. The static key, if properly entered into both VPN peers, provides adequate security for the exercise, obviates the overhead involved when conducting periodic re-keying, and side-steps the poorly supported certificate validation issue that plagues public key infrastructure (PKI) implementations.

7. Endpoint Devices

Through consideration of price, complexity, and overall suitability of the three choices: the VPN Concentrator, the VPN-capable router, and the general purpose

computer running open source VPN software; it was decided that the ideal gateway device was the VPN-capable router using the security device manager (SDM) graphical user interface (GUI).

The VPN-capable router using the SDM GUI interface is superior to the VPN Concentrator for linking cyber-exercises via LAN-to-LAN connectivity. First, many potential cyber-exercise organizations already own a router that is either VPN-capable or can undergo an internetwork operating system (IOS) upgrade to allow VPN functionality. Second, router configuration is an area where many cyber-exercise participants already have expertise. Configuration of the router, with a VPN, would be familiar, straightforward, and quick. Last, the VPN-capable router can take advantage of all aspects of a VPN including LAN-to-LAN split tunneling.

8. Recommended Solution

The optimal VPN solution for cyber-exercises is shown in Table 27.

IKE Policy
Encryption: AES128
Hash: MD5
Authentication: Pre-Share
IPSec Transform Set
Mode: ESP, Tunnel
Encryption: AES128
Authentication: MD5_HMAC

Table 27. Optimal VPN Solution For Cyber-Exercises

C. RECOMMENDATIONS FOR FUTURE WORK

1. Open Source VPNs

With the discontinuation of support for FreeS/WAN, follow-on work could be completed investigating other open-source standards for constructing software-based VPNs that can run on general purpose computers. Then, one or more of these open

source products could be selected to build a VPN, possibly using the Linux or Sun operating systems (OSs). These VPNs could be compared for efficiency and interoperability with each other. Finally, the compatibility of an open-source VPN with a Cisco VPN device could be examined.

2. VPN Performance

This thesis looked at the ease of use and theoretical concerns of choosing a VPN for a cyber-exercise. NPS owns a packet generator. Follow-on work could be completed constructing VPNs using Cisco devices and combinations of tunnel / transport mode, AH / ESP protocols, and integrating the packet generator to test and compare the performance and efficiency of these VPNs. This would provide an alternative metric to those used in this thesis for determining the ideal VPN for a cyber-exercise.

3. Integration of the NPS CA

Recent work at NPS resulted in the building of a certificate authority (CA) using the Netscape Certificate Management System (NCMS) on a Sun workstation. [KEL04] Follow-on work could be conducted that would involve the complete online integration of the NCMS system with the Bastion Network Project. A second network could be constructed in the Bastion Network Project spaces and a separate NCMS could be built and integrated so the VPN connecting the two networks would use NCMS-generated certificates for authentication. Alternately, one CA could be built and both networks could access that CA and obtain their certificates.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[ADA99] Adams, C., Farrell, S., *Internet X.509 Public Key Infrastructure Certificate Management Protocols,* RFC-2510, SSE. March 1999, URL: http://www.ietf.org/rfc/rfc2510.txt, Accessed August 2004.

[AMP01] *AMPHION CS5010 DES-3DES Encryption Codes*, URL: http://www.actel.com/ipdocs/CS5010_40.pdf , Accessed August 2004.

[BAL96] Baldwin, Bob. *MD5 vs. SHA-1, Performance & Pedigree*, URL: http://www.netsys.com/ipsec/1996/msg00590.html, Accessed August 2004.

[BEY02] Beyond If, Inc. *Comparison White Paper Based On Lenstra Paper and Upgrades After Tu-Einhoven.* URL: http://www.beyondif.com/docs/HRC_compare_white_paper.pdf, Accessed August 2004.

[BLA96] Blaze, M., Diffie, W., Rivest, R. *Minimum Key Lengths For Commercial Ciphers to Provide Adequate Commercial Security*, January 1996, URL: http://www.schneier.com/paper-keylength.pdf, Accessed August 2004.

[CIS01] Cisco, Inc. *Advanced Integration Module Installation in Cisco 2600 Series, and Cisco 3700 Series Routers, URL: http://www.cisco.com/en/US/products/hw/routers/ps259/prod_module_installation_guide09186a00801ac5f5.html, Accessed August 2004.*

[CIS02] Cisco, Inc. *DES/3DES/AES VPN Encryption Module (AIM-VPN/BPII), URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftaimvpn.htm, Accessed August 2004.*

[CIS03] Cisco, Inc. *Virtual Private Network Modules for the Cisco 1700, 2600, 3600, and 3700 Series* (Cisco Press, 2003), URL: http://newsroom.cisco.com/dlls/VPNMODDS.pdf, Accessed August 2004.

[CIS04] Cisco, Inc. *Cisco VPN 3000 Series Concentrator Software*, URL: http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm, Accessed August 2004.

[CIS05] Cisco, Inc. *Cisco PIX VPN Accelerator Card*, URL: http://www.cisco.com/warp/public/cc/pd/sqsw/vpncl/prodlit/vacds_ds.pdf, Accessed August 2004.

[CIS06] Cisco Inc., *Configuration Information for an Administrator VPN 3000 Series Concentrators Configuration Information,URL:* http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_6/admin_gd/vcach1.htm, Accessed August 2004.

[DAI01] Dai, Wei. *Benchmarks: Speed Comparison of Popular Crypto Algorithms*. URL: http://www.eskimo.com/~weidai/benchmarks.html, Accessed August 2004.

[DAV01] Davis, Carlton R. IPSec: Seuring VPNs (Osbourne, 2001).

[DEF01] *DEFCON: Welcome to the Largest Underground Hacking Event in the World* URL: www.defcon.org, Accessed August 2004.

[DEN98] Denning, Dorothy. *Is Triple DES Secure?* April 3, 1998, URL: http://www.cs.georgetown.edu/~denning/crypto/3des.txt, Accessed August 2004.

[DES01] *DES Encryption*, URL: http://www.tropsoft.com/strongenc/des.htm , Accessed August 2004.

[DHA02] Dhawan, Priya. *Performance Comparison: Security Design Choices*, URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnbda/html/bdadotnetarch15.asp, Accessed August 2004.

[DUN01] Dunnigan, Tim. *Virtual Private Network Performance*. URL: http://www.csm.ornl.gov/~dunigan/vpnperf.html, Accessed August 2004.

[DUN96] Dunnigan, Tom. *Virtual Private Network Performance*, 1996. URL: http://www.csm.ornl.gov/~dunigan/vpnperf.html, Accessed August 2004.

[ENC01] *MD5*. Encyclopedia: The Free Dictionary, URL: http://encyclopedia.thefreedictionary.com/md5, Accessed August 2004.

[ENC02] *Encryption and Security: The Data Encryption Standard*. http://www.madchat.org/crypto/DES.pdf, Accessed August 2004

[FOR01] Forouzan, Behrouz A. *Data Communications and Networking* 2nd Edition (McGraw-Hill 2001).

[FSW01] *FreeS/WAN Project Bows Out*, URL: http://slashdot.org/article.pl?sid=04/03/02/014215&mode=thread, Accessed August 2004.

[FUL04] Fulp, J. D. *Course Notes for CS3690, Network Security*, NPS CISR, 2004.

[GLE98] Glenn, R., Madson, C. *RFC-2404: The Use of HMAC-SHA-1-96 within ESP and AH,* URL: http://rfc.sunsite.dk/rfc/rfc2404.html, Accessed August 2004.

[HAR00] Harrison, Ann. *Advanced Encryption Standard* (Computerworld, May 30 2000) URL: http://www.computerworld.com/news/2000/story/0,11280,45282,00.html, Accessed August 2004.

[HOU02] Housley, R., Polk, W. *RFC-3208: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, April 2002, URL: http://www.ietf.org/rfc/rfc3280.txt?number=3208, Accessed August 2004.

[JAC04] Jackson, William. *NIST Wants To Phase Out DES For Encryption*, (Government Computer News, 08/02/04, Vol. 23 No. 21), URL: http://www.gcn.com/vol1_no1/technology-policy/26721-1.html, Accessed August 2004.

[KEL04] Kelly, A., Ambers, V. *Installation, Configuration, and Operational Testing of a PKI Certificate Server and its Supporting Services*, June 2004, URL: http://library.nps.navy.mil/uhtbin/cgisirsi/Mon+Aug+23+17:50:51+PDT+2004/SIRSI/0/520/04Jun_Ambers.pdf, Acccessed August 2004.

[LEN99] Lenstra, Arjen. *Selecting Cryptographic Key Sizes*. URL: http://security.ece.orst.edu/koc/ece575/papers/cryptosizes.pdf, Accessed August 2004.

[LEW01] Lewis, Brian C. *Information Warfare*, URL: http://www.fas.org/irp/eprint/snyder/infowarfare.htm, Accessed August 2004.

[MAI02] Mairs, John. *VPNs: A Beginner's Guide* (McGraw Hill 2002)

[MAS02] Mason, Andrew G. *Cisco Secure Virtual Private Networks* (Cisco Press, 2002)

[MAS04] Mason, Andrew G. CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN), Second Edition, (Cisco Press, 2004).

[MAU98] Maughan, D., Schertler, M. *RFC-2408: Internet Security Association and Key Management Protocol (ISAKMP)*, URL: http://www.ietf.org/rfc/rfc2408.txt, Accessed August 2004.

[MER99] Merkow, Mark S. *Virtual Private Networks for Dummies* (IDG Books, 1999)

[MIL04] Millard, E., *Digital Signature Concerns Emerge*, URL: http://www.linuxinsider.com/story/35926.html, Accessed August 2004.

[MOR02] Morris, Scott. *DES vs. 3DES, Performance vs. Security*. http://tcpmag.com/qanda/article.asp?EditorialsID=163, Accessed August 2004.

[MYE99] Myers, M., Ankney, R. RFC-2560: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, June 1999, URL: http://www.ietf.org/rfc/rfc2560.txt?number=2560, Accessed August 2004.

[PRE01] Preneel, Bart. *Report on the Performance Evaluation NESSIE Candidates I*, November 20, 2001, URL: https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/D14.pdf, Accessed August, 2004.

[REA01] Reavis, Jim. *Goodbye DES, Hello AES*. Network World 7/30/01. URL: http://www.nwfusion.com/research/2001/0730feat2.html, Accessed August 2004.

[REK96] Rekhter, Y., Moskowitz, B., *Address Allocation for Private Internets*, RFC-1918, Network Working Group February 1996.

[SCH04] Schmeing, Claudia. *Ending Letter*. April 2004, URL: http://www.freeswan.org/ending_letter.html, Accessed August 2004

[SIL04] Silberschlag, Shimon. V*PN: AES and 3DES performance on Cisco Routers*, http://sisyphus.iocaine.com/pipermail/vpn/2004-March/004673.html, Accessed August 2004.

[SMI01] Smith, Richard. *Deciphering the Advanced Encryption Standard*, Network Magazine, March 2001, URL: http://www.networkmagazine.com/article/NMG20010226S0010, Accessed August 2004.

[TAN02] Tanenbaum, A. *Computer Networks*, 4th Edition (Prentice Hall, 2002)

[THA98] Thayer, R., Doraswamy, N., Glenn, R., *IP Security Document Roadmap*, RFC 2411, November 1998

[TOU96] Touch, Joe. *MD5 vs. SHA-1, Selection Criteria*, URL: http://www.sandelman.ottawa.on.ca/ipsec/1996/05/msg00085.html, Accessed August 2004.

[TOU97] Touch, Joe. *Re: MD5 vs. SHA-1, Selection Criteria*, URL: http://www.netsys.com/ipsec/1996/msg00584.html, Accessed August 2004.

[VER02] Verton, Dan. *Experts: Don't Dismiss Cyberattack Warning*. Nov 18, 2002, URL: http://www.computerworld.com/securitytopics/security/story/0,10801,76000,00.html, Accessed August 2004.

[WAN04] Wang, X., Feng, D., Lai, X., Yu, H., *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*, URL: http://eprint.iacr.org/2004/199.pdf, Accessed August 2004.

[WIK01] *SHA-1 (Secure Hash Algorithm).* Wikipedia: The Free Encyclopedia URL: http://en.wikipedia.org/wiki/SHA-1, Accessed August 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Director, Marine Corps Research Center, MCCDC,
   Code C40RC
   Quantico, Virginia

4. Director, Training and Education, MCCDC
   Code C46
   Quantico, Virginia

5. Marine Corps Tactical Systems Support Activity
   (Attn: Operations Officer)
   Camp Pendleton, California

6. George Bieber
   OSD
   Washington, DC

7. RADM Joseph Burns
   Fort George Meade, MD

8. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

9. CDR Daniel L. Currie
   PMW 161
   San Diego, CA

10. LCDR James Downey
    NAVSEA
    Washington, DC

11. Richard Hale
    DISA
    Falls Church, VA

12. LCDR Scott D. Heller
SPAWAR
San Diego, CA

13. Wiley Jones
OSD
Washington, DC

14. Russell Jones
N641
Arlington, VA

15. David Ladd
Microsoft Corporation
Redmond, WA

16. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

17. Steve LaFountain
NSA
Fort Meade, MD

18. Dr. Greg Larson
IDA
Alexandria, VA

19. Penny Lehtola
NSA
Fort Meade, MD

20. Ernest Lucier
Federal Aviation Administration
Washington, DC

21. CAPT Sheila McCoy
Headquarters U.S. Navy
Arlington, VA

22. Dr. Vic Maconachy
NSA
Fort Meade, MD

23. Doug Maughan
Department of Homeland Security
Washington, DC

24. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

25. John Mildner
SPAWAR
Charleston, SC

26. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

27. Dr. Ralph Wachter
ONR
Arlington, VA

28. Jessica Watts
Cisco Systems, Inc.
Austin, TX

29. Mike Wenstrom
Cisco Systems, Inc.
Austin, TX

30. David Wirth
N641
Arlington, VA

31. Daniel Wolf
NSA
Fort Meade, MD

32. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

33. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

34. J.D. Fulp
Naval Postgraduate School
Monterey, CA

35. LtCol D.F. Overton, USMC
Naval Postgraduate School
Monterey, California

36. Michael A. Sherman
Naval Postgraduate School)
Monterey, CA