Department of Energy

CIAC

Computer Incident Advisory Capability

UCRL-TR-206168

High-end Home Firewalls

CIAC-2326

William J. Orvis

September 2003

Lawrence Livermore National Laboratory

DISCLAIMER

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

This work was performed under the auspices of the U.S. Department of Energy by University of California Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48 between the U.S. Department of Energy (DOE) and The Regents of the University of California (University) for the operation of UC LLNL. The rights of the Federal Government are reserved under Contract 48 subject to the restrictions agreed upon by the DOE and University as allowed under DOE Acquisition Letter 97-1.

TABLE OF CONTENTS

DOCUMENT CONVENTIONS

Characters you type exactly as shown are in **bold** type. This includes commands, paths, and switches. The names of user interface elements are also bold, such as the names of dialog boxes and long program names.

Variables for which you must supply a value are in *italic*.

Code samples are in `monospaced` font.

Boxed Notes provide relevant information that is not directly part of the current thread.

> Security Tip – Security tips and information related to the current thread.
>
> Warning – Something to worry about concerning the current thread.
>
> Tech Note – Other information related to the current thread but that is not security related.

High-end Home Firewalls
CIAC – 2326

William J. Orvis

1 OVERVIEW

Networking in most large organizations is protected with corporate *firewalls* and managed by seasoned security professionals. Attempts to break into systems at these organizations are extremely difficult to impossible for an external intruder.

With the growth in networking and the options that it makes possible, new avenues of intrusion are opening up. Corporate machines exist that are completely unprotected against intrusions, that are not managed by a security professional, and that are regularly connected to the company network. People have the option of and are encouraged to work at home using a home computer linked to the company network. Managers have home computers linked to internal machines so they can keep an eye on internal processes while not physically at work. Researchers do research or writing at home and connect to the company network to download information and upload results.

In most cases, these home computers are completely unprotected, except for any protection that the home user might have installed. Unfortunately, most home users are not security professionals and home computers are often used by other family members, such as children downloading music, who are completely unconcerned about security precautions. When these computers are connected to the company network, they can easily introduce viruses, worms, and other *malicious code* or open a channel behind the company firewall for an external intruder.

In the same vein as home computers, small (< 10 users), remote company offices and workers on travel also have vulnerable machines. These systems also have the same problem in that the machines are not well protected and can make a hole to the network behind a company firewall for an intruder to use.

To protect these systems requires training, antivirus software, anti *adware* software, anti *spiware* software, *software firewalls*, and *hardware firewalls*. All of these pieces need to be professionally managed in a system to protect a home network from different threats.

This paper discusses the high-end, hardware, home firewalls and their use in a home or small office network. The high-end home firewalls are characterized by their capability to be remotely managed and that they do real *stateful packet inspection* rather than simple blocking. The high-end home firewalls are actually the low-end of corporate firewall product lines and have many of the characteristics of the corporate firewalls including similar command sets and management capabilities.

There are more systems than the three described in this paper that could be considered high-end home firewalls however, the three described here should give you a good idea as to the costs and capabilities of this class of firewall. It will also discuss their capability to be remotely managed by a security professional, which should significantly improve the security of the home or small office network that resides behind it.

2 INTRODUCTION

Firewalls used in the home and small office environments for remote access computing come in two different types:

- Software Firewalls – Programs that run on the machine being protected to filter incoming and outgoing connections. They normally do not protect an internal subnet unless that subnet is using the protected machine as its gateway to the Internet. *NAT (Network Address Translation)* and *DHCP (Dynamic Host Configuration Protocol)* services are not included in software firewalls but are provided by modern operating systems used as a gateway to the Internet.

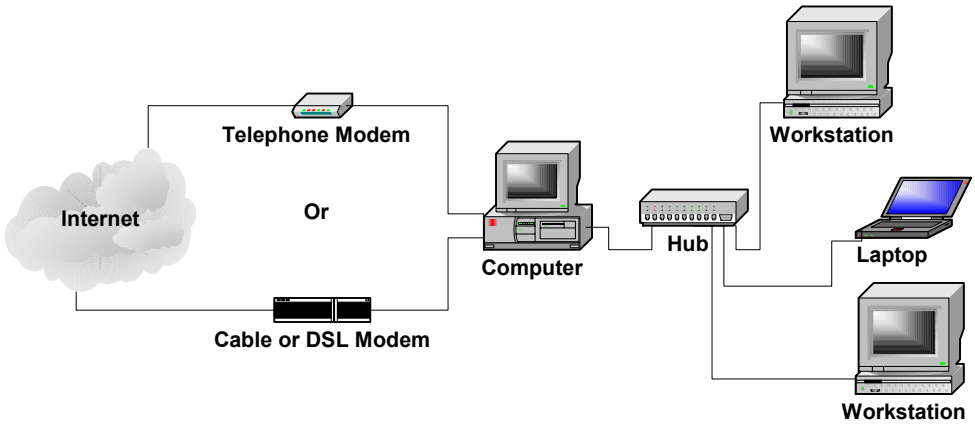
- Hardware Firewalls – A hardware appliance that connects between an internal subnet and an external network, usually the Internet, such as a *cable* or *DSL modem*. Some have the capability to use telephone modems to connect to the Internet. They protect a whole subnet rather than a single machine. They provide NAT and DHCP services to allow the machines on a subnet to share a single IP address.

This paper is primarily concerned with the high-end, hardware, home firewalls, what they do, and when you would need them. Appendices A, B, and C demonstrate how to create IPSec and PPTP tunnels between systems.

2.1 SOFTWARE HOME FIREWALLS

Software firewalls run on the machine being protected, filtering all incoming and outgoing connections to the Internet. All incoming packets must be examined to see if they are allowed or are part of an existing connection. Outgoing packets are examined to see if they are allowed, that is, they are coming from a process that is allowed to connect to the Internet and that they are not going to a blocked site. Allowed packets are then routed to the appropriate process or network connection.

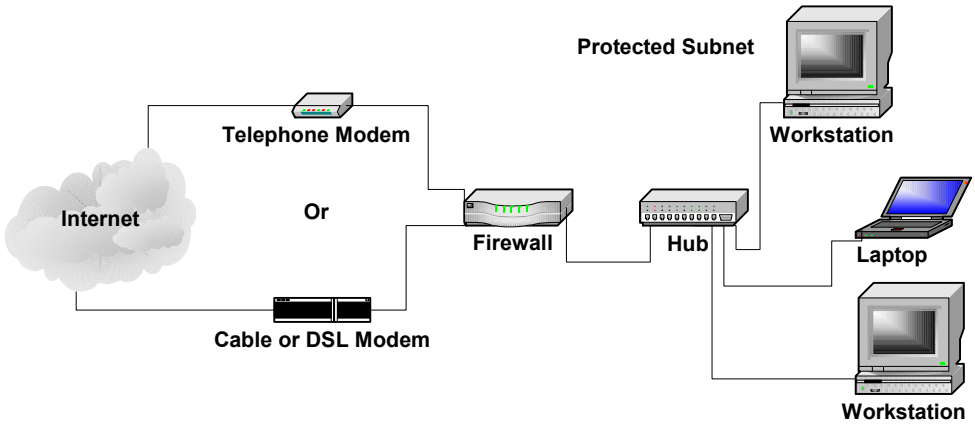
Most modern systems have the capability to be a *gateway* to the Internet for a subnet of home systems. They do this by *routing* packets from the Internet connection interface (a modem or an Ethernet connection to a cable or DSL modem) to a second interface for the internal network. The second interface is usually an Ethernet card that connects to a *hub* or *switch* and then to the machines on the internal subnet. The routing machine must generally supply DHCP and NAT services to the internal network. A software firewall on the gateway machine must filter the packets for that system and all the systems on the protected subnet. Providing these services slows the gateway machine, depending on the amount of packet traffic it must filter and route.



A feature of software firewalls is that on the protected system they can know what process on the protected machine is trying to connect to the network and can block or allow that connection based on a list of processes that are allowed to connect to the network. Hardware firewalls can only see what port is being used to open a connection and not what process is actually using that port. For example, if the mail client program (such as Eudora or Outlook Express) is connecting to the mail *port* (25) on a remote mail server that would be considered normal and would be allowed. If, on the other hand, the program xyzzy.exe tries to connect to port 25, it would be blocked unless it was specifically added to the list of allowed processes. A hardware firewall could only see that port 25 was being used.

2.2 HARDWARE HOME FIREWALLS

Hardware firewalls are separate hardware appliances on a home subnet that provides a gateway to the network's Internet connection. As such, the services they provide do not slow any of the systems on the subnet. The hardware home firewalls, at a minimum, provide NAT and DHCP services to the protected network as well as blocking of incoming sessions. As they are separate from the machines they protect, they cannot know what application on a system is trying to connect to the Internet only what port is being used. Some hardware firewalls can block outgoing connections based on the port number the connection is using.



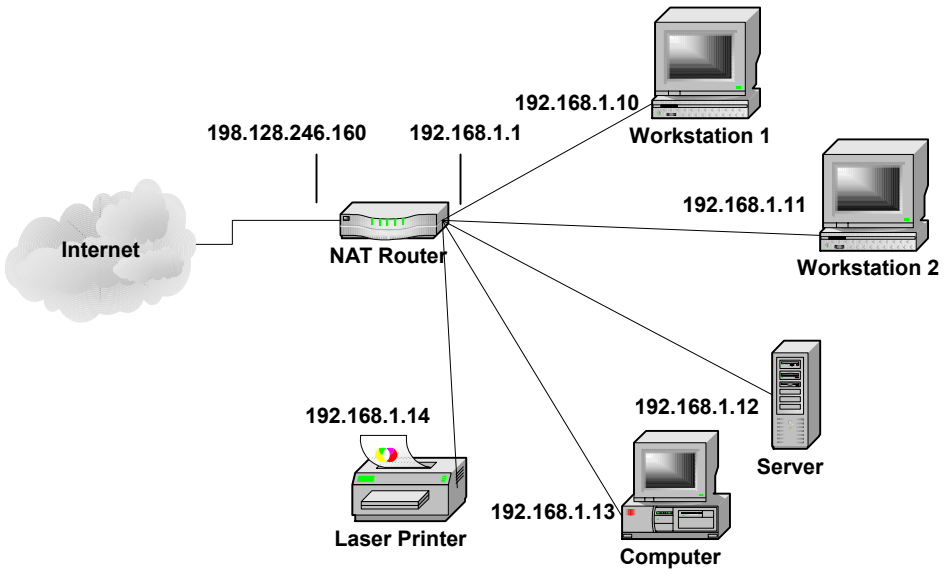
Hardware home firewalls can be divided into two general classes, high-end and low-end. Though there is actually a whole range of hardware firewalls for the home or small office with prices from around $50 to $1000, depending on the features.

2.3 LOW-END HOME FIREWALLS

The low-end home firewalls generally cost in the range of $50 to $200 and are built around NAT Router technology. NAT router technology allows multiple machines on a subnet to share a single IP address when connecting to an external network, such as the Internet. A NAT router can only open outgoing sessions so this, in itself provides a basic firewall by blocking all incoming and allowing all outgoing *sessions*.

> **Tech Note:** When we say a firewall blocks all incoming sessions and allows all outgoing sessions, we are not talking about individual packets, but about the direction traveled by the initial packet that started the session of two-way communication. That is, if a session is opened by an internal machine to an external machine, all packets that are related to that session, no matter what direction they are actually traveling, are part of an outgoing session and are allowed through the firewall. If a machine on the outside attempts to open a connection to an internal machine, that would be the start of an incoming session and would be blocked.

A NAT router is configured as shown in the following diagram. The internal, protected subnet uses a selection of subnet addresses taken from one of the private subnets (for example, 192.168.1.x). The external address of the NAT router is a public address such as 198.128.246.160. If DHCP is turned on, the NAT router assigns an IP address to each of the internal systems when it is turned on. If you don't use DHCP, you must manually assign an IP address to each of the internal machines.



When an internal system wants to connect to an external system, it connects through the NAT router which is the gateway to the Internet. The NAT router takes the packet from

its internal interface and changes the "source" address to the router's external address, assigns a high-numbered source port, and then passes the packet to the external network. The external system thinks the packet came from the NAT router and directs any replies back to the high-numbered port on the router. When the NAT router receives an incoming packet at a high-numbered port and from the machine it opened that high-numbered port for, it readdresses the packet to the internal system that started the session and passes it to the internal network. Thus, the internal and external systems communicate with each other and don't realize that there is a router in between that is readdressing the packets.

If, on the other hand, an external system without an existing open session sends a packet to the firewall, it will be dropped because there is no open session to tell the NAT router which internal machine to route the packet to. Even if the external machine tries to use the port number of an existing session to a different machine, the packet will still not pass as both the external machine name and the port must match the system that opened the session. If the external system tries to use the private address of the internal system, the packets will be blocked at the first router they hit and will probably never make it to the NAT router.

Tech Note: Several blocks of addresses in the IP address space are designated as *private* and should not be routed out of a single customer's network. The private addresses are available for any customer to use and assign in any way that they want with the caveat that they will not be recognized or routed outside of that customer's network. The result is that while there can be only one machine on the Internet with the address 198.128.246.160 (www.llnl.gov) there can be many machines with the address 192.168.1.1. The private address ranges are:

10.0.0.0 – 10.255.255.255	One *class A subnet*.
172.16.0.0 – 172.31.255.255	Sixteen *class B subnets*.
192.168.0.0 – 192.168.255.255	Two hundred fifty six *class C subnets*.

The least expensive hardware, home firewalls are simply NAT routers and let that capability provide the firewall function. Slightly more expensive hardware, home firewalls actually do stateful packet inspection to control incoming and outgoing connections. They all provide NAT and DHCP services and may do NAT in addition to the stateful packet inspection.

Another capability of the low-end home firewalls is the ability to proxy an internal service to the outside world. A *proxy server* makes an internal server, such as a web server, appear to be on the outside of the firewall. This allows incoming connections from the Internet to pass through the firewall and connect to the internal server. Only the proxied connections are allowed through and only one server of each type can be proxied to the outside. That is, if a web server is proxied to the outside, incoming connections to the web server port (80) on the outside of the firewall are routed to the web server on the inside of the firewall. Incoming connections to other ports are still blocked. If you want to make a second web server available on the outside, you will have to place it on a non-standard port such as 1080 instead of 80 because port 80 is already in use.

Beyond these basic services, as the price goes up low-end home firewalls add *print servers*, *url blocking* (blocking access to offensive websites), virus scanning, and other similar capabilities. Most of these extra capabilities require a paid subscription of some kind to keep the service up to date.

2.4 HIGH-END HOME FIREWALLS

The high-end, hardware, home firewalls are distinguished by the fact that they are actually small versions of existing corporate firewalls. They range in price from $400 to about $1000. For example, the Sofaware S-Box contains a Firewall-1 enforcement module. In most cases, these small versions do everything the corporate firewalls do, they are just not as fast and cannot handle as many users, open sessions, etc. They are generally configured in exactly the same way as the larger, corporate versions.

The high-end home firewalls do everything the low-end home firewalls do, including NAT, DHCP, and proxies. In addition, you can rewrite the rule sets to control not only the incoming connections but outgoing connections as well. For example, you could block outgoing connections from all the known backdoor ports to prevent your system from being used even if you have inadvertently installed the backdoor.

Proxies can also be better controlled using firewall rules. The proxies created by the low-end home firewalls are accessible to anyone who can access the external port on the firewall. Using rules in the high-end home firewalls, you can specify exactly who on the outside can connect to the proxy, significantly reducing your risk of compromise.

Another capability of the high-end firewalls is *VPN*. VPN is a way to create an encrypted pipeline from the home network, through the Internet, to another firewall or to a company's internel network. Systems on the home network then appear to be on the company network making access to resources much easier and protecting all communications between the home network and the company network.

> **Tech Note:** VPN (Virtual Private Network) is a method of tunneling packets through the Internet to some protected internal company network. The tunneling process works by detecting connections directed to the internal network. Those packets are completely encrypted, including the headers and placed in the body of a new packet. That new packet is then directed out onto the Internet to the company network. When a tunneled packet is received, it is authenticated, decrypted, the source IP address is changed if needed, and the packet is placed on the company's internal network. Packets going in the other direction are treated in the same way. As far as the systems on either end of the tunnel are concerned they are on the same subnet while they may actually be far apart.

In addition to more flexible rules and VPN, the high-end home firewalls have the added advantage that they can be remotely managed using the same industry standard management software as is used on the corporate versions. This capability is of special interest to companies who have employees and others working at home and other remote sites. The company security managers can then control the configuration of the remote

firewall to make sure it is up-to-date and that the rules adequately protect the remote subnet and by extension the company network.

3 WHAT KIND OF FIREWALL DO YOU NEED?

So, what kind of firewall do you need; high-end or low-end? The choice between a low-end and a high-end home firewall is largely one of control and connectivity needs. The low-end home firewalls block all incoming connections, allow all outgoing connections, and you cannot make more than minor adjustments to those rules. The high-end home firewalls have extremely flexible rule sets that can control not only the direction of communications, but who can make connections to what services in either direction. The high-end home firewalls can also be centrally managed.

For the average Internet user, one of the low-end home firewalls provides more than enough capability to protect a home network, including a home network that is occasionally connected to a company's internal network. The firewall keeps most attacks out of your network and some up-to-date antivirus software keeps out most Trojans, viruses, and worms. Combine this with a software VPN product and the user can connect to an internal company network and safely do work. All of this can be done for less than $200 per seat (not including the VPN server at the company).

The home user who connects more often to the company network or who is continuously connected to the company network should consider a high-end home firewall. Also, the home user who needs to allow specific external systems to connect to his system should also consider a high-end home firewall. Lastly, home users who are incapable of managing their own home network security should either get a low-end home firewall that requires little configuration or get a high-end home firewall and let the security managers at their company manage their network.

For example, if a home user needs to continuously monitor a work system, a high-end home firewall makes the most sense. By adding additional rules, the home user can allow the remote system being monitored to open a connection to the home system without opening up that connection to the whole world.

If a company needs more assurance that a home network is correctly configured before that network is allowed to connect to a company network, they should consider the high-end home firewalls. If you have a company requirement that all home systems are managed by company security experts, the high-end home firewalls make the most sense as they are configured with the same tools those experts currently use to manage the company firewalls.

One more thing to consider is that it is possible to create a VPN tunnel from some Windows and other systems to a company firewall or router without the need for a home firewall or a software VPN solution. Using the IPSec configuration options within Windows you can add the rules necessary to force all network traffic to go through the company network. The problem here is that it is difficult to configure and does not scale well to large numbers of machines.

4 VPN; WHAT IT IS AND HOW IT WORKS

VPN (Virtual Private Networking) is a set of protocols for *tunneling* information from one network to another and for authenticating the users at each end of the tunnel to insure that the data going through the tunnel is coming from and going to the expected locations.

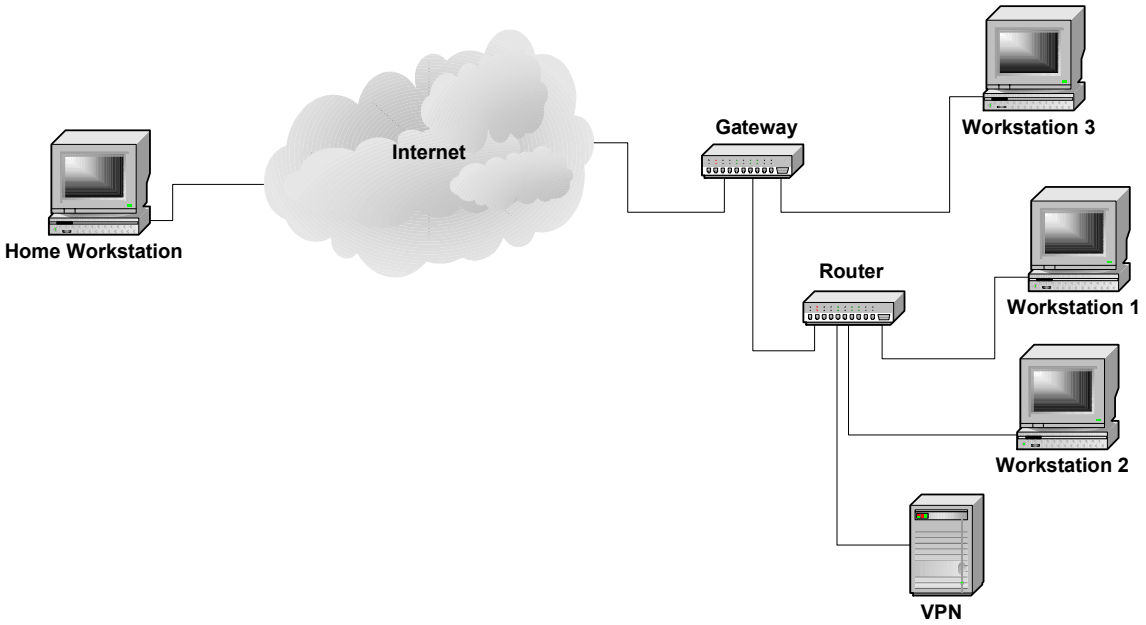
4.1 TUNNEL BASICS

Tunneling information between networks involves encrypting packets at one end of the tunnel, passing them through the tunnel, and decrypting them at the other end. This tunneling makes the systems at each end of the tunnel appear to be on the same subnet while they are actually on two different subnets, often with the Internet in between.

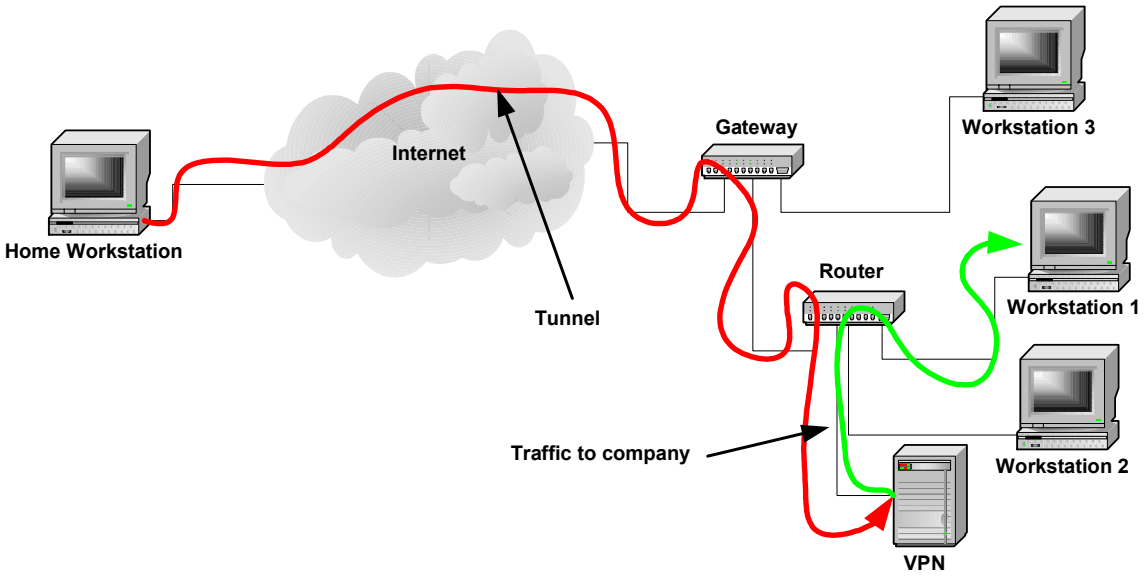
Tunnels are implemented with rules in a hardware firewall or filters in the IP stack of the sending machine. When these rules or filters determine that an outgoing packet is bound for a machine that is on the other side of the tunnel, the packet is diverted into the tunneling software. The tunneling software encrypts the whole packet, including all the headers. This encrypted packet becomes the data portion of a new packet that is sent to the machine at the other end of the tunnel. The machine at the far end of the tunnel, receives the packet, decrypts it and examines the headers of the decrypted packet. Examining the headers tells where the packet is bound in the remote network. Depending on the configuration, the system at the far end of the tunnel may change the address of the source system in the header before placing the packet on the remote network for delivery.

> **Security Tip:** There is not a big difference between a *firewall rule* and a *filter*. In general, a filter contains the information needed to select certain packets from the packet stream. Those selected packets are then passed on to another object that does something with them. A rule contains both the filter information plus what to do with the selected packets. They are actually just two different analogies for describing the action of selecting certain packets and doing something with them.
>
> In the rule analogy, a packet is passed down a set of rules. The first rule to match a packet fires and performs whatever task is indicated in the rule.
>
> In the filter analogy, packets go through a stack of filters. If a packet matches a filter, they are diverted out of the stack to be processed.

Consider the figure below. A home user connects through the Internet to the company's external gateway router (Gateway) to machines inside the network. To protect the company network, the Gateway should also include a firewall that blocks most incoming connections. To connect to the inside, there must be a rule in the Gateway firewall that allows the home user's connections to come in. A problem here is that the home user's connection through the Internet is in the clear and could be listened to by anyone along the path between the home workstation and the destination workstation within the company network. Incoming connections can also be spoofed to cause a denial of service attack or to allow an intruder into the internal network.

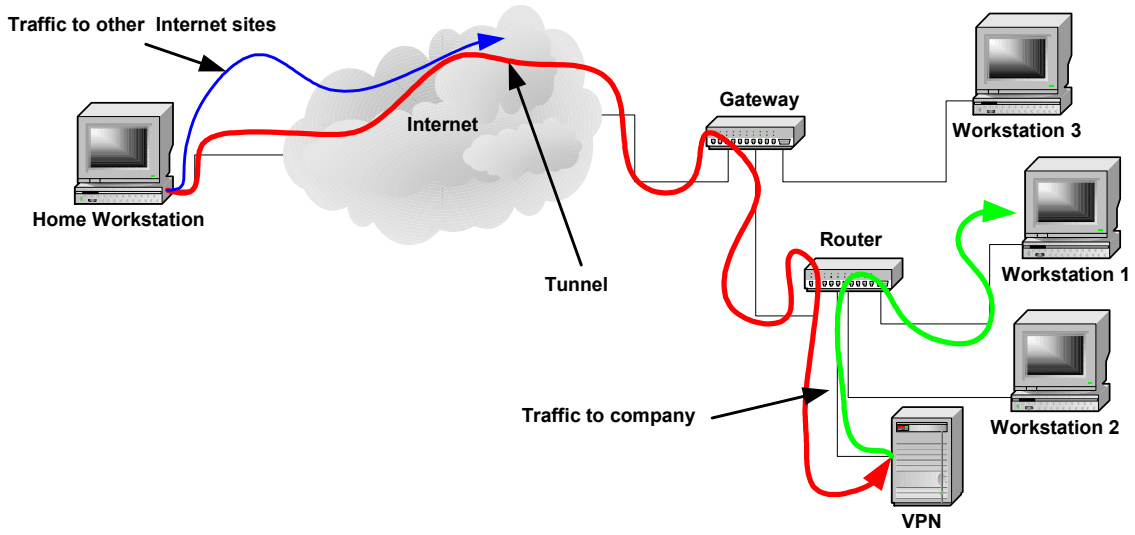


To fix this problem the home user would open a VPN tunnel to the VPN server within the company network. The firewall would have a rule to allow encrypted VPN connections into the company network rather than clear connections from a home user. All traffic from the home workstation would go through the tunnel to the VPN computer which would decrypt the packets and put that traffic on the internal network. The home workstation would then logically appear to be at the same location as the VPN server on the internal network and would communicate with other machines on the internal network as if it were there. As shown below, a connection from the home workstation to Workstation 1 involves sending packets through the tunnel to the VPN server where the tunnel ends. The packets are then sent in the clear to Workstation 1 over the company network. Connections to other internal systems proceed in the same manner.

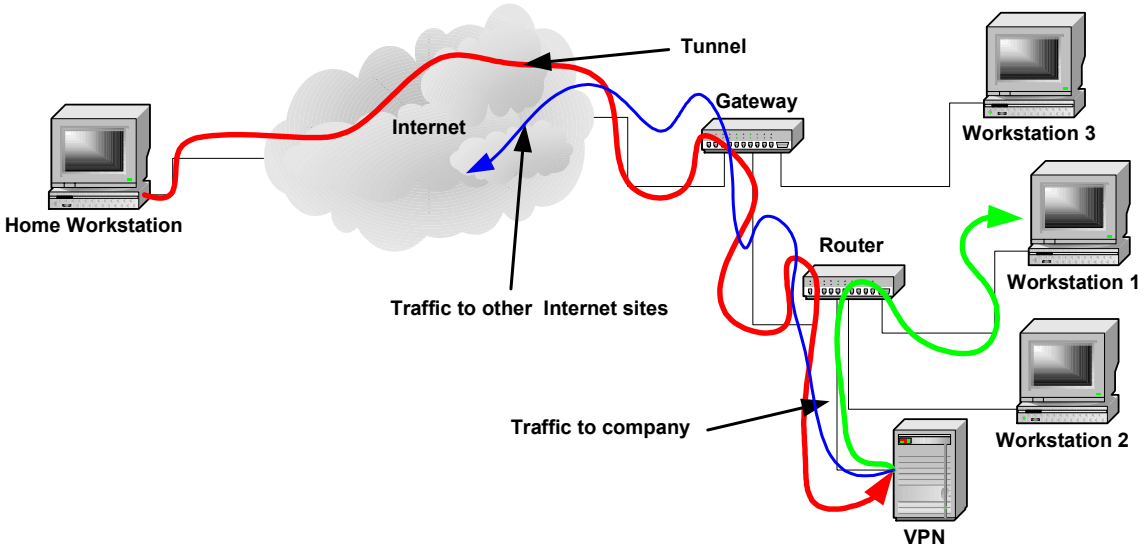


4.2 SPLIT TUNNELING

When implementing a remote VPN tunnel to an internal network, you need to decide if you want all communications from the remote system to go through the tunnel or only those directed to the company network. One method, called *Split Tunneling*, directs all packets to the company network to go through the tunnel and packets going to other Internet sites to go directly there as shown below. A problem with this setup is that an intruder can come into the system from the Internet and then go through the tunnel to get inside the company network. We have seen this happen in a case with a remote user who had a dial-up Internet connection and an ISDN connection to a company site.



Routing all the remote users traffic through the VPN tunnel is safer as all the packets must traverse the company firewall as shown below where they can be inspected and blocked if necessary. The tradeoff is that this increases the activity of the company firewall.



4.3 VPN PROTOCOLS

There are three main protocols used to create VPN tunnels: *Point to Point Tunneling Protocol* (*PPTP*), *Layer 2 Tunneling Protocol over IPSec* (*L2TP/IPSec*), and an *IP Security* (*IPSec*) Tunnel. PPTP is the most commonly available protocol while L2TP/IPSec has better encryption. IPSec has good encryption but is basically a machine to machine protocol.

Probably the most important part of setting up a Tunnel with a remote user is establishing the identity of that user. Breaking the encryption used in a protocol is much more difficult than getting the username and password of the user at the end of a Tunnel. Thus, the better your authentication, the more secure the tunnel.

The object of a VPN is to make a computer appear to be connected to a local, private network even though there is a large, public network (such as the Internet), between it and the private network. To do so, you need to maintain a session between a system and the remote network, protect the packet contents as they pass over the public network, validate that the packet has not changed, and authenticate the user so you know who you are communicating with.

When protecting a packet of information for transmission over a public network, there are two modes of operation used, Transport Mode and Tunnel Mode. In transport mode, only the body of the packet is encrypted. The header, which contains the source and destination addresses and the source and destination ports, is unchanged. An intruder examining the packet while it crosses the public network will not be able to see the packet contents but will know where it came from, who it is going to, and what service is handling the communication (for example, port 80 would be the world wide web).

In tunnel mode, the whole packet destined to a remote system is encrypted. That encrypted packet is then encapsulated within a new packet that is sent to the remote end of the tunnel. At the remote end, the packet is decrypted and placed on the remote network. An intruder capturing one of these packets will only know the addresses of the ends of the tunnel.

4.3.1 Point to Point Tunneling Protocol (PPTP)

The Point to Point Tunneling Protocol (PPTP) is an extension of the Point to Point Protocol (PPP) to allow it to be routed over a network. The PPP protocol is designed to allow a computer connected via a serial link to another computer to appear to have a network connection on the same network as that other computer. It was primarily designed for computers making modem connections into a network. In PPTP, the PPP *datagrams* are encapsulated in IP Protocol 47 GRE packets so that they can be routed over a network. PPTP also adds encryption to the protocol so that it is protected while it is being routed through a network.

PPTP uses TCP/IP port 1723 to negotiate and control the tunnel and IP Protocol 47 Generic Route Encapsulation (GRE/IP) to carry the tunnel data (See Microsoft

Knowledge Base Article 241251, *VPN Tunnels - GRE Protocol 47 Packet Description and Use* http://support.microsoft.com/?kbid=241251). The PPTP tunnel can package and transport any other networking packet type. PPTP is available on all Windows systems, Macintosh OS X, and Linux systems.

A description of the Microsoft implementation of the PPTP tunnel can be found in the Knowledge Base Article 241252, *VPN Tunnels - PPTP Protocol Packet Description and Use* (http://support.microsoft.com/default.aspx?scid=kb;EN-US;241252). The RFC for PPTP can be found at, ftp://ftp.isi.edu/in-notes/rfc2637.txt

Appendix C demonstrates the creation of a PPTP tunnel between a workstation and a firewall.

4.3.2 L2TP/IPSec

L2TP normally uses UDP/IP port 1701 which is not a problem over a serial link where data is unlikely to be lost. However when creating a L2TP tunnel over the Internet, you need to have a transport protocol that assures delivery. By running L2TP over an IPSec tunnel (a TCP/IP protocol), you get the assured delivery that is not available with UDP alone.

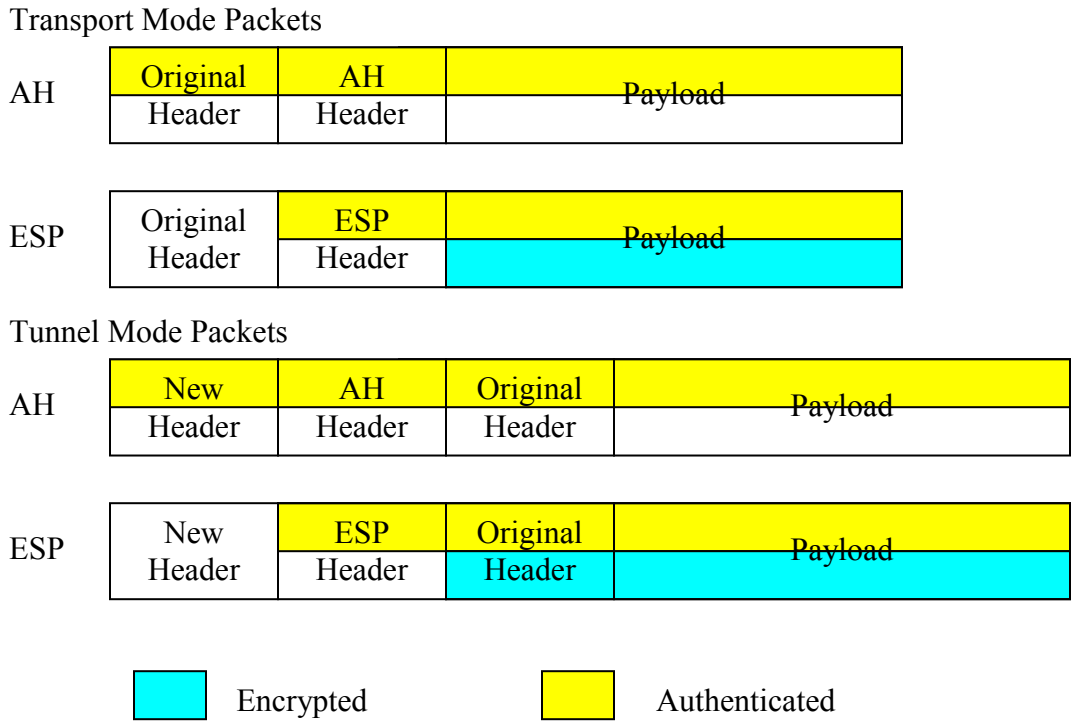
L2TP/IPSec is built in to Windows 2000 and Windows XP and is available as an addin for other versions of Windows. For more information, see the Microsoft Knowledge Base Article – 324915, *Description of the Microsoft L2TP/IPSec Virtual Private Networking Client for Earlier Clients* (http://support.microsoft.com/default.aspx?scid=kb;en-us;324915). The RFC for L2TP/IPSec can be found at, ftp://ftp.isi.edu/in-notes/rfc2661.txt.

4.3.3 IPSec Tunnel

IPSec is a suite of protocols for securely transporting packets from one machine to another. That is, it is a machine to machine tunneling protocol. Within the protocol itself, there is nothing for maintaining a session or authenticating users. These things must be done separately by the applications sending information through the tunnel. There is authentication of the endpoints of the tunnel so you know what machine you are connecting to. Some implementations have added the capability to keep a tunnel open by sending keep alive packets every few seconds and for authenticating users. An IPSec tunnel has a set of filters and rules. The filters examine each packet going to or from a system. If a packet matches a filter, the rule associated with that filter is applied. The rule consists of encryption and validation protocols to apply to the packet.

The method of establishing a tunnel can be done manually (Manual Key) or automatically. In a manual key configuration, all of the encryption and validation parameters are set manually at the ends of the tunnel. Automatic configuration is the more common way to configure the tunnel and is generally more secure as the *session key* can be changed automatically to make it much more difficult to break.

There are two modes of transport, Transport Mode and Tunnel Mode, and two transport protocols, *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*. The figure below shows how an original packet header and payload are converted for each combination of mode and protocol.



In transport mode, the original packet header is not changed. An additional protocol header is added after the original header, followed by the packet data. The protocol header tells how the packet is encrypted or not, and how it is authenticated or not. Thus, the original source and destination addresses are available in the clear.

In Tunnel mode, the whole original packet is encapsulated in a protocol packet that determines the encryption and authentication applied to the packet, and then in a new packet that specifies the source and destination for the packet. In Tunel mode, the visible source and destination addresses are the ends of the tunnel, which may not be the source and destination of the original packet.

The AH protocol only authenticates the packet contents by applying a cryptographic checksum such as *MD5* or *SHA-1*. A packet transported or tunneled with the AH protocol is not encrypted. AH is much faster if encryption of the packet data is not needed. The authentication certifies that the packet came from the source and that it has not been changed along the way.

An ESP protocol packet is encrypted and authenticated before it is sent, protecting both the contents and the authenticity of the packet. An ESP packet is encrypted with a protocol such as *DES*, *3DES*, or *AES* and then authenticated with a cryptographic checksum such as MD5 or SHA-1.

Automatic establishment of a tunnel proceeds in two phases: tunnel negotiation and data transport. Each phase can use a different encryption and validation mechanism though it is normal to use the same for both. When an IPSec tunnel starts to open, the systems at the ends of the tunnel first negotiate an encryption protocol, a validation protocol, and a Diffe-Hellman group. Commonly, the encryption protocols are DES, 3DES, or AES, and the validation protocols are MD5 and SHA-1. After the protocols are negotiated, the tunnel uses a Diffe-Hellman key exchange to generate and exchange a session key. All communication after the session key is generated are encrypted.

During Phase 2 negotiation, the encryption and validation protocols for the data exchange are also negotiated and can be different from those negotiated for Phase 1 though commonly they are the same.

At this point, each end knows all the parameters needed to operate and the tunnel opens. Tunneled packets use IP protocol 50 – Encapsulating Security Payload (ESP/IP) or IP protocol 51 – Authentication Header (AH/IP).

Appendix A shows how to open an IPSec tunnel between a Windows workstation and a firewall and Appendix B shows how to create an IPSec tunnel between two firewalls.

4.4 AUTHENTICATION

Authentication in a VPN tunnel is a certification that the systems at the ends of the tunnels are who they say they are. There are three main methods for authenticating VPN tunnels: shared secret, certificates, and Kerberos. Each method has its own strengths and weaknesses.

4.4.1 Shared Secret

A *shared secret* is essentially a password that is known by the systems at both ends of the tunnel. A shared secret is considered the least secure of all the methods as the secret tends to be a static value that could be discovered by someone and used to break into the system protected by the tunnel.

4.4.2 Certificates

Security certificates use *public key cryptography* to validate the ends of the tunnel. Each end of the tunnel has a secret key and a public key. The system maintaining the end of a tunnel gets the public key for the other end of the tunnel from a key registry. The keys are then used to authenticate the tunnel.

4.4.3 Kerberos

Kerberos is another kind of certificate authority where the Kerberos server provides a certificate for each end of the tunnel. The certificate is then used to validate the setup of the tunnel.

4.5 OPEN-ENDED TUNNELS

In many cases, the address of the machine at one end of a tunnel is not known when the system is setup. Most commonly this is a system whose address is served by a DHCP server. Most home systems work this way in that they do not get their IP address until they dial-in to the server. This is a difficulty as the tunnel server at one end does not know which packets to filter into the tunnel. A tunnel of this type must be opened from the system with the changing address to the system with the fixed address. In this case, the system with the changing address connects to and logs into the tunnel server with the fixed address. The process of authenticating identifies the address of the system with the changing address and the tunnel now has the information it needs and can open. This tunnel is usually kept open with keep-alive packets sent every few seconds. After the tunnel is open, new sessions can open from either end and use the tunnel.

5 SOFAWARE S-BOX (FIREWALL 1)

The Sofaware S-box is a small network appliance that contains a Firewall-1 enforcement module. Firewall-1 is one of the oldest firewall products in the market. It is developed by Check Point Software Technologies Ltd. of Ramat-Gan, Israel.

The enforcement module is the part of Firewall-1 that actively examines packets, compares them to the ruleset, and either passes or blocks them. The other parts of Firewall-1 include the ruleset editor and compiler and the compiled ruleset server. These parts are generally part of a Firewall-1 management station and are not part of the S-box package.

5.1 HARDWARE DESCRIPTION

The S-box hardware consists of a single box containing all the electronics and an external power supply. The interfaces consist of a single, Ethernet 10/100 uplink WAN port and a four port, Ethernet 10/100 LAN switch. The WAN port hooks to the external, untrusted network, such as a cable modem, DSL modem, or other network. The 4 LAN ports are for the network protected by the S-box. Additional protected ports could be obtained by branching from one of the LAN ports to a multi-port switch.

The hardware itself is a 133 MHz MIPS CPU with 32 Mbyte RAM and 8 Mbyte. flash memory. The system software is stored in the flash memory which is divided into two areas so if you trash a software update you can always reset the box and get back to the original software. The operating system is a small Linux kernel.

Throughput performance is 22 Mbits/s for unencrypted connections to NATed internal devices or 1.5 Mbits/s through a 3DES encrypted VPN.

Hardware installation consists simply of plugging the WAN port into your incoming network device, plugging the systems to be protected into the LAN ports, and plugging in the power supply. The default system comes up in a protected mode and must be configured using the built-in web interface before it can be used. Basic configuration consists of setting up the internal and external IP addresses, NAT, and the DHCP server.

Tech Note: 10-baseT and 100-baseT Ethernet ports come in two different types, uplink and downlink. The difference is that the transmit and receive wires are switched so that when you connect a straight through (pin 1 on one end connects to pin 1 on the other end and so forth) Ethernet cable from an uplink port on one system to a downlink port on another that the transmit on one system is connected to the receive on the other and vice versa. If you don't do this, the cable cannot transmit data.

Most network hardware such as hubs, switches, firewalls, and routers have an uplink port to connect to the device above it in the network hierarchy and one or more downlink ports to connect to devices below it. For example, the *WAN* port on the S-box is an uplink port and the *LAN* ports are downlink ports. The Ethernet port on the back of your computer is an uplink port.

Some hardware have a switch to change a port from one type to another, others come with a crossover cable to make the switch. Modern units automatically detect and switch to whatever kind of port they need to be.

5.2 SOFTWARE DESCRIPTION

The software in the S-box essentially consists of two modules, the Firewall-1 enforcement module and a web-based configuration and management module. The configuration and management module makes it possible to manage the hardware settings of the S-box (IP address, DHCP address range, etc.) and some of the Firewall-1 settings. Missing from the internal configuration and management software is the capability to modify the Firewall-1 policies. You can import a new policy but cannot edit an existing policy or create a new one using the built-in web interface.

Firewall-1 policies are compiled binary documents as opposed to a text list of rules. Creating or editing a Firewall-1 policy document currently requires that you have access to a Check Point, Firewall-1 policy editor and compiler. If you have a corporate version of Firewall-1 you can use the policy editor that is part of that product to create and compile a new policy which can then be imported into the S-box.

The internal software is fully upgradable by downloading a new software image file from Sofaware and uploading it to the S-box. Software updates can be done either from a computer on the protected network or from a remote management server that the S-box has been configured to accept management commands from. The box is also upgradable to different versions of the box (for example, safe@home to safe@office) by purchasing and installing a different license key. All versions of the S-box operate on the same hardware platform.

5.3 PRODUCT MATRIX

The S-box is a single hardware module that comes in four different versions and is fully upgradable from one version to another by simply changing a license key. That is, all

hardware and software for all the versions is contained in the basic product. The features of the different versions are enabled by the license key.

	Safe@home	Safe@home Pro	Safe@office	Safe@office Plus
Max. Nodes Behind Firewall	5	5	10	25
WAN Port	10/100 port	10/100 port	10/100 port	10/100 port
LAN Ports	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch
Other Ports	none	none	none	none
Authentication	Internal database	Internal database	Internal database	Internal database
VPN Encryptions Available	n/a	AES DES 3DES	AES DES 3DES	AES DES 3DES
VPN Authentication Available	n/a	MD5 SHA-1	MD5 SHA-1	MD5 SHA-1
Max. VPN Tunnels	n/a	5	10	10
VPN Type	n/a	client	client or server	client or server
Local Management	Web Interface	Web Interface	Web Interface	Web Interface
Remote Management[#]	HTTPS SMP	HTTPS SMP	HTTPS SMP	HTTPS SMP
Logging*	Basic	Advanced	Advanced	Advanced
Speed Mbits/s	22 No Tunnel	22 No Tunnel 1.5 3DES VPN	22 No Tunnel 1.5 3DES VPN	22 No Tunnel 1.5 3DES VPN
Extras	Antivirus URL Blocker	Antivirus URL Blocker	Antivirus URL Blocker	Antivirus URL Blocker
Streeet Price 5/03	$229	$299	$476	$887

[#]HTTPS = Encrypted web interface, SMP = Sofaware Management Portal.

*Basic logging consists only of logging events within the firewall. Advanced logging includes more details and allows logging in external servers such as the management server or a syslog server.

5.4 SPECIAL CAPABILITIES

In addition to the standard, firewall capabilities, the S-box comes with the capability to implement two specialty modules,

- E-mail Virus scanner
- URL filter

Both of these modules require the use of a remote management server that actually provides the capabilities. Use of the remote server is not included in the purchase price but must be contracted for separately.

The e-mail virus scanner operates by capturing all incoming e-mail packets and routing them to a remote, antivirus server. The packets are scanned cleaned in the server and returned to the S-box where they are delivered to the user. The operation is transparent to the user who only detects a slight delay when downloading e-mail.

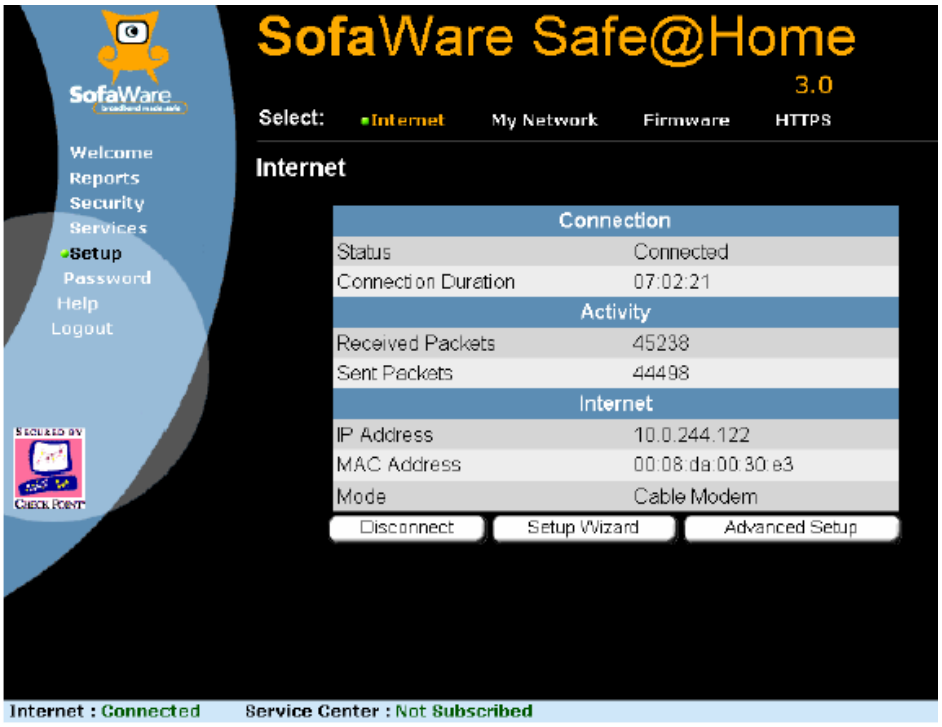
The URL filter is used to block access to a list of URLs based on the content served from the URLs. The S-box has a list of blocked URLs that it compares to the destination address of each new connection. If the address is not in the internal list, the S-box connects to a server to check if the particular connection is allowed. The result of this check is stored in the internal list for use the next time a connection is opened.

5.5 LOCAL MANAGEMENT

Local management of the S-box is accomplished using the web management console from a connection on the LAN interface. The system is initially configured as a DHCP server so configure a workstation to get its IP address using DHCP, open a web browser, and connect to the S-box. The S-box is initially configured to respond to http://my.firewall or http://192.168.10.1.

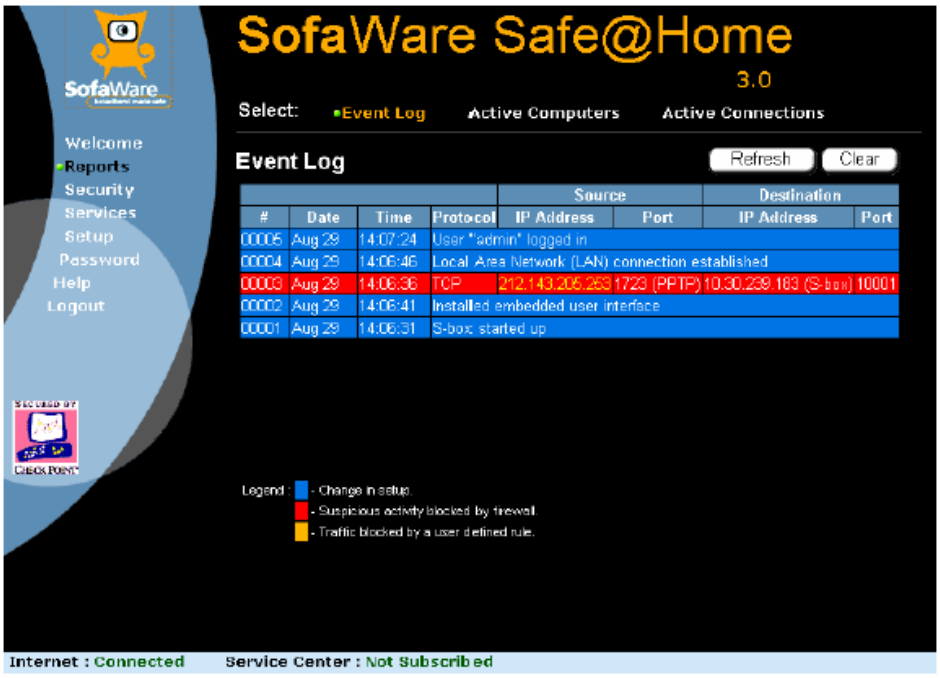
The first time you connect to the S-box you will see a configuration wizard that sets the password and networking settings of the box such as the IP addresses of its interfaces. The second time you login, you will be asked for the password you set during the initial configuration and you will see the following screen.

Along the left side are the menus you can use to make changes to the settings in the system. The setup menu brings up settings that allow you to change most of the systems networking settings such as the WAN and LAN settings. From here you can also upload a new version of the firmware and set an address for secure, remote management of the system. For the LAN settings, you can enable or disable NAT and DHCP and set the address ranges associated with these services.



Tech Note: Be careful that you don't specify a configuration that is inaccessible by your management system or you won't be able to make changes. If you do so, you must hold down the reset button on the back of the system for seven seconds to reset the box back to the factory defaults. If you do this, all settings and licenses will have to be redone.

The reports section shows the current event log plus information on currently attached systems to the LAN interface and open connections to systems on the WAN interface. The event logging shown in the image below is the only logging that is available in the safe@home system. Higher level systems allow more complete logging to a syslog server or to a remote management station.



The security section is used to select one of three security policies to apply to the system. This is one section that is different from normal, Firewall-1 policies. When the security rules are created in the Firewall-1 policy, each rule is tagged with one or more of the names: high, medium, and low. When you select high, medium, or low in the Security section of the web manager, you are selecting only those rules with the matching tags. Other rules are ignored. With this capability, you can have three different policies stored in the S-box that you can select using the web manager.

Security Tip: The three different policies stored in the S-box do not need to be high-security, medium-security, and low-security but can be any three different security policies. For example, you could have one policy for when you are on the road and another for when you are at home. The slider in the web manager will still say High, Medium, and Low so you will need to be careful that your users understand what those settings really stand for. Also, changing the policies requires that you have access to the Firewall-1 policy editor to create the compiled policy document.

Changing the level between High, Medium, and Low is the only modification you can make to the Firewall-1 policies using the web interface. However, you can override some of the policy settings by proxying systems or ports to the outside of the firewall and by setting Allow, Block, and DMZ rules using other settings in this area . The image below shows the default S-box policy displayed in the Firewall-1 policy editor. This editor is not currently included with the S-box.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	Any	Any	accept		Off	Any	Future use
2	Dynamic_GW	Any	ICMP_frag_needed	accept		High Low Medium	Any	Allow fragmented ICMP from the S-box
3	Any	Dynamic_GW	echo-request	accept		Low	Any	Allow echo requests to the S-box in Low
4	Dynamic_GW	Any	echo-reply	accept		Low	Any	Allow echo replys from the S-box in Low
5	Home_network	Any	Any	accept		Low	Any	All all outgoing traffic in Low
6	Home_network	Any	Hazards	accept		Medium	Any	Allow All trafic except NBT in Medium
7	Home_network	Any	High_Services	accept		High	Any	Allow only the following services in High: http, https, imap, pop3, smtp, nntp, ftp telnet, dns udp,ike, udp encap (2746) FW-topo (256)
8	Any	Dynamic_GW	Any	drop	Long	High Medium Low	Any	Drop and log un-authorized traffic from the Internet to the S-box
9	Home_network	Any	Any	reject	Long	High Medium	Any	Reject and log un-authorized traffic generated from the home network
10	Any	Any	Any	drop		High Medium BlockAll Low	Any	Drop all other BlockAll is for future use

For those of you who understand Firewall-1 policies, note the Install On column which determines which rules apply for each setting in the web management window. The result of these rules in combination with NAT is that no incoming connections are allowed unless they are specifically proxied to the inside. Connections to the WAN interface is

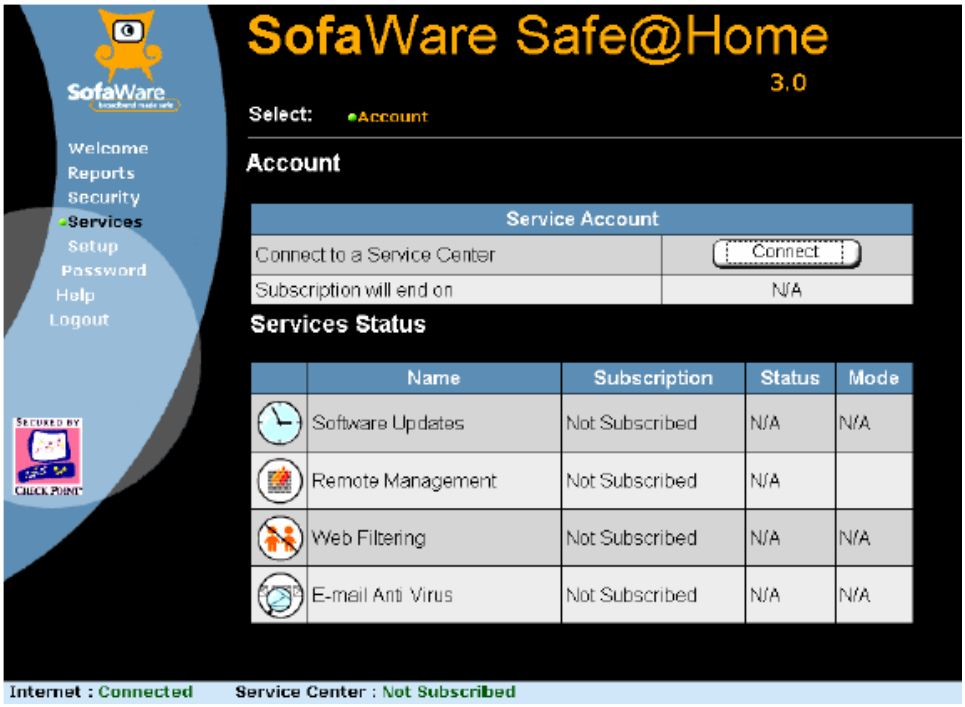
limited to ICMP echo request at the low security setting and none for medium and high. The outbound rules allow any outbound connection at the low setting, anything but NetBIOS connections (ports 137, 138, 139, 445) at the medium setting and at the high setting, only HTTP, HTTPS, IMAP, POP3, SMTP, NNTP, FTP, TELNET, DNS, IKE, port 2746 UDP, port 256 TCP. The last two ports are used by Check Point for remotely configuring systems.

As mentioned, you can only choose to implement the high, medium, or low version of the default ruleset using the web interface. You cannot change the rules themselves. To change the rules, you must have access to the Check Point Policy editor that comes with the SmartCenter product and costs several thousand dollars. If your company uses a Check Point Enterprise level firewall you have at least one copy of the policy editor. You do not have to purchase a separate copy of the policy editor for just this product but can use the policy editor included with Check Point's Enterprise product to create and save a new policy.

The security area is also where you set service proxies. If you have a service on a system on your LAN that you need to have accessible to people on the WAN, you use a service proxy. For example, if you have a web server on your LAN and you want it accessible on the WAN you would proxy port 80 on the WAN side of the S-box to port 80 on your web server. Any connections to port 80 on the WAN side of the S-box would be routed to the web server on your LAN. Alternately, you can specify a system on your LAN to be on the DMZ which receives all incoming connections instead of just those to a single service.

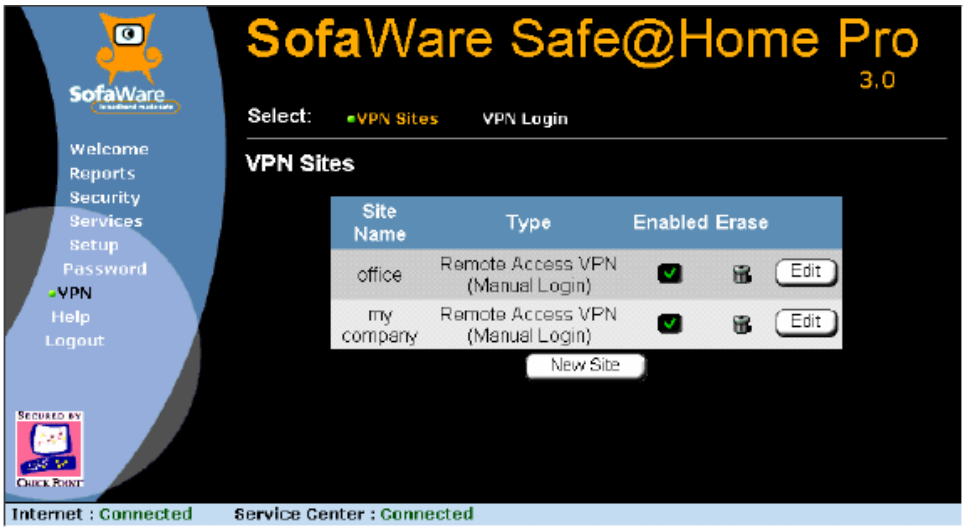
The allow and block sections allow you to create special rules that override the default rules in the firewall-1 ruleset. These rules allow you to create special cases for connections through the firewall either allowing them or specifically blocking them.

The services section allows you to add or enable several services. These services are for the most part extras that you must purchase before using. This area is also where remote management is enabled (another service).



In the VPN section, you can setup VPNs between this S-box and other systems. The @home Pro version of the S-box can only be a VPN client while the @office versions can also be servers. The VPNs implemented with these systems generally must be connected to Check Point VPN servers. Most non-Check Point VPN solutions are not compatible with the Check Point VPN clients.

Security Tip: Software based VPN clients for use with the Check Point VPN servers is available at no cost. These clients may be used to connect individual machines to a Check Point VPN server through a VPN tunnel.



5.6 REMOTE MANAGEMENT

One of the biggest incentives for getting a high-end home firewall is its capability to be remotely managed. Especially in a situation where a company has people working at home this gives the company the ability to remotely manage the firewall to insure that the settings are compatible with the company's security policy. It also reduces the risk that a less knowledgeable user will not open his home network and thus the company network to unrestricted access by the Internet.

Sofaware implements remote management using the Sofaware Management Portal, which consists of the Sofaware Management Center (SMC), the S-box additions to the Check Point policy editor, and the Sofaware Management Server (SMS).

When an S-box that has been configured for remote management starts up, it immediately connects to its management server. The S-box and the management server authenticate with each other using a shared secret. The management server contains the current settings, policy document, and firmware for the S-box. Any of these items that have changed since the last time the S-box connected are immediately updated, including uploading and installing a new version of the firmware.

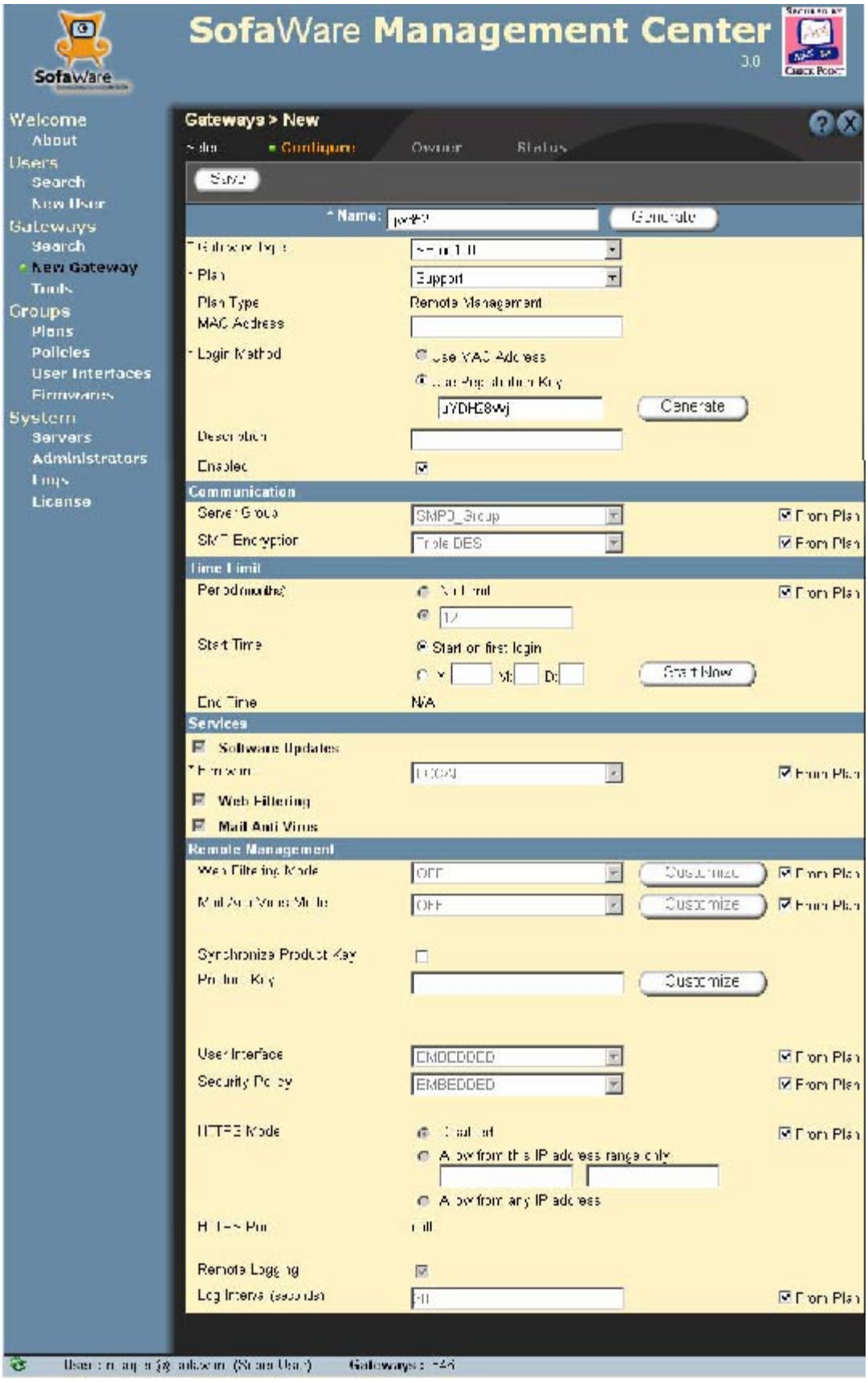
Management of the settings for an individual S-box (known as a gateway) is done using the management console. The management console, firewall policies, and S-box settings have all been designed with scalability to manage thousands of remote S-boxes in mind. While each individual S-box must be named in the manager and have a shared secret, the rules and settings can be applied to groups of S-boxes.

Management of S-boxes is based on gateways and a series of plans. A gateway describes an individual S-box and contains its unique characteristics including its shared secret and

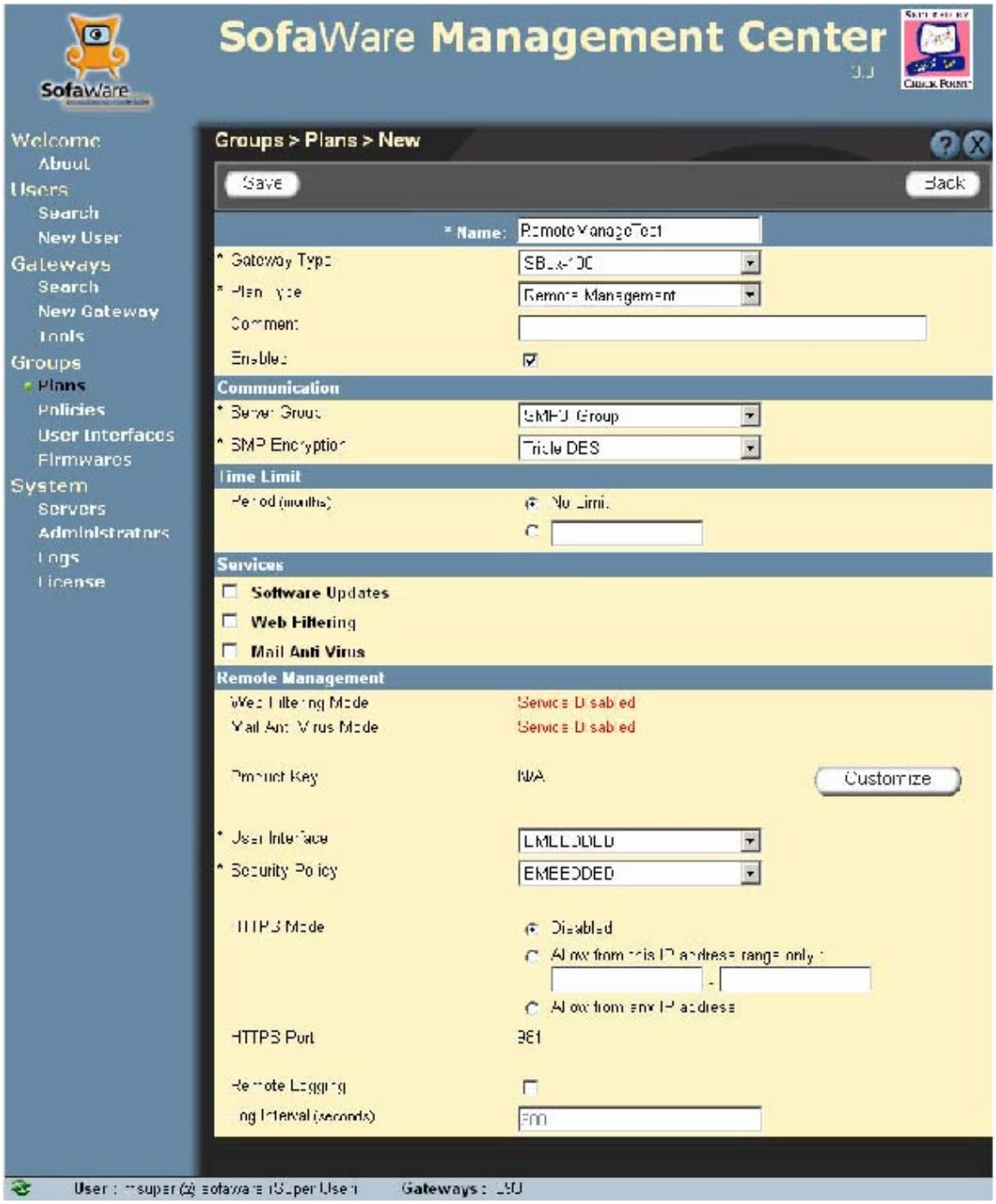
owner information. A gateway also contains a link to the plan that describes the non-specific settings for an S-box.

> **Tech Note:** Some of the plan settings can be overridden in the gateway settings so that an individual who needs a small change to a plan can do so but still remain part of a plan. Overriding a plan's settings should be done as little as possible as it breaks the scalability of the system.

The SMC is licensed according to the number of clients you are going to manage. Current licenses range from 10 clients for $2,000 to 5000 clients for $50,000.

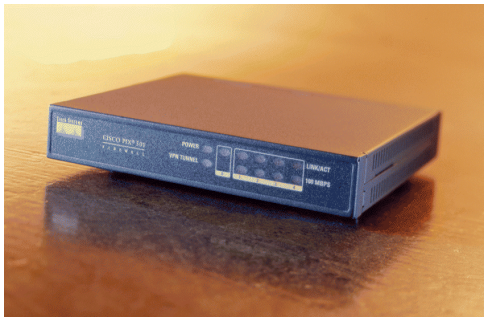

SofaWare Management Center
3.0
Welcome
About
Users
Search
New User
Gateways
Search
New Gateway
Tools
Groups
Plans
Policies
User Interfaces
Firmwares
System
Servers
Administrators
Logs
License
Gateways > New
Configure
Owner
Status
Save
Name:
Generate
Plan
Support
Plan Type
Remote Management
MAC Address
Login Method
Use MAC Address
jYDHE8wj
Generate
Description
Enabled
Communication
Server Group
SMP0_Group
From Plan
SIC Encryption
Triple DES
From Plan
Time Limit
Period (months)
From Plan
Start Time
Start or first login
Start Now
End Time
N/A
Services
Software Updates
From Plan
Web Filtering
Mail Anti Virus
Remote Management
Web Filtering Mode
OFF
Customize
From Plan
Mail Anti Virus Mode
OFF
Customize
From Plan
Synchronize Product Key
Product Key
Customize
User Interface
EMBEDDED
From Plan
Security Policy
EMBEDDED
From Plan
HTTPS Mode
From Plan
Allow from this IP address range only
Allow from any IP address
Remote Logging
Log Interval (seconds)
From Plan

A plan is a settings document consisting of generic S-box settings, a security policy, and a firmware version. When an S-box is added to a management server it is assigned a plan based on what kinds of protections the owner wants and what kinds of extra services (such as e-mail virus scanning) he has paid for. When new settings are needed or a new policy needs to be applied the changes are made to the plan which automatically makes changes to all S-boxes assigned to that plan.



Tech Note: The configuration and layout of the management server is currently undergoing significant changes to more closely tie it to the Check Point console and management tools, especially the Policy Editor.

6 CISCO PIX-501

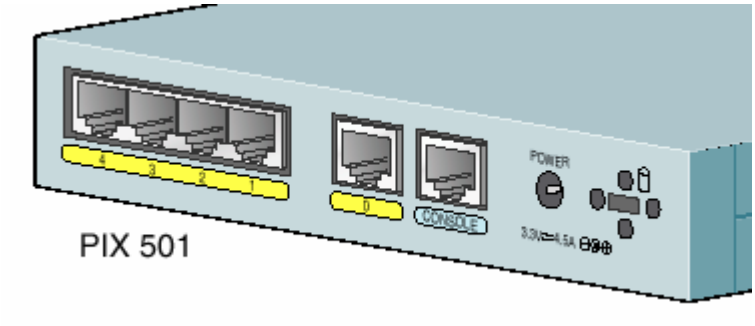


The CISCO PIX 501 is a PIX firewall that operates with the same routing engine, commands, and setup as the larger PIX firewalls. In addition to the router like PIX command language, the PIX 501 also contains a web interface for locally configuring the system using a GUI interface.

6.1 HARDWARE DESCRIPTION

The PIX 501 hardware consists of a single box containing all the electronics and an external power supply. The interfaces consist of a single, Ethernet 10-baseT uplink WAN port, a four port, Ethernet 10/100 LAN switch, and a serial console port. The WAN port hooks to the external, untrusted network, such as a cable modem, DSL modem, or other network. The 4 LAN ports are for the network protected by the PIX. Additional protected ports could be obtained by branching from one of the LAN ports to a multi-port switch. The console port is for configuring the PIX without using the LAN. The console port is most useful when you have configured the network ports in such a manner that you can no longer login to the PIX.

> **Tech Note:** Note that configuring the PIX so that you cannot login to it over the LAN ports is not difficult to do during system setup. Especially when you are changing the address settings of the LAN ports.



The hardware itself is a 133 MHz AMD SC520 CPU with 16 Mbyte RAM and 8 Mbyte. flash memory. The system software is stored in the flash memory which can be updated when new versions are available.

Throughput performance is 37 Mbits/s for unencrypted connections to NAT addressed internal devices, 6 Mbits/s through a DES VPN, 2 Mbits/s through a 3DES encrypted VPN, and 3 Mbits/s through an AES-128 encrypted VPN.

Hardware installation consists simply of plugging the WAN port into your incoming network device, plugging the systems to be protected into the LAN ports, and plugging in the power supply. The default system comes up in a protected mode and must be configured using the built-in web or command line interface before it can be used. Basic configuration consists of setting up the internal and external IP addresses, NAT, and the DHCP server.

6.2 SOFTWARE DESCRIPTION

There are essentially two software packages on the PIX 501, the command line based firewall engine and the web based PIX Device Manager which provides GUI-based settings and writes command line commands to the firewall engine. Configuration of all firewall settings can be done through either of these two interfaces. People who are comfortable with configuring routers with a command line interface will be right at home with the PIX command line interface while others can use the GUI interface. Note that the command line interface is always available at the console port so if you are unable to connect to the network ports you can configure or reset the system using the console port.

> **Tech Note:** It is very common to maintain a copy of the configuration file on the workstation you are using to configure a system. When you want to change the configuration you can issue individual commands to make the desired changes but it is more common to edit a copy of the configuration file, reset the firewall, and then upload the whole file of configuration commands, not just the changes. This is done to better track the current configuration and to make sure that the configuration can be repeated.

6.3 PRODUCT MATRIX

	PIX 501-bun-k8	PIX 501-bun-k9o	PIX 501-50-bun-k8	PIX 501-50-bun-k9
Max. Nodes Behind Firewall	10	10	50	50
WAN Port	10-baseT port	10-baseT port	10-baseT port	10-baseT port
LAN Ports	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch
Other Ports	Console	Console	Console	Console
Authentication	Internal username/ password, TACACS+, RADIUS	Internal username/ password, TACACS+, RADIUS	Internal username/ password, TACACS+, RADIUS	Internal username/ password, TACACS+, RADIUS
VPN Encryptions Available	DES	3DES, AES	DES	3DES, AES
VPN Authentication Available	MD5 SHA-1	MD5 SHA-1	MD5 SHA-1	MD5 SHA-1
Max. VPN Tunnels	5	5	5	5
VPN Type	client or server	client or server	client or server	client or server
Local Management[#]	PDM or command line	PDM or command line	PDM or command line	PDM or command line
Remote Management	HTTPS SSH SNMP CiscoWorks Solsoft	HTTPS SSH SNMP CiscoWorks Solsoft	HTTPS SSH SNMP CiscoWorks Solsoft	HTTPS SSH SNMP CiscoWorks Solsoft
Logging*	Advanced	Advanced	Advanced	Advanced
Speed Mbits/s	37 No Tunnel 6 DES VPN	37 No Tunnel 2 3DES VPN 3 AES-128 VPN	37 No Tunnel 6 DES VPN	37 No Tunnel 2 3DES VPN 3 AES-128 VPN
Extras				
Streeet Price 5/03	$445	$525	$879	$955

#PDM = PIX Device Manager (Java Application).

*Basic logging consists only of logging events within the firewall. Advanced logging includes more details and allows logging in external servers such as the management server or a syslog server.

6.4 SPECIAL CAPABILITIES

The CISCO PIX 501 is sold as a single purpose security appliance and does not currently provide any special services such as an antivirus mail scanner. It can provide URL blocking but that must be done with the firewall ruleset rather than with an extra module. Mail antivirus scanning could also be done using the routing commands to route mail packets to an external scanner and then routing back the cleaned results.

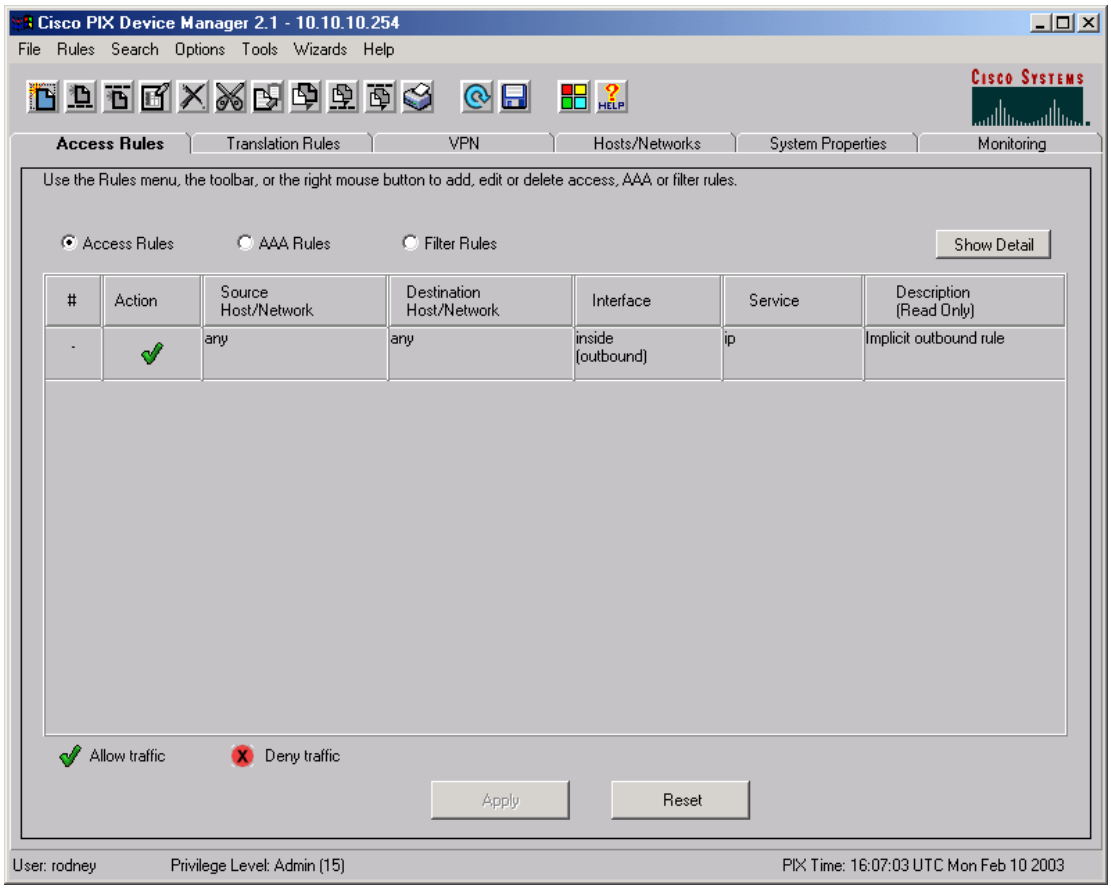
6.5 LOCAL MANAGEMENT

Local management of the PIX 501 is either through the java based GUI or the command line interface. The command line interface is accessible through the console port or through the java GUI. Selections made in the GUI interface are actually translated into text commands which are fed to the command line interface. Either interface produces equivalent results. I have found it useful to go back and forth between the two interfaces to see how changes in one affects the other.

To open the GUI, you need a workstation connected to the LAN interface that is set to use DHCP to get its address. The default address of the PIX 501 is 192.168.1.1. To startup the PIX Device Manager open a web browser and connect to

```
https://192.168.1.1/startup.html
```

Follow the instructions to set the initial settings for the PIX, including the login username and password. The next time you login, you will see a GUI interface like the following.



Visible in the image above is the default outbound rule that says all outbound connections are allowed.

The other way to add rules and settings is with the command line interface, which is a simple teletype like interface. Listing the configuration displays the commands necessary to create that configuration so if you want to backup a configuration, you simply list the configuration and save that list to a file. For example, the following is a configuration file for a PIX 501 that implements a PIX to PIX VPN tunnel.

```
:start
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname demopix
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

```
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list 90 permit ip 10.10.10.0 255.255.255.0 192.168.10.0
255.255.255.0
access-list 91 permit ip 10.10.10.0 255.255.255.0 192.168.10.0
255.255.255.0
pager lines 24
logging console debugging
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 192.168.1.101 255.255.255.0
ip address inside 10.10.10.254 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm location 10.10.10.1 255.255.255.255 inside
pdm location 192.168.1.101 255.255.255.255 outside
pdm location 192.168.1.109 255.255.255.255 outside
pdm location 192.168.1.106 255.255.255.255 outside
pdm location 192.168.1.106 255.255.255.255 inside
pdm location 192.168.1.109 255.255.255.255 inside
pdm history enable
arp timeout 14400
global (outside) 10 interface
nat (inside) 0 access-list 91
nat (inside) 10 10.10.10.0 255.255.255.0 0 0
access-group inside_access_in in interface inside
route outside 0.0.0.0 0.0.0.0 192.168.1.109 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa authentication enable console LOCAL
aaa authentication ssh console LOCAL
aaa authorization command LOCAL
http server enable
http 10.10.10.1 255.255.255.255 inside
http 192.168.1.109 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set strong esp-des esp-md5-hmac
;crypto ipsec security-association lifetime seconds 3600
crypto map toWin2k 20 ipsec-isakmp
crypto map toWin2k 20 match address 90
crypto map toWin2k 20 set peer 192.168.1.109
crypto map toWin2k 20 set transform-set strong
```

```
;crypto map toWin2k 20 set security-association lifetime seconds
28800 kilobytes 4608000
crypto map toWin2k interface outside
isakmp enable outside
isakmp key abc123 address 192.168.1.109 netmask 255.255.255.255
;isakmp identity address
isakmp policy 9 authentication pre-share
isakmp policy 9 encryption des
isakmp policy 9 hash md5
isakmp policy 9 group 2
isakmp policy 9 lifetime 1000
telnet timeout 5
ssh 192.168.1.106 255.255.255.255 outside
ssh timeout 5
dhcpd address 10.10.10.1-10.10.10.9 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
dhcpd enable inside
username rodney password TiWzUlj7GolYii.N encrypted privilege 15
privilege show level 0 command version
privilege show level 0 command curpriv
privilege show level 3 command pdm
privilege show level 3 command blocks
privilege show level 3 command ssh
privilege configure level 3 command who
privilege show level 3 command isakmp
privilege show level 3 command ipsec
privilege show level 3 command vpdn
privilege show level 3 command local-host
privilege show level 3 command interface
privilege show level 3 command ip
privilege configure level 3 command ping
privilege configure level 5 mode enable command configure
privilege show level 5 command running-config
privilege show level 5 command privilege
privilege show level 5 command clock
privilege show level 5 command ntp
terminal width 80
:end
```

These configuration commands can be typed or copied and pasted into a command line interface window in the PIX Device Manager or into the console.

6.6 REMOTE MANAGEMENT

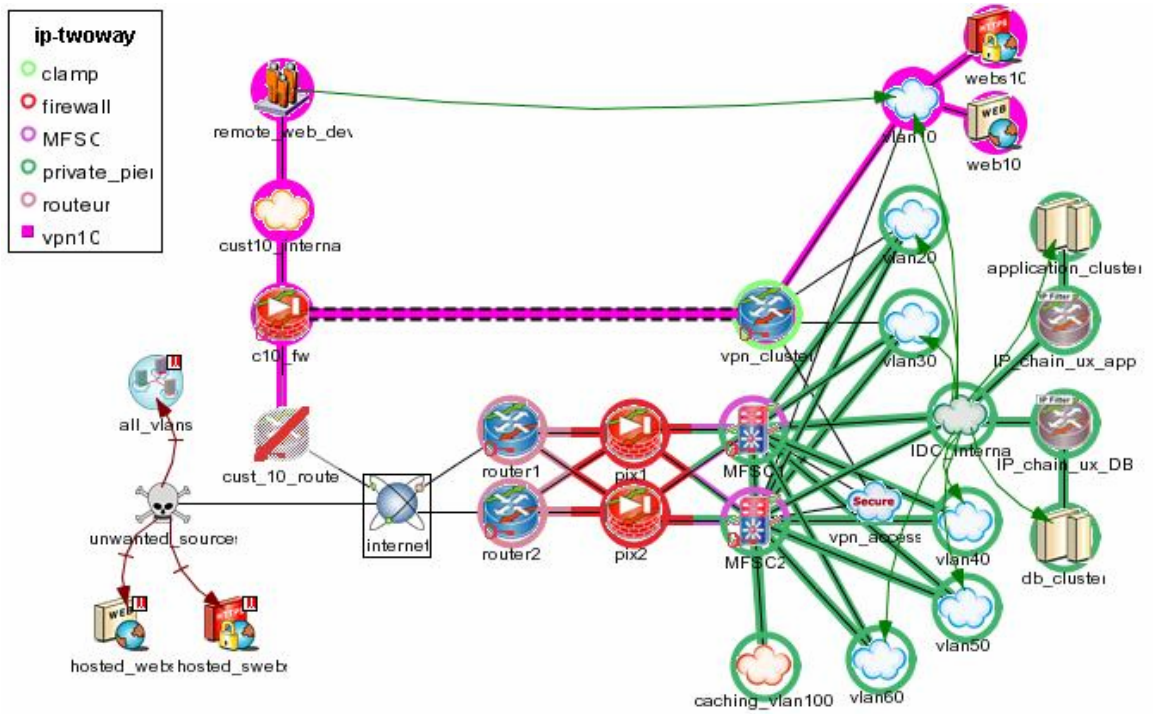
There are multiple ways to remotely manage the PIX 501. All management commands are accessible via the command line interface. The command line interface can be remotely accessed with telnet or ssh or can be manipulated with snmp. In addition, the PIX 501 can be configured to allow remote access to the Pix Device Manager via the WAN port.

> **Tech Note:** It is a good idea to disable the telnet connection because passwords are sent in the clear over the network when you use telnet.

To remotely manage a single system, simply open an ssh connection to that system and issue configuration commands at the command line interface.

For managing large numbers of PIX 501s you need something like the Cisco Secure Policy Manager (CSPM) or CiscoWorks, the upgrade from CSPM, which can remotely manage multiple CISCO products including the PIX firewall. Another manager is the Solsoft NP Workstation which can also manage multiple network devices including PIX firewalls. The following image shows part of the CISCO Secure Policy Manager.

The Solsoft manager handles not only firewalls but routers and switches. Rules and policies are created in a graphical manner. For example, a VPN tunnel between two devices is created by drawing the tunnel in the network diagram. Solsoft then generates all the settings needed to create the VPN and then configures the routers and firewalls. The following image shows a Solsoft configuration.



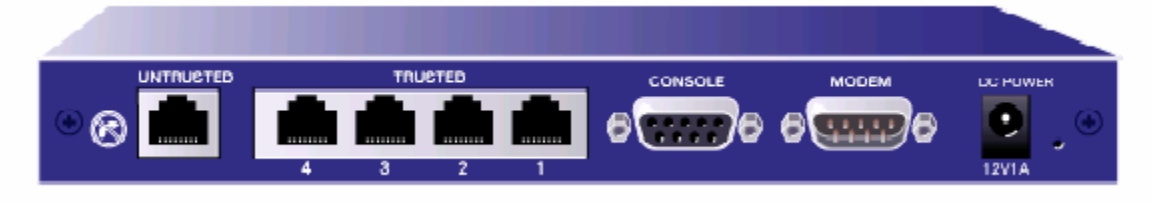
7 NETSCREEN 5XT

The NetScreen 5XT is a small version of the larger, NetScreen, corporate firewalls. It uses the same configuration settings and configuration management methods as the larger systems. Configuration is via a text based command user interface or via a web-based GUI.

7.1 HARDWARE DESCRIPTION

The 5XT consists of a single hardware box containing all the electronics and an external power supply. The network interfaces consist of a single, Ethernet 10/100 uplink WAN port (untrusted), a four port Ethernet 10/100 LAN switch (trusted), a serial console port and a serial modem port. The WAN port is connected to the untrusted, external network such as a DSL or Cable Modem, or other unprotected network. Communications between the WAN port and the four port LAN switch is protected by the 5XT firewall. The current version of the firewall software has the capability to split the LAN ports into two different security domains and to write firewall rules to control connections between these two domains as well as to the WAN port.

The console port is always available for configuring the system in case you cannot connect to the configuration software through the LAN ports. The modem port is used for a telephone failover should the Ethernet network connected to the WAN port goes down.



The hardware of the 5XT is a custom ASIC designed specifically for packet inspection and routing.

Throughput performance is 70 Mbits/s for unencrypted connections to a NAT addressed internal device and 20 Mbits/s through a 3DES VPN connection.

Hardware installation consists simply of plugging the WAN port into your incoming network device, plugging the systems to be protected into the LAN ports, and plugging in the power supply. The default system comes up in a protected mode and must be configured using the built-in web or command line interface before it can be used. Basic configuration consists of setting up the internal and external IP addresses, NAT, and the DHCP server.

7.2 SOFTWARE DESCRIPTION

The software consists of the NetScreen ScreenOS operating system which provides both a command line and a web-based GUI interface and a startup wizard for performing the initial configuration. The command line interface can be used through either of the two network interfaces and through the console port. The system contains built-in web, telnet, and ssh servers which can be used to manage the system. The GUI interface can only be used through the network ports via the built-in web server.

Much like the Cisco PIX, command line configuration consists of a file of commands that configure the system and set the firewall rules.

> **Tech Note:** It is very common to maintain a copy of the configuration file on the workstation you are using to configure a system. When you want to change the configuration you can issue individual commands to make the desired changes but it is more common to edit a copy of the configuration file, reset the firewall, and then upload the whole file of configuration commands, not just the changes. This is done to better track the current configuration and to make sure that the configuration can be repeated.

The NetScreen command language is similar enough to the CISCO command language to seem familiar to users who have configured CISCO products but different enough to be confusing. Be sure you understand the NetScreen security model before making significant changes to the configuration.

Of the three systems examined in this report, the manuals included with the NetScreen are the most complete in terms of describing the operation and configuration of the system. They are filled with sample configurations for many different situations. They are available online at,

```
http://www.netscreen.com/resources/manuals/screenos.jsp
```

The newest version of the ScreenOS software provides the capability to split the protected LAN ports into two different security zones and to have separate firewall rules for communications between the LAN and WAN ports and between the two separate LAN ports. The most common configuration is the Home/Work mode where two of the LAN ports are designated for your work machine at home and the other two are designated for your other home machines. The default ruleset allows no connections to open from the home to the work network to protect the work machine from attacks by the home machines which may be operated in a less than secure mode. The configuration does allow for connections from the work to the home network so the work system can share printers and file servers on the home network.

New software can be uploaded and installed from a tftp server or via the ScreenOS.

7.3 PRODUCT MATRIX

	5XT-10 user	5XT Elite
Max. Nodes Behind Firewall	10	Unlimited
WAN Port	10/100 port	10/100 port
LAN Ports	4 port 10/100 switch	4 port 10/100 switch
Other Ports	Console, Modem	Console, Modem
Authentication	Internal database RADIUS SecureID LDAP XAUTH	Internal database RADIUS SecureID LDAP XAUTH
VPN Encryptions Available	DES 3DES AES	DES 3DES AES
VPN Authentication Available	MD5 SHA-1 PKI	MD5 SHA-1 PKI
Max. VPN Tunnels	10	10
VPN Type	client or serve	client or serve
Local Management	ScreenOS Command line	ScreenOS Command line
Remote Management	HTTPS SSH telnet SNMP Global Pro	HTTPS SSH telnet SNMP Global Pro
Logging*	Advanced	Advanced
Speed Mbits/s	70 No Tunnel 20 3DES VPN	70 No Tunnel 20 3DES VPN
Extras	Split LAN interface Dial-up failover Antivirus	Split LAN interface Dial-up failover Antivirus
Streeet Price 5/03	$575	$992

*Basic logging consists only of logging events within the firewall. Advanced logging includes more details and allows logging in external servers such as the management server or a syslog server.

7.4 SPECIAL CAPABILITIES

There are two special capabilities of the NetScreen 5XT, modem failover and the ability to split the protected LAN ports into two security zones. Modem failover allows you to put a modem on the modem port and configure the 5XT to automatically dial into your network provider if the high-speed connection goes down. Newer systems are adding an antivirus solution.

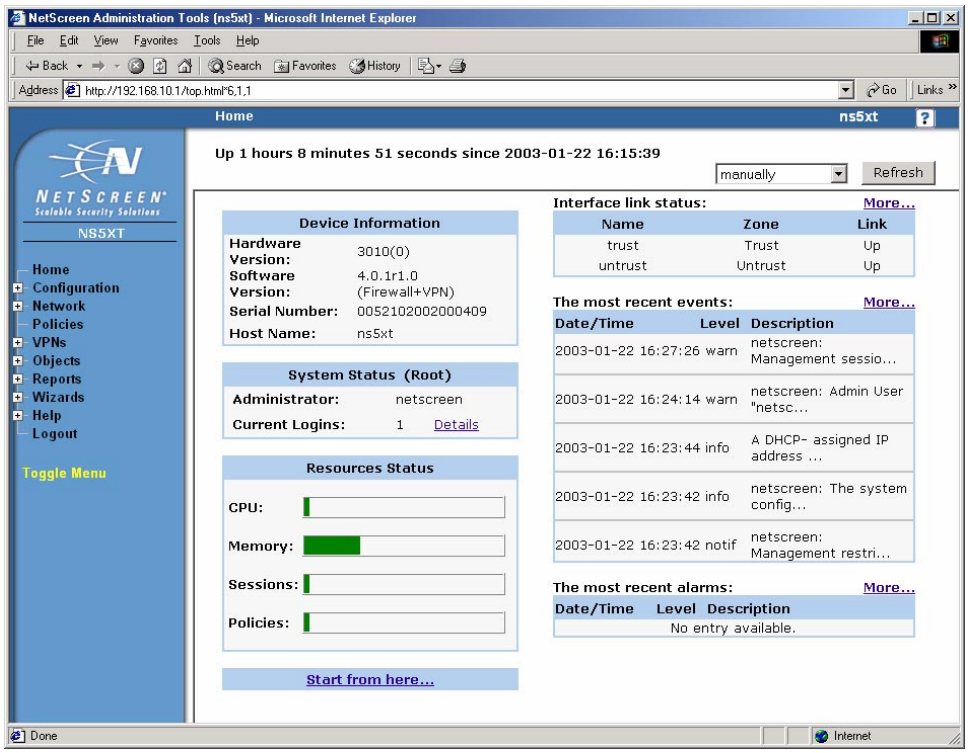
The split LAN port capability has been discussed above and allows you to have three, separate security zones instead of just two (trusted and untrusted). With three security zones defined in the system, you can establish different levels of trust for two different groups of home systems to better protect the more critical systems. In a household where children and other users make regular use of a network, the risk that the network will be compromised is much higher than one where a single user performs only company business on his system.

7.5 LOCAL MANAGEMENT

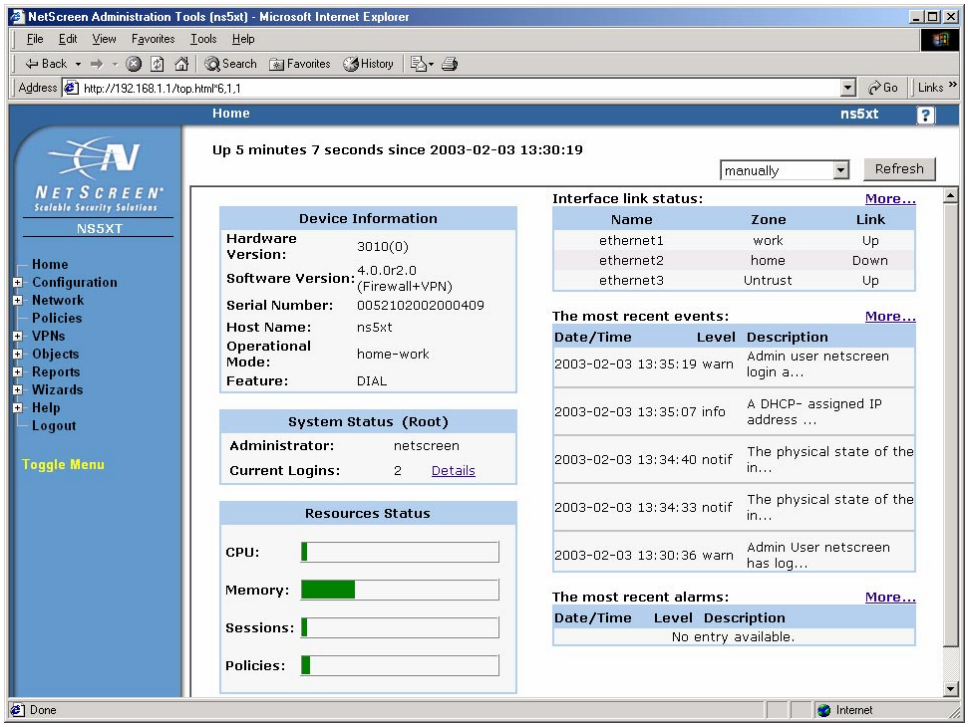
Local management of the PIX can be performed through the console port using a simple terminal program, or through the LAN ports using a web browser or an ssh connection. The easiest is the web connection which allows both GUI and command line configuration.

> **Tech Note:** We have found that it is useful to connect a terminal onto the console port during configuration and testing and to configure the system to send all log events to the console. This gives you real time logging information to help you interpret your configuration and testing.

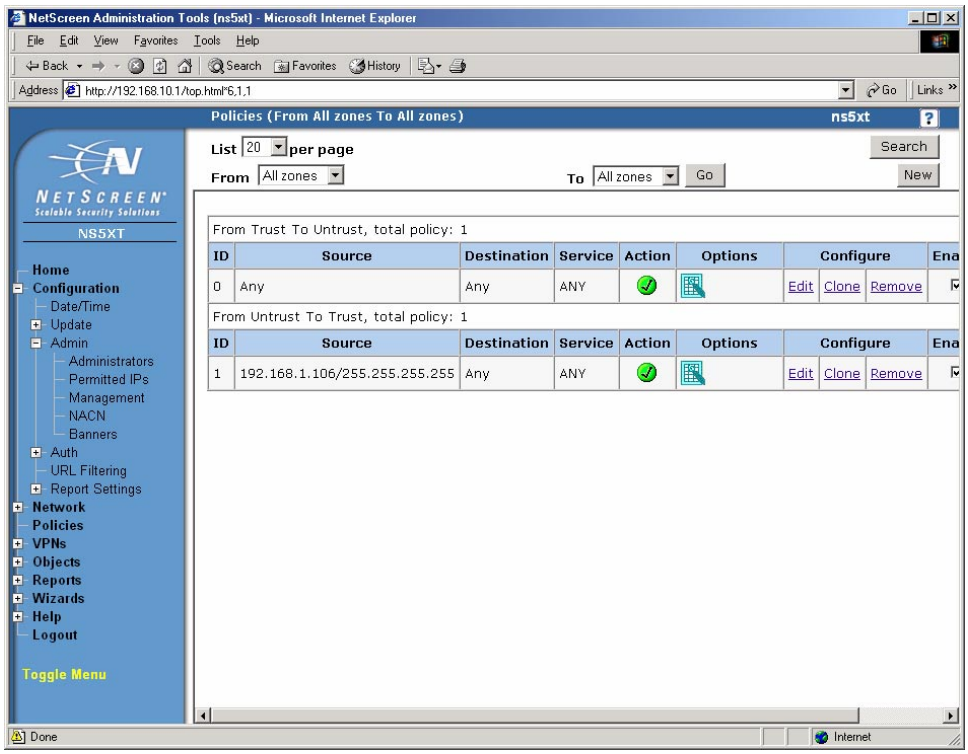
On a system connected to the LAN ports, open a web browser and connect to 192.168.1.1 which is the default address of the internal ports. To login use the default username and password, both of which are “netscreen” (without the quotes.) At the first login to a new system, a configuration wizard runs that gets the minimum configuration information necessary to run the system. The first item is to change the username and password. Be sure to do this as all the hackers know the default username and password and you don’t want them reconfiguring your system for you. Other initial configuration includes the IP addresses of the trusted and untrusted ports, and the use and configuration of DHCP and NAT. At this point, the basic configuration is done and you are passed to the main ScreenOS web page.



If you have split the LAN into a work and home security zones, the initial page looks like the image below. Note that the Interface Link Status now contains three interfaces instead of two.

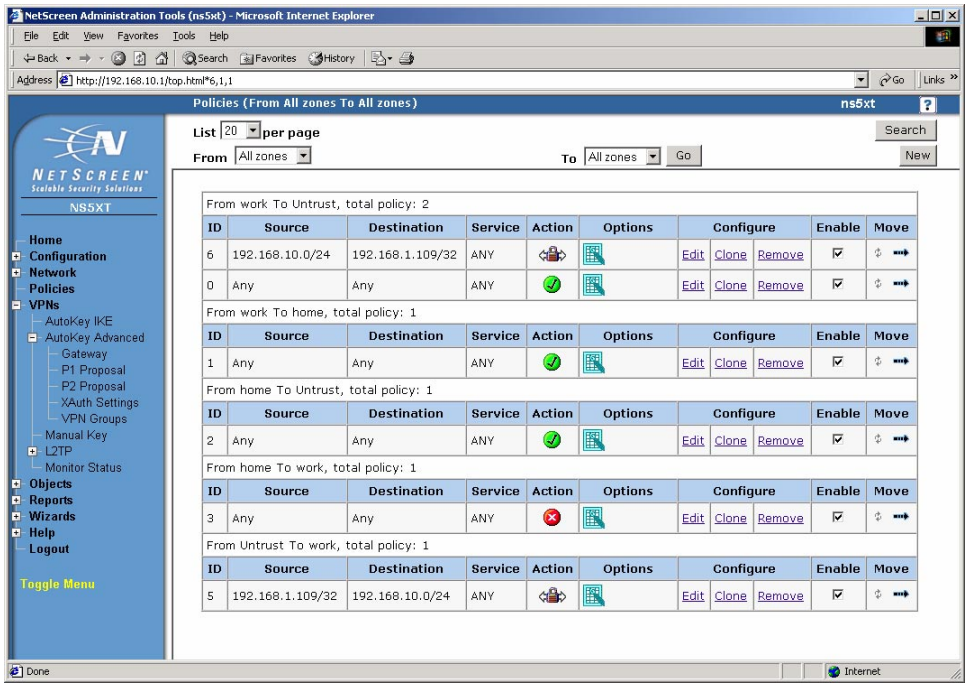


The menu along the left side of the screen is used to configure the system, adding new policies, VPNs, users, etc. Configuration is generally from the bottom up with this menu as you must create a user before using him in a VPN and you must create a VPN before using it in a Policy. The Configuration and Network menus contain commands to do most of the system configuration, including network names, addresses, allowed users, and features. Firewall rulesets are created as Policies.

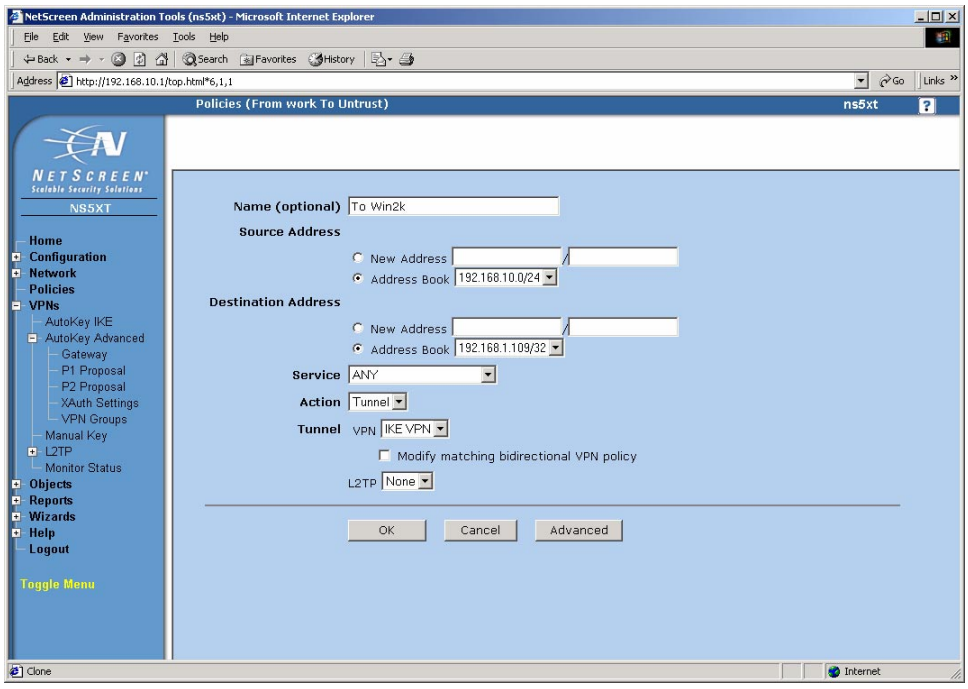


Each pair of interfaces has two sections in the policies window that represent connections between the two interfaces and the direction of the initial connection that starts the session that passes through the interfaces. Policies include source and destination addresses, destination ports, actions (allow, deny, tunnel), and options (log). In the case above, all outgoing connections and incoming connections from 198.128.1.106 are allowed. Everything else is denied.

The policy window below shows a more complex system with the home/work setup including some VPNs (Policy IDs 5 and 6.)



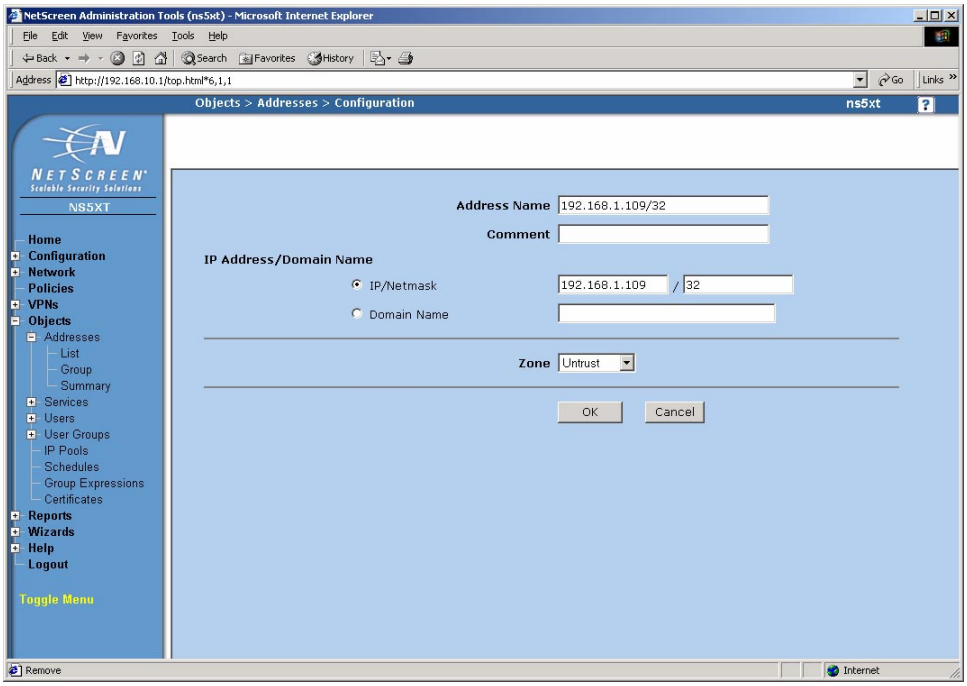
New policies are created by pressing the new button and filling in the following form.



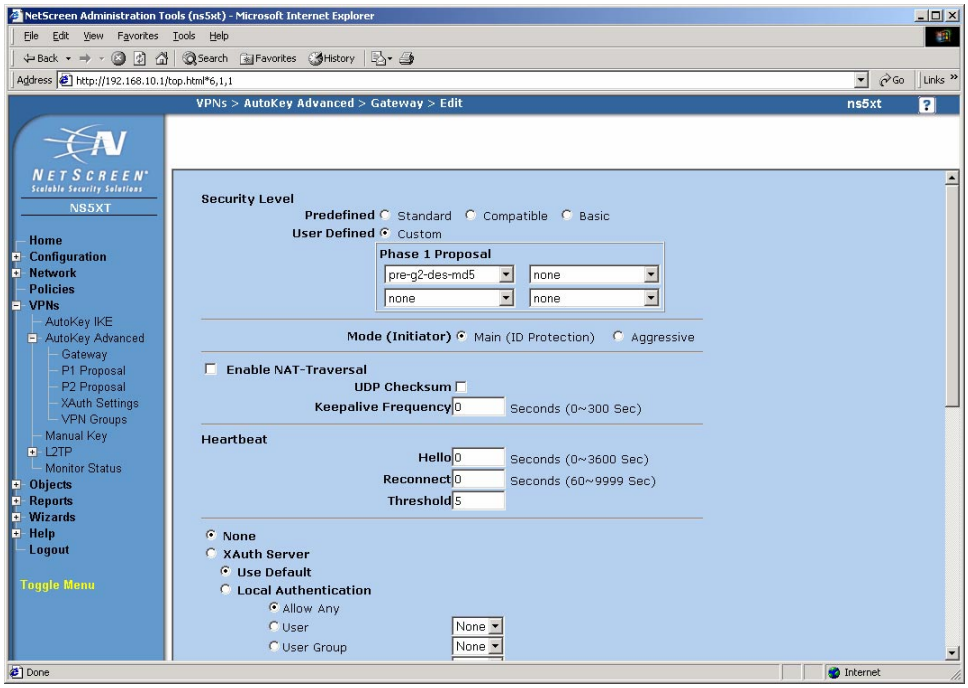
The Objects menu is where you create named items for use in the other commands. Generally, if you are in a window that requires an object, you can create one at that moment for use in the window instead of having to quit the current command, create the

object, recreate the window and then use the object in the command. That is, you are not forced to create an object before using it but can create it when it is needed.

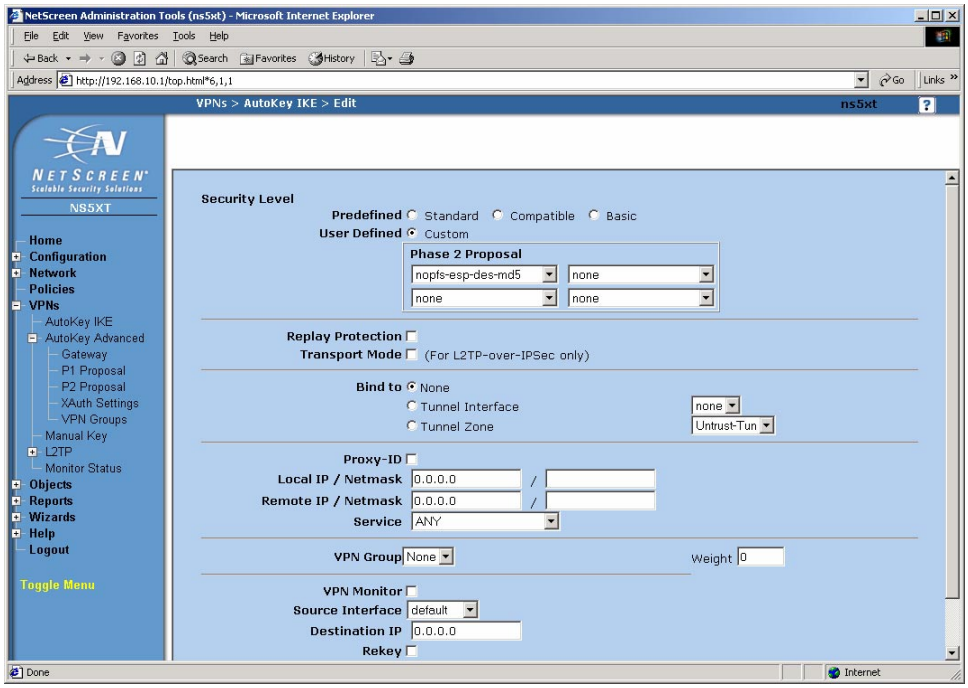
The Objects menu below shows the creation of an IP address or network address object. The name can then be used in other windows that need the address as an argument. Defining other objects proceeds in much the same way.



The VPN menu is where you make all the settings for creating VPNs. The settings here are general purpose and are not organized by type of VPN. Thus, there is no IPSec page or PPTP page so you must know what settings you need for a particular VPN. There are wizards under the wizards menu to help you make the settings for a particular type of VPN. There are also many examples in the documentation. In the image below, you see the creation of a Gateway, whose settings handle Phase 1 of an IPSec tunnel.



In this image, you see the creation of an Autokey IKE, which contains the settings for Phase 2 of an IPSec tunnel.



The Reports menu is just that, it is where you create reports on the setup of the 5XT, logs of its operation, lists of current sessions passing through the 5XT, and DHCP leases of IP addresses. Logging can be set to be saved within the 5XT, or sent to the console port, or to an external syslog server.

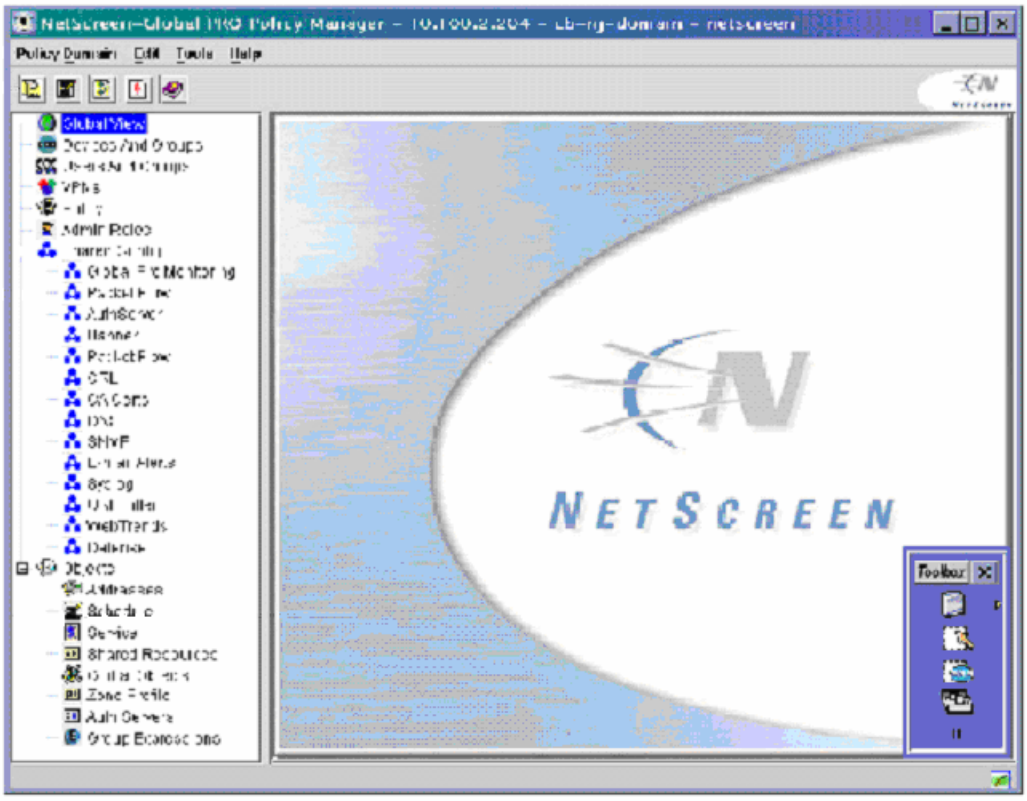
7.6 REMOTE MANAGEMENT

Remote management can be done via web, secure web, telnet, ssh, SNMP, and NetScreen Global Pro manager. Remote management using regular web services and telnet should not be allowed. For managing large numbers of remote systems, the NetScreen Global Pro manager is available.

The NetScreen Global Pro Policy Manager is available in two different versions. Global Pro Express for up to 100 systems ($15K for 100 systems or $6K for 25 systems) and Global Pro for up to 10,000 systems ($56K for first 1000 systems plus $12K for each additional 1000 systems.)

Part of the cost of the Policy Manager is that the server component is delivered as a network appliance, preinstalled on a Sun NETRA server running Solaris 8. Management of the systems is through the Policy Manager consoles which run on Windows platforms and communicate with the server.

Installation of the Policy Manager Consoles is performed by making a web connection to the Policy Manager server which automatically downloads and installs the Console.



Global policies are created using this manager and applied to groups of firewalls to make the system scalable. When changes need to be made, the Policy Manager logs into the firewall using an encrypted connection and makes the changes.

Tech Note: Having the initial connection go from the manager to the firewall is problematic for managing home systems. Most home systems use DHCP to get their IP address. If the IP address of the home system changes, the policy manager will not be able to find it. Netscreen gets around this problem by having the Netscreen Address Change Notification (NACN) service running on the firewalls. Whenever the IP address of the WAN interface changes the NACN service contacts the Policy Server and gives it the new address. The NACN service authenticates using the firewall serial number and a shared secret (password).

8 DISCUSSION

The hardware firewalls described in this report are representative of the high-end of the home firewall market or the low-end of the corporate firewall market, depending on your point of view. As such, they are a melding of the capabilities of the home and corporate firewalls. From the home firewall side, they can operate, out of the box as an anything is allowed out, nothing is allowed in firewall. This same capability is also available in much less expensive units. From the corporate firewall side, these units can be configured using the same methods, command language, and management stations as the larger firewalls and routers from which they are derived. They also have capabilities such as VPN tunneling and remote management capabilities which are not available in the less expensive units.

If you need to protect a few home machines and an all out/none in kind of protection scheme is sufficient, these are not the units for you. There are other home firewalls available in the under $100 range that will provide this capability. On the other hand, if you need remote management, more flexible rulesets that can allow in some external systems but block others, or VPN tunnels to bind your home network to a work network, you should look closely at these systems. Systems of this type would also be useful for protecting systems in individual offices in addition to the protection afforded by a sites gateway firewall. Any large installations of these units would require good, scalable, remote management which all of these units have.

This report does not describe all available high-end home firewalls but gives a good cross section of the capabilities of some of the market leaders in this area. This is a rapidly growing market and other manufacturers are creating new, similar units all the time.

8.1 PRODUCT MATRIX

The following table places the capabilities of the three units examined in this report side by side. Something to keep in mind when examining this table is that the capabilities and speeds indicated are from vendor documentation not actual testing. Our testing was primarily concerned with determining if the firewall capabilities worked, if the VPN capabilities worked, how hard they were to manage locally, and if the remote management capability was scalable to large numbers of systems. In all cases, these three machines did what they claimed they can do.

Not specified in the table are some of the common characteristics of all three firewalls. All three firewalls provided,

DHCP Server – To provide addresses automatically to the protected systems.

DHCP Client – For the WAN interface so it can work in most modern networks.

NAT – For the protected network to allow multiple systems to share a single address.

Transparent mode – In transparent mode, NAT is not used to translate the system addresses. The systems behind the firewall have real addresses that are visible outside of the firewall. The firewall still provide protection of the systems.

PPPoE – Used when connecting to a network through an ISDN network.

Attack Detection – All the systems have the capability to detect certain kinds of attacks. This is only really useful if you need to know how you are being attacked. The firewall rules themselves still protect a system even when the firewall does not know what kind of an attack is being used.

	S-box Safe@home	S-box Safe@home Pro	S-box Safe@office	S-box Safe@office Plus	PIX 501-bun-k8	PIX 501-bun-k9o	PIX 501-50-bun-k8	PIX 501-50-bun-k9	5XT-10 user	5XT Elite
Nodes	5	5	10	25	10	10	50	50	10	Unlimited
WAN Port	10/100 port	10/100 port	10/100 port	10/100 port	10-baseT port	10-baseT port	10-baseT port	10-baseT port	10/100 port	10/100 port
LAN Ports	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch	4 port 10/100 switch
Other Ports	none	none	none	none	Console	Console	Console	Console	Console, Modem	Console, Modem
Authentication	Internal database	Internal database	Internal database	Internal database	Internal username/ password, TACACS+, RADIUS	Internal username/ password, TACACS+, RADIUS	Internal username/ password, TACACS+, RADIUS	Internal username/ password, TACACS+, RADIUS	Internal database, RADIUS, SecureID, LDAP, XAUTH	Internal database, RADIUS, SecureID, LDAP, XAUTH
VPN Encryptions	n/a	AES, DES, 3DES	AES, DES, 3DES	AES, DES, 3DES	DES	3DES, AES	DES	3DES, AES	DES, 3DES, AES	DES, 3DES, AES
VPN Authentication	n/a	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1, PKI	MD5, SHA-1, PKI
Max Tunnels	n/a	5	10	10	5	5	5	5	10	10
VPN Type	n/a	client	client or server	client or server	client or serve	client or serve	client or server	client or server	client or serve	client or serve
Local Management	Web Interface	Web Interface	Web Interface	Web Interface	PDM or command line	PDM or command line	PDM or command line	PDM or command line	ScreenOS, Command line	ScreenOS, Command line
Remote Management[#]	HTTPS, SMP	HTTPS, SMP	HTTPS, SMP	HTTPS, SMP	HTTPS, SSH, SNMP, CiscoWorks, Solsoft	HTTPS, SSH, SNMP, CiscoWorks, Solsoft	HTTPS, SSH, SNMP, CiscoWorks, Solsoft	HTTPS, SSH, SNMP, CiscoWorks, Solsoft	HTTPS, SSH, telnet, SNMP, Global Pro	HTTPS, SSH, telnet, SNMP, Global Pro
Logging*	Basic	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced
Speed, Mbits/s	22 No Tunnel, 1.5 3DES VPN	22 No Tunnel, 1.5 3DES VPN	22 No Tunnel, 1.5 3DES VPN	22 No Tunnel, 1.5 3DES VPN	37 No Tunnel, 6 DES VPN	37 No Tunnel, 2 3DES VPN, 3 AES-128 VPN	37 No Tunnel, 6 DES VPN	37 No Tunnel, 2 3DES VPN, 3 AES-128 VPN	70 No Tunnel, 20 3DES VPN	70 No Tunnel, 20 3DES VPN
Extras	Antivirus, URL Blocker	Antivirus, URL Blocker	Antivirus, URL Blocker	Antivirus, URL Blocker					Split LAN interface, Dial-up failover, Antivirus	Split LAN interface, Dial-up failover, Antivirus
	$229	$299	$476	$887	$445	$525	$879	$955	$575	$992

#PDM = PIX Device Manager (Java Application).

*Basic logging consists only of logging events within the firewall. Advanced logging includes more details and allows logging in external servers such as the management server or a syslog server.

8.2 TRADEOFFS

There are very few tradeoffs between the operational capabilities of these systems. They are all about the same speed and are capable of handling the small home network or office without any problem. Tradeoffs begin to show in the management capabilities and documentation.

All three units can be managed locally. The Cisco and Netscreen can be fully managed with a web browser or a serial terminal. All settings can be made and all rulesets can be created or changed. The S-box can be configured locally for most situations but the expensive, Firewall 1 policy management software is needed to change and recompile the underlying firewall ruleset. All of these units are likely to be remotely managed as part of a large network using special remote management software. Because of this, the cost of the expensive policy manager is spread across many units making it less of a concern as a tradeoff.

The documentation for the Netscreen is better than that for the CISCO and significantly better than that for the S-Box. For someone new to networking and firewalls, it is much easier to figure out how to configure a system with the Netscreen documentation as it has lots of detailed examples. CISCO also has a lot of examples and documents but they are spread among dozens of whitepapers on the CISCO website. The information is available, you just must dig to find it. The S-box is a new system and the documentation is somewhat sparse in comparison but is growing rapidly.

Of the three units, only the CISCO has a 10-baseT WAN interface. All others have a 10/100 interface. For a home network connecting to a cable or DSL modem, this is not a problem as the modem it is connected to cannot make use of the higher speed. For a system used to protect an office in a corporate network the 10-baseT connection will be a bottleneck for people transferring large amounts of data through the firewall. Average network users are unlikely to notice a difference.

The most important consideration when choosing between these systems is what other systems you already have. If you already manage a CISCO network then the PIX will likely be the strongest contender. Likewise if you are using a Firewall-1 or Netscreen firewall, you will likely choose the S-box or the Netscreen respectively. This is because you can leverage your existing skills and management software to manage the new units.

Some useful testing that was not done here would be to see how many open sessions you can have at one time and how responsive the system is when many sessions are open. The system literature all indicate that they can handle more than a thousand open sessions. However, it is likely that system response will suffer badly before you reach that number.

You might wonder why you would need thousands of open sessions for the 5 to 10 systems you are likely to have behind a home firewall. The reason is that many

applications open multiple sessions to make better use of the limited bandwidth available to most home networks. File sharing software is known to open hundreds of sessions when transferring files. Opening a single web page opens a different session for each component of that page which may come from different sources.

I have seen a network that uses one of the older, smaller, and less capable home firewalls become unresponsive when one person on the protected network downloads some audio files. Web, mail, and other connections start timing out waiting for a free session. The high-end home firewalls described in this report should not have that problem (my old firewall allows only 128 simultaneous sessions) but newer software and file sharing capabilities in the not too distant future might cause them problems.

9 CONCLUSIONS

High-end, hardware home firewalls provide firewall protection for the home and small office using a system that is operationally equivalent to corporate firewalls of the same brand. While not as fast and flexible, they provide similar firewall protections to the home and small office as their big brothers provide to a corporate network including stateful packet inspection and VPN tunneling.

Keep in mind that there are more high-end home firewalls than the three described in this report. Most corporate firewall manufacturers have a low-end system that fits within this classification. The other thing to keep in mind is that this whole market is in a state of rapid flux with increasing capabilities of these systems and new models appearing all the time.

As was mentioned previously, the system you choose will likely depend on what type of systems you are currently using, especially if you are already remotely managing a large network. You will likely pick a solution that fits into your current management scheme to ease the management of the new devices and to insure compatibility between devices.

10 REFERENCES

The following vendor websites contain a considerable amount of information about the firewalls described in this report.

CISCO, *http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html*

NetScreen, *http://www.netscreen.com/products/firewall/*

S-Box, *http://www.sofaware.com, http://www.checkpoint.com/*

APPENDIX A – CONFIGURING AN IPSEC TUNNEL BETWEEN A WORKSTATION AND A FIREWALL

This appendix shows an example of setting up an IPSec tunnel between a Windows 2000 system and a Netscreen firewall. Similar connections can be created between pairs of IPSec compliant devices. Windows 2000 has IPSec security built in to the operating system so no extra hardware or software needs to be acquired to make it work.

In this case, we know the addresses of all the systems involved. In the event that a remote system uses DHCP to get its address as most home systems must do these days, the home system must make the initial connection that opens the VPN tunnel. After that, connections allowed by the policy can start at either end.

Figure A1 shows the configuration of the network we are going to use for this tunnel. The internal system is behind the firewall and has address 192.168.10.33. The firewall uses NAT so the 192.168.10.x subnet is not normally visible from outside the firewall (the network cloud). Note that the default subnet for the internal interface named *work* is 192.168.1.x which has been changed for this example. The firewall's external address is 192.168.1.101 and the remote system's address is 192.168.1.109. There is a second internal interface called *home* with the subnet 192.168.20.x that is not shown here and is not used in this example.

What we want to do is to create an encrypted tunnel from the remote system to the network behind the firewall. Any communication starting in either direction between the remote system and the internal subnet should go through the tunnel. Any other communications goes outside the tunnel. Authentication of the remote systems is through a pre shared key or password. We could also use security certificates and other authentication mechanisms.

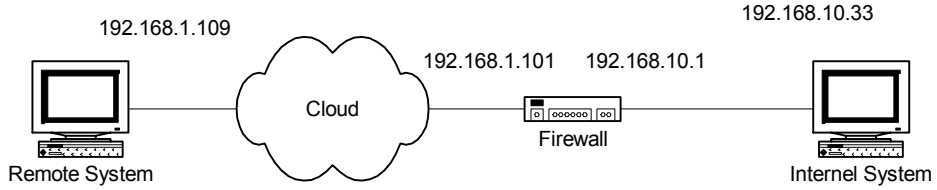
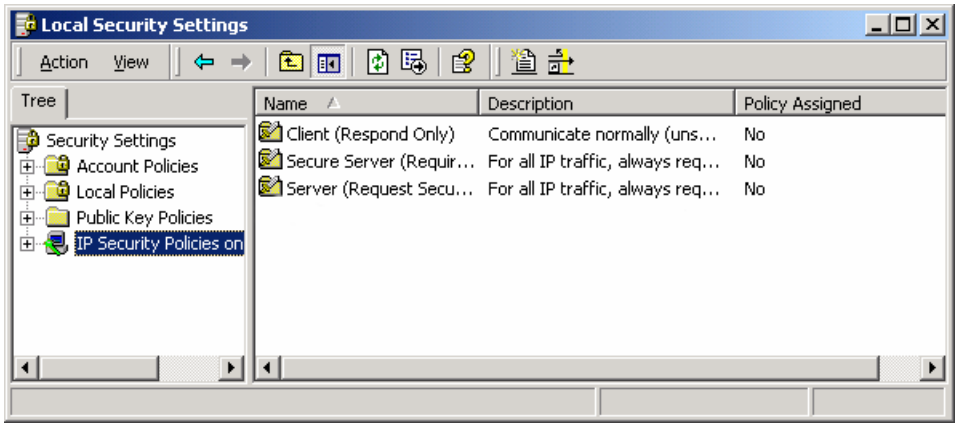


Figure A1. Network configuration.

Configuring the Windows 2000 System

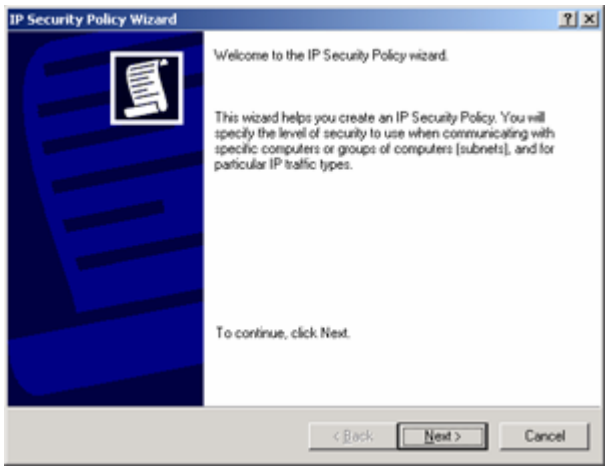
1. Run: Control Panel\Administrative Tools\Local Security Policy

2. Select: IP Sec Policies on Local Machine



3. Choose: Action/Create IP Security Policy

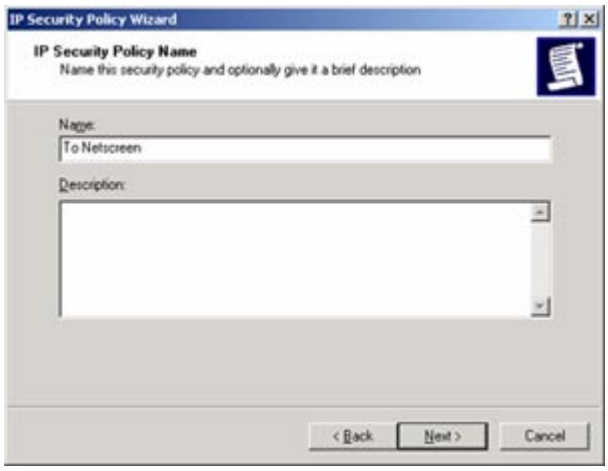
This creates a new security policy. The security policy wizard appears and walks you through the initial creation of a new policy. All security rules that you want in force at any one time must be in the currently active policy. Only one policy may be active at a time.



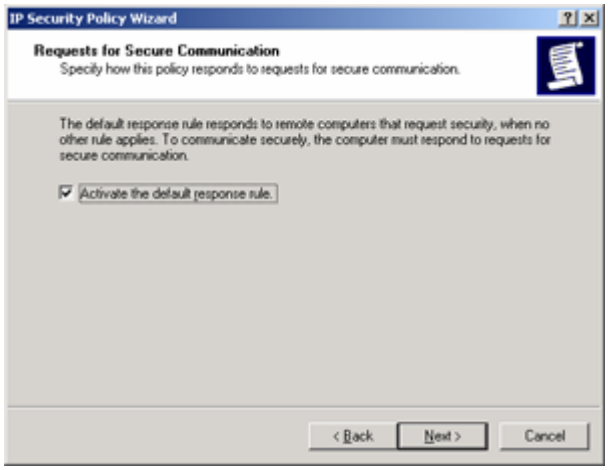
4. Click Next.

5. Type a name for the new policy and click Next.

   Name=To Netscreen

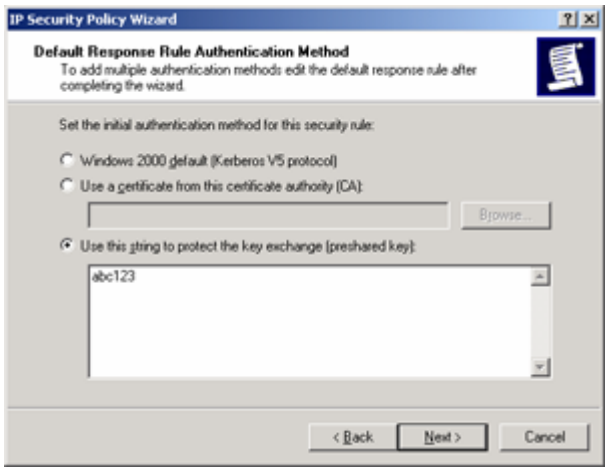


6. Leave checked, Activate the default response rule, and click Next.

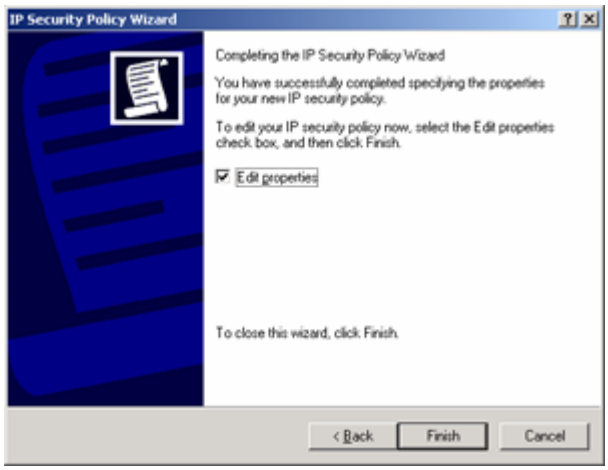


7. Click, Use this string to protect the key exchange (preshared key), type a password and click Next. (You should pick a more secure key than the one used in this example.)

   Key = abc123

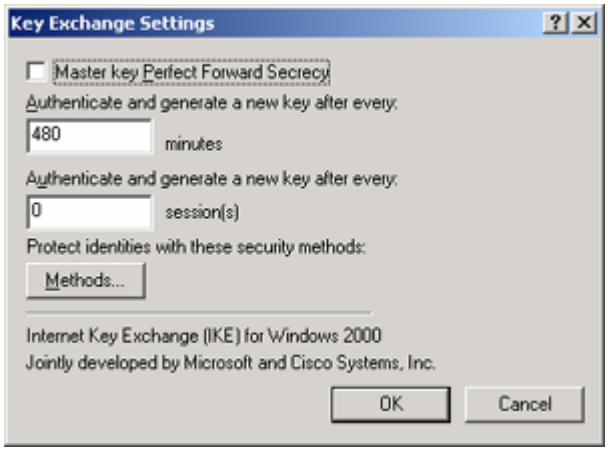


8. Leave checked, Edit parameters, and click Finish. The To Netscreen properties window opens.



9. Select the General tab and type a description if you want. Leave the other settings at their default values.

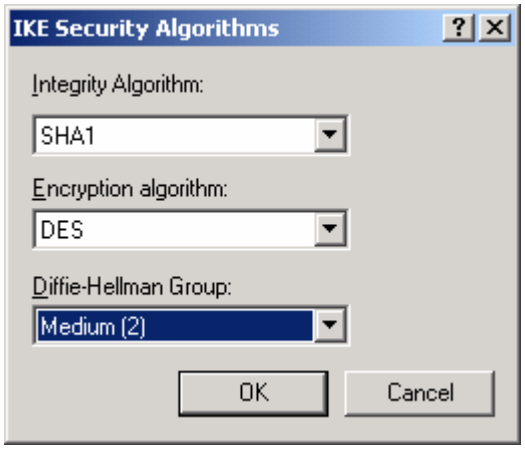
10. Click Advanced. Leave these settings at their default values.



11. Click Methods.

12. In the dialog box select IKE DES SHA1 and click Edit.

13. Change the Diffe-Hellman Group to Medium (2) and click OK.

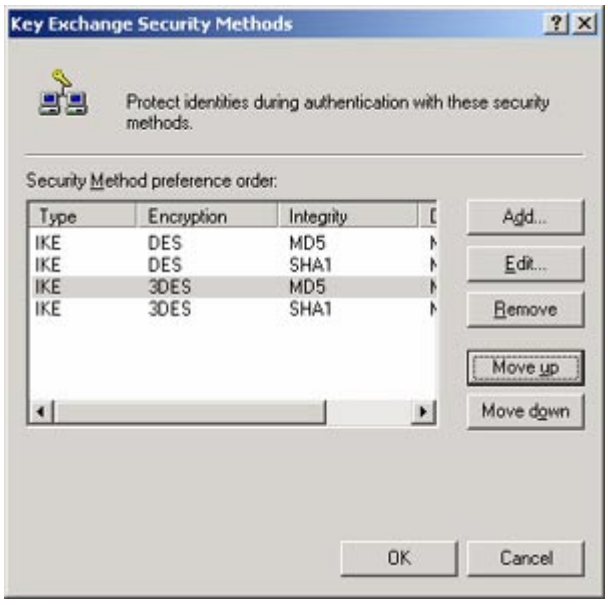


14. In the dialog box select IKE DES MD5 and click Edit.

15. Change the Diffe-Hellman Group to Medium (2) and click OK.

16. Using the Move Up and Move Down buttons in the dialog box, put the four rules in the following order.

    IKE DES MD5
    IKE DES SHA1
    IKE 3DES MD5
    IKE 3DES SHA1



17. Click OK twice to get back to the Netscreen Properties dialog box and select the Rules tab.

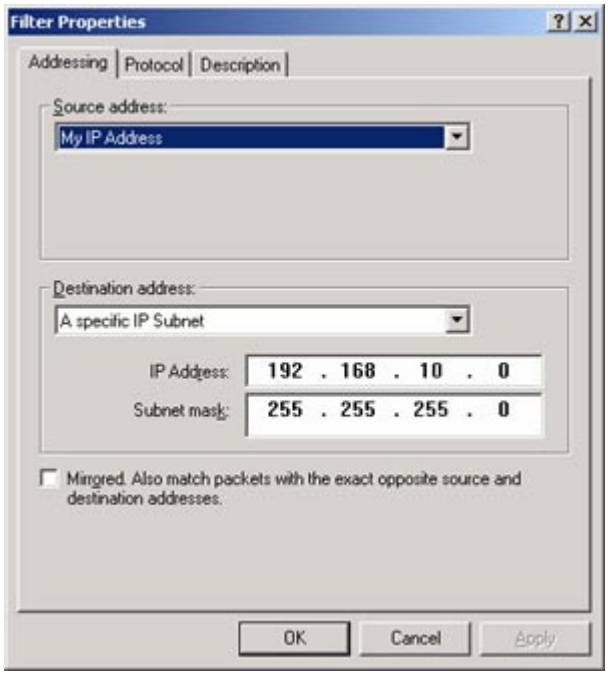
18. Uncheck, Use Add Wizard and click Add to create a new rule.

19. Select the IP Filter List tab and click Add to create a new filter. First create a filter to select traffic going from this Windows 2000 system to the subnet behind the Netscreen firewall. Set the name and uncheck, Use Add Wizard.

20. Click Add.

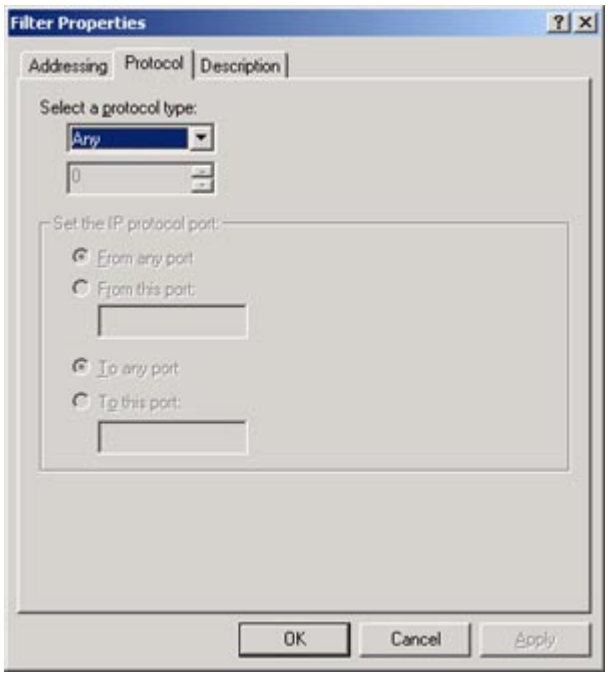
21. In the Filter properties dialog select the Addressing tab and make the following settings.

    Source Address = My IP Address
    Destination Address = A Specific IP Subnet
    IP Address = 192.168.10.0
    Subnet Mask = 255.255.255.0
    Mirrored = Unchecked.



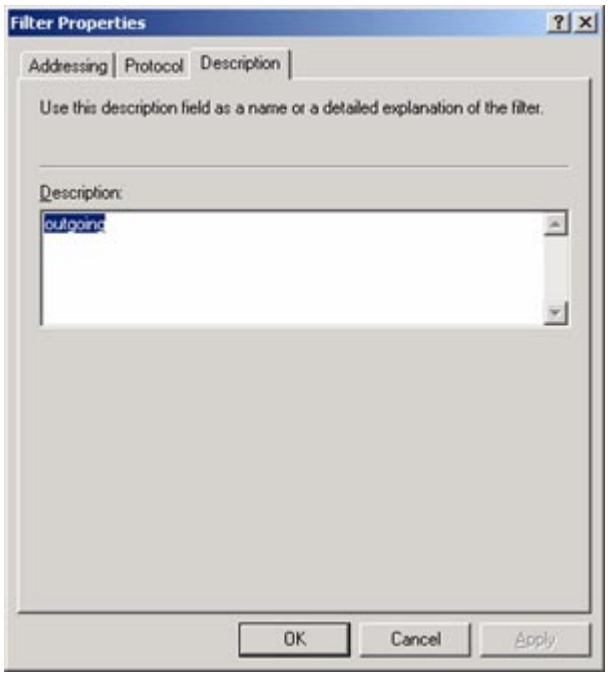
22. Select the Protocol tab and make the following setting.

Protocol = Any



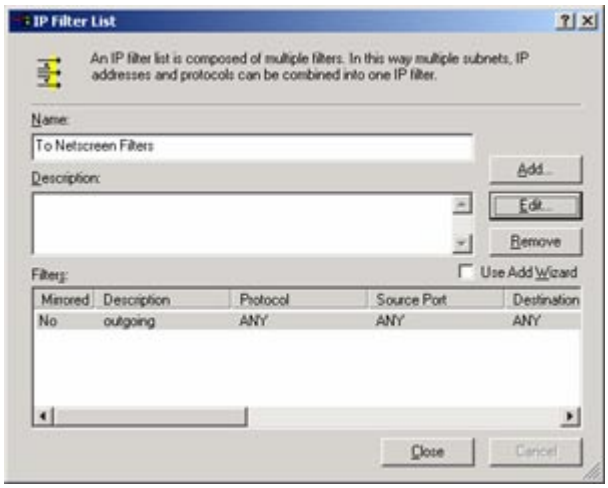
23. Select the Description tab and make the following setting.

Description = outgoing

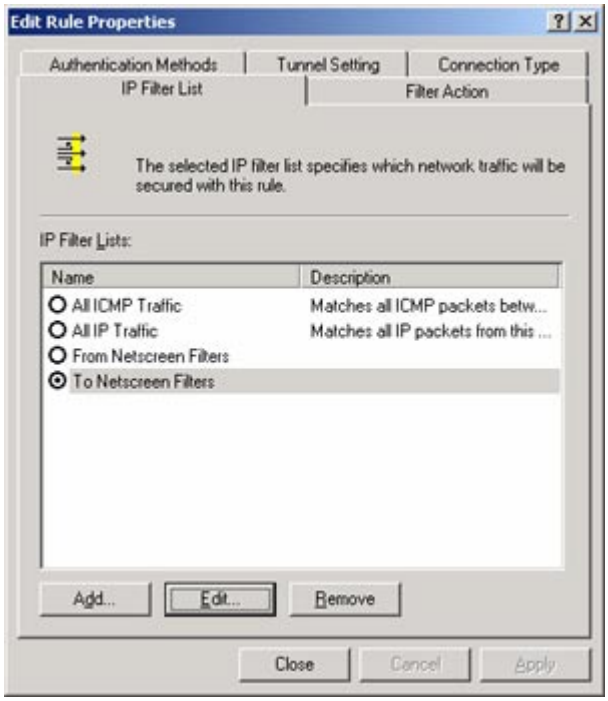


24. Click OK.

25. Click Close



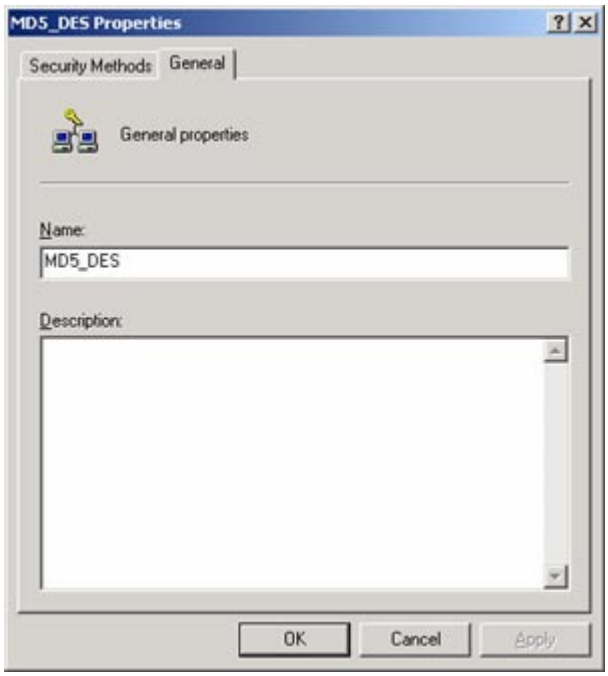
26. Make sure To Netscreen Filters is selected.



27. Choose the Filter Action tab, uncheck Use Add Wizard and click Add.

28. Choose the General tab and type a name for the filter action.

Name = MD5_DES

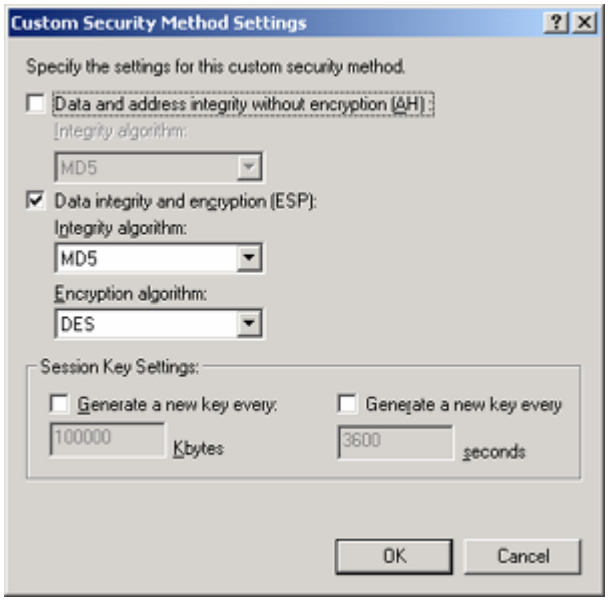


29. Choose the Security Methods tab, select Negotiate security and click add.

30. Select Custom and click Settings.

31. In the Custom Security Method Settings dialog make the following settings and click OK.

    Data integrity and encryption (ESP) = checked
    Integrity algorithm = MD5
    Encryption algorithm = DES

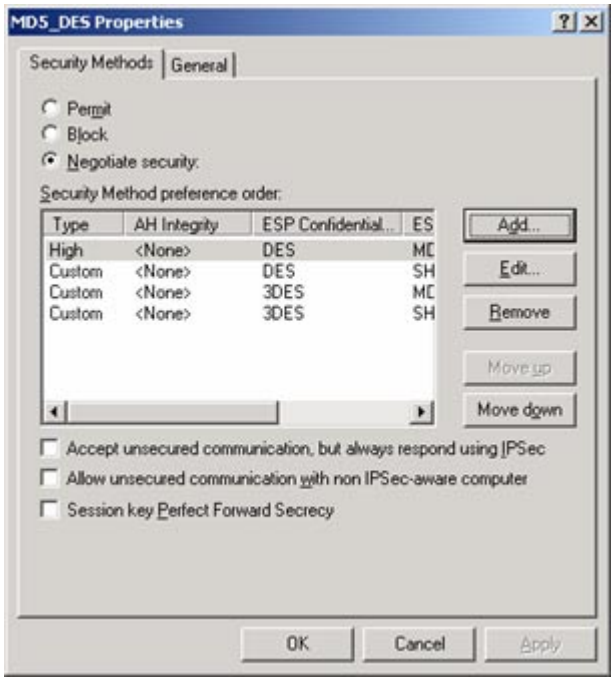


32. Windows displays a dialog box indicating that these settings are the same as its High (ESP) setting. Click OK in the warning and note that Windows has changed the custom setting to High.

33. Click OK

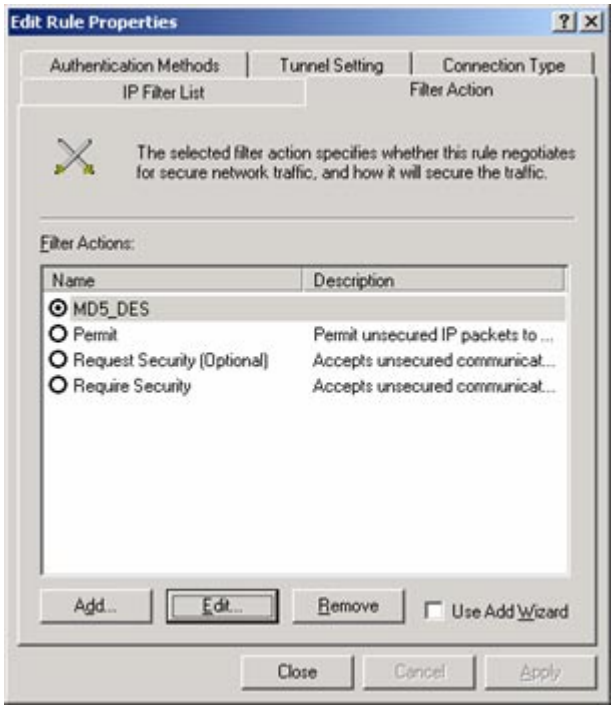
34. Make three more security methods with the following settings and in the following order.

    ESP, DES, SHA1
    ESP, 3DES, MD5
    ESP, 3DES, SHA1



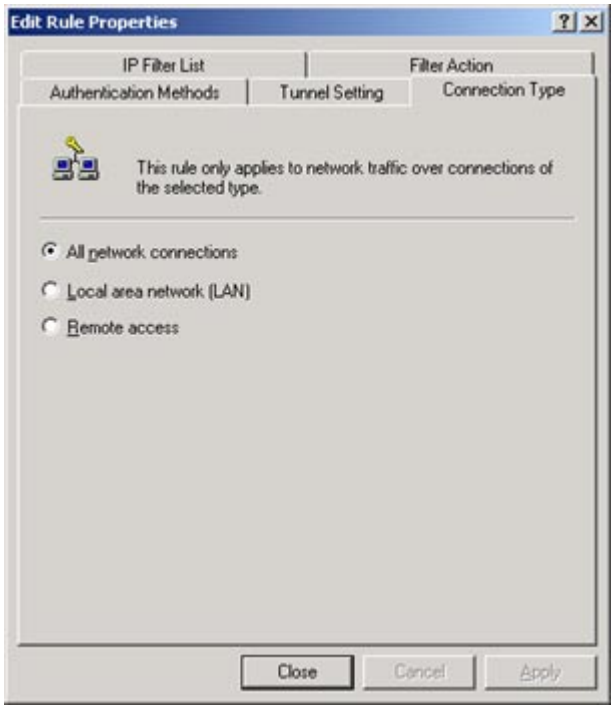
35. Click OK.

36. Make sure MD5_DES is selected.



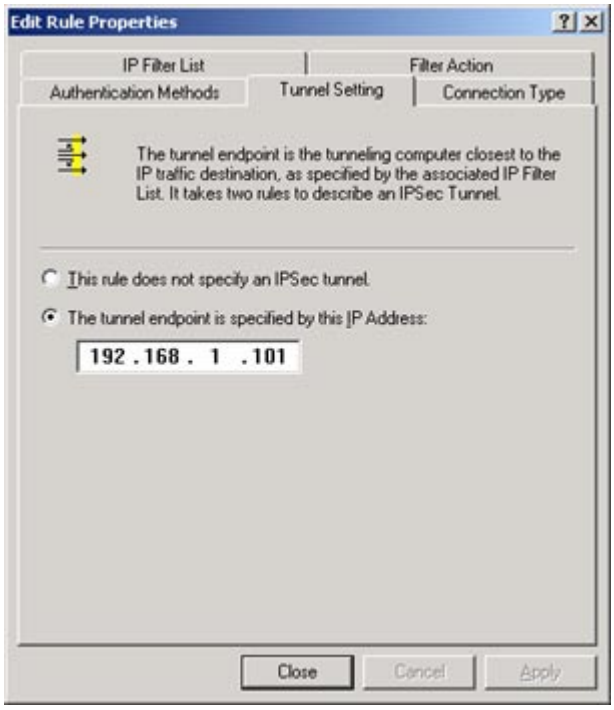
37. Choose the Connection Type tab and make the following settings.

Connection type = All network connections.



38. Select the Tunnel settings tab and make the following settings. The IP address specified here is the external interface of the firewall.

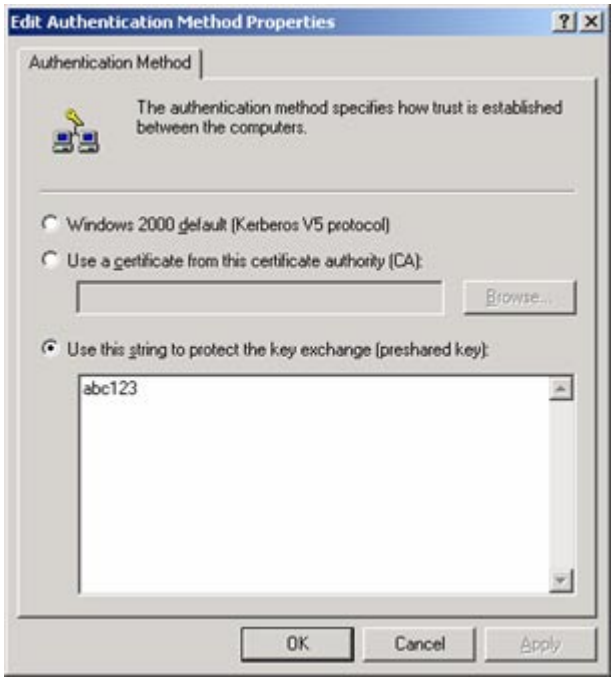
    The Tunnel endpoint is specified by this IP address = checked
    IP = 192.168.1.101



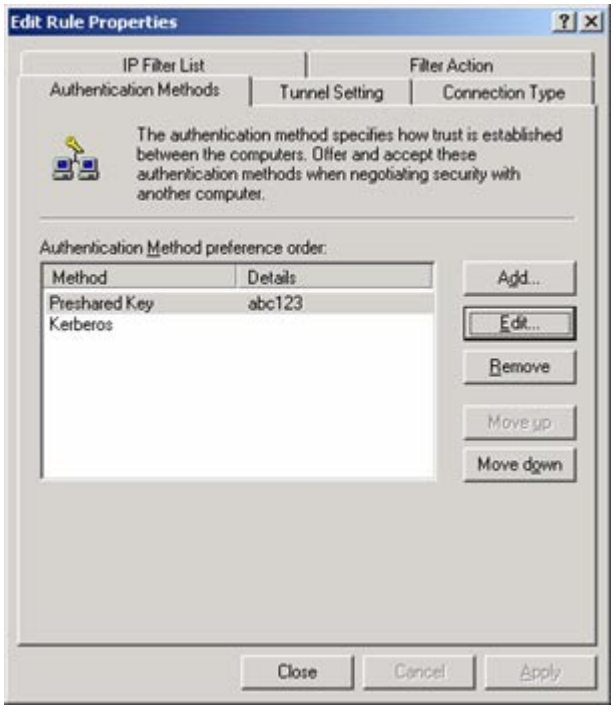
39. Select the Authentication Methods tab and click Add.

40. Choose Use this string to protect the key exchange (preshared key) and type a key value.

    Key = abc123



41. Click OK. Make sure preshared key is at the top. Use the Move Up and Move Down buttons if necessary.



42. Click Close and you are back to the To Netscreen properties dialog box. You now need to add a rule for incoming connections from the firewall.

43. Click Add, choose the IP filter List tab, and click Add again.

44. Set the name of the new filter to From Netscreen Filter.

45. Click Add.

46. In the Filter properties dialog make the following settings.

    Addressing tab

        Source Address = A Specific IP Subnet
        IP Address = 192.168.10.0
        Subnet Mask = 255.255.255.0
        Destination Address = My IP Address
        Mirrored = Unchecked.

    Protocol tab

        Protocol = Any

    Description tab

        Description = incoming

    Filter Action tab

        Check the MD5_DES filter action.

    Connection Type tab

        Connection = All network connections

    Tunnel Settings tab

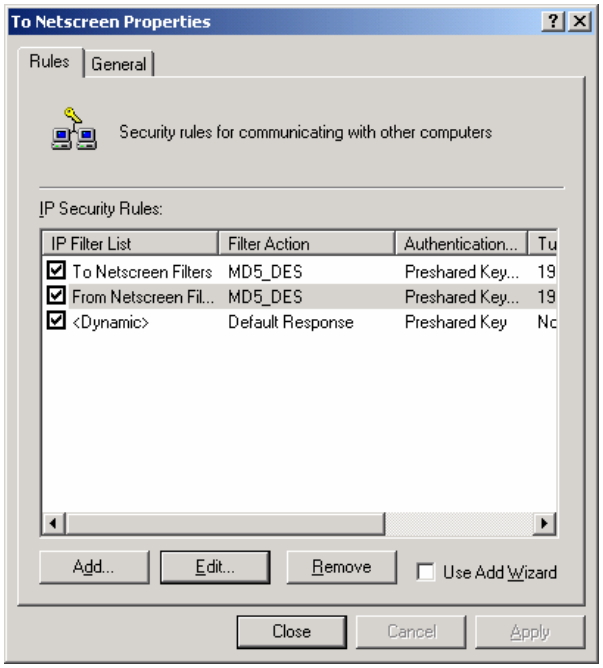
        Check: The tunnel endpoint is specified by this IP address.
        IP = 192.168.1.109 (This is the address of the Windows 2000 system.)

    Authentication Methods tab

        Create a preshared key, exactly the same as for the outgoing filters.

47. Click Close.

48. All three filters should be checked.



49. Click Close

50. Select the To Netscreen policy and choose Action, Assign to make it the active policy.

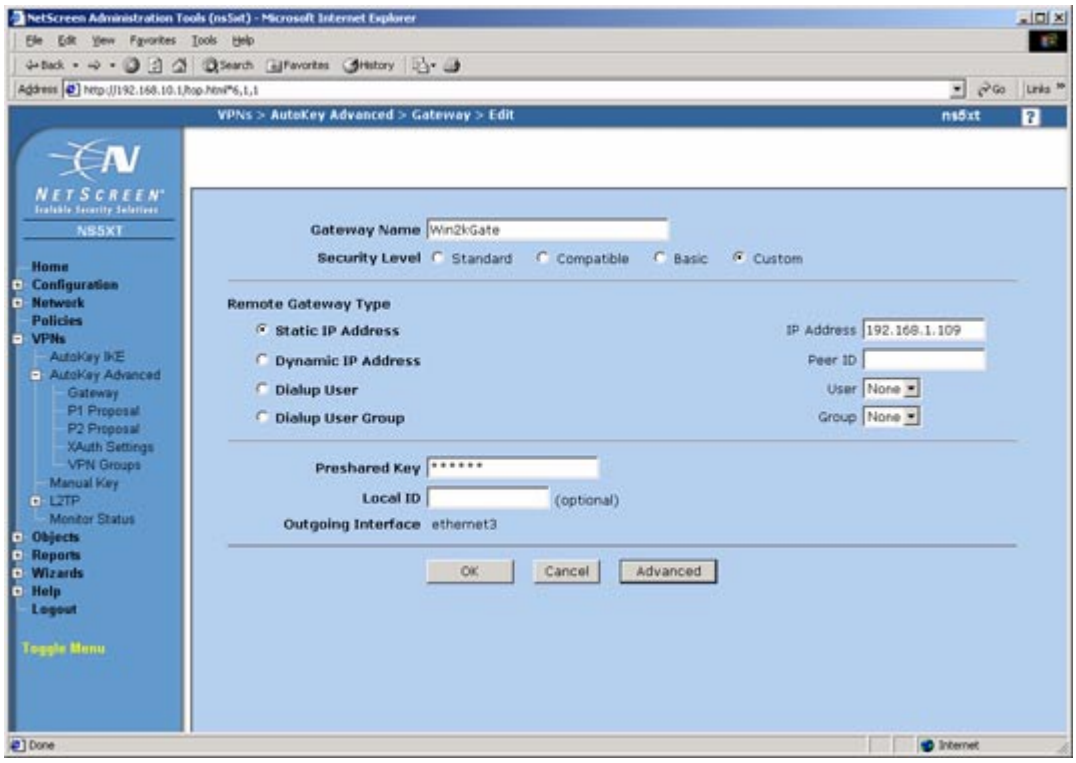
This completes the configuration of IPSec on the Windows 2000 system. Now you need to configure the Netscreen firewall to accept connections from this system and open a tunnel. Configuration of the Netscreen is either through the web based screen os or through a configuration file. The configuration file is at the end of this section.

1. Open a web browser on a system inside the Netscreen and login to the management port. This system is setup as a Work/Home system which has three ports, a work and home port inside the firewall and an untrusted port on the outside. We will be creating the tunnel between the internal Work port and the external Windows 2000 system.

2. Choose VPNs, AutoKey Advanced, Gateway and click New.

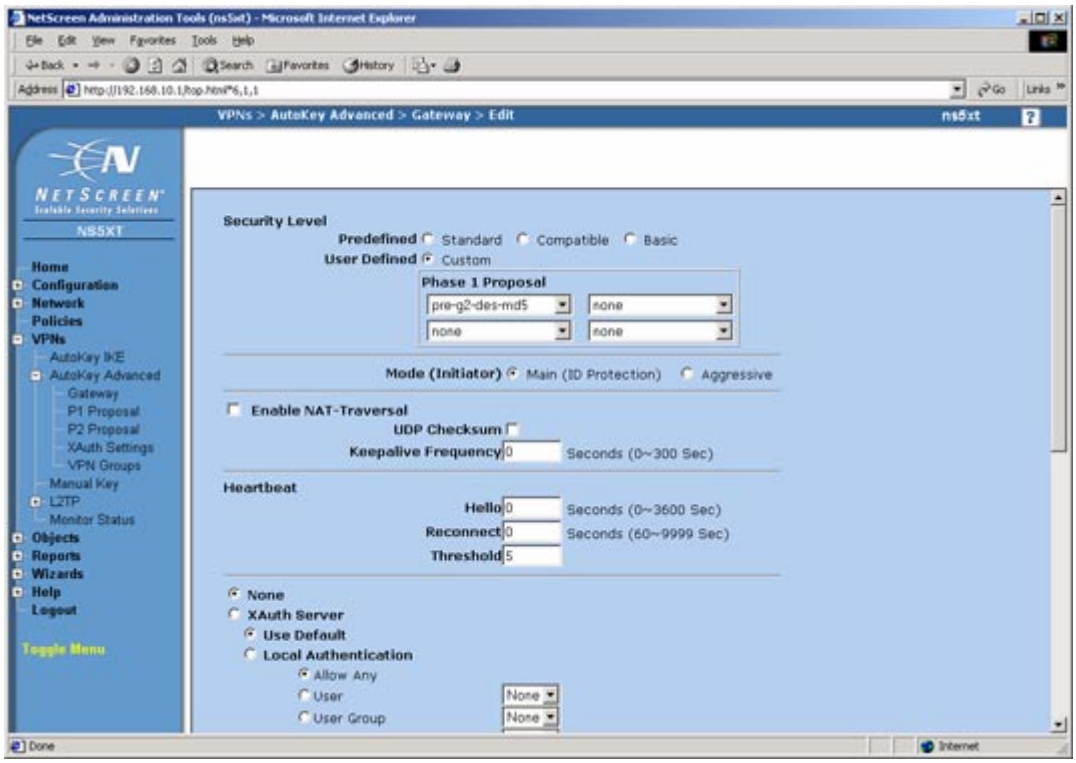
3. Make the following settings on the screen.

Gateway Name = Win2kGate
Security level = Custom
Remote Gateway Type = Static IP Accress
IP Address = 192.168.1.109
Preshared Key = abc123



4. Click Advanced and make the following settings on the screen.

   Security Level = Custom
   Phase 1 proposal = pre-g2-des-md5
   mode = main

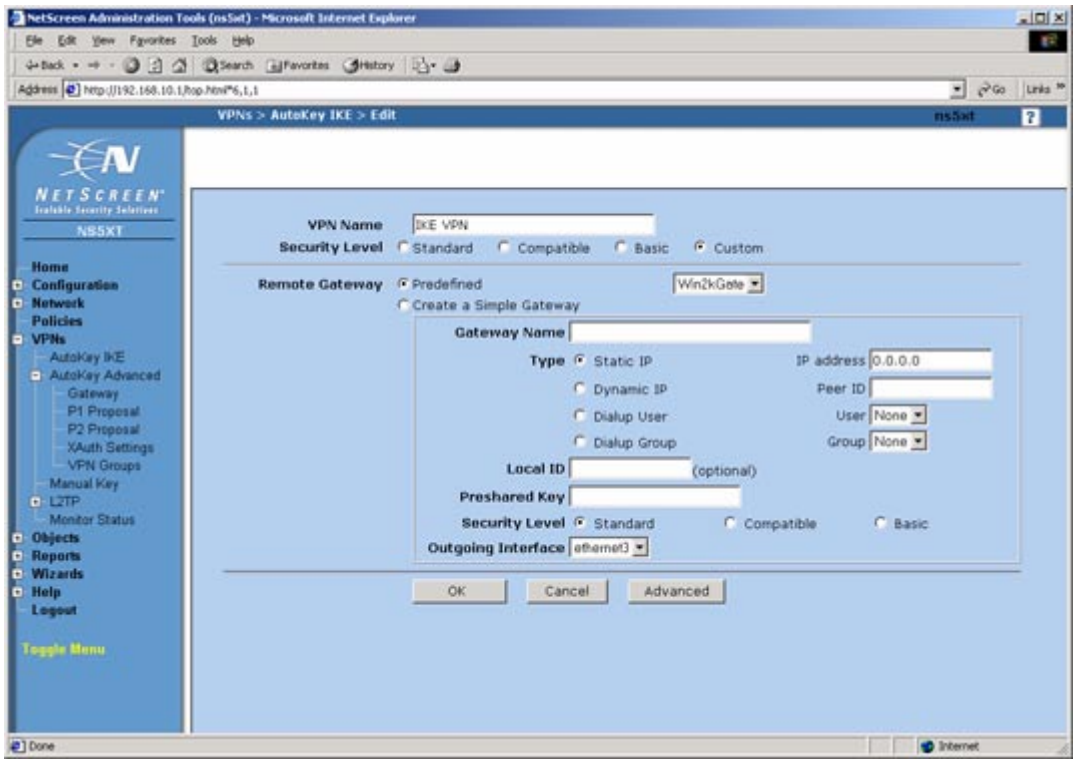


5. Scroll to the bottom of the page, click Return and then click OK.

6. Select VPNs, Autokey IKE and click New

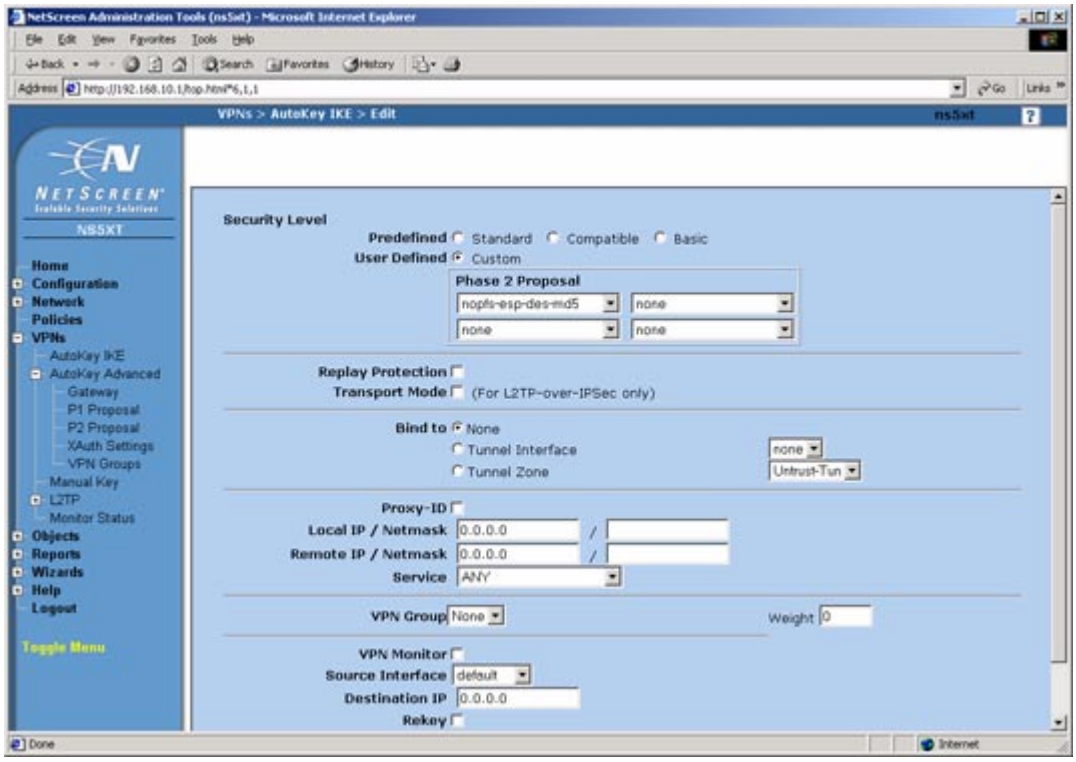
7. Make the following settings on the screen.

VPN Name = IKE VPN
Security Level = Custom
Remote Gateway = Predefined = Win2KGate



8. Click Advanced and make the following settings on the screen.

   Security Level = Custom
   Phase 2 Proposal = nopfs-esp-des-md5

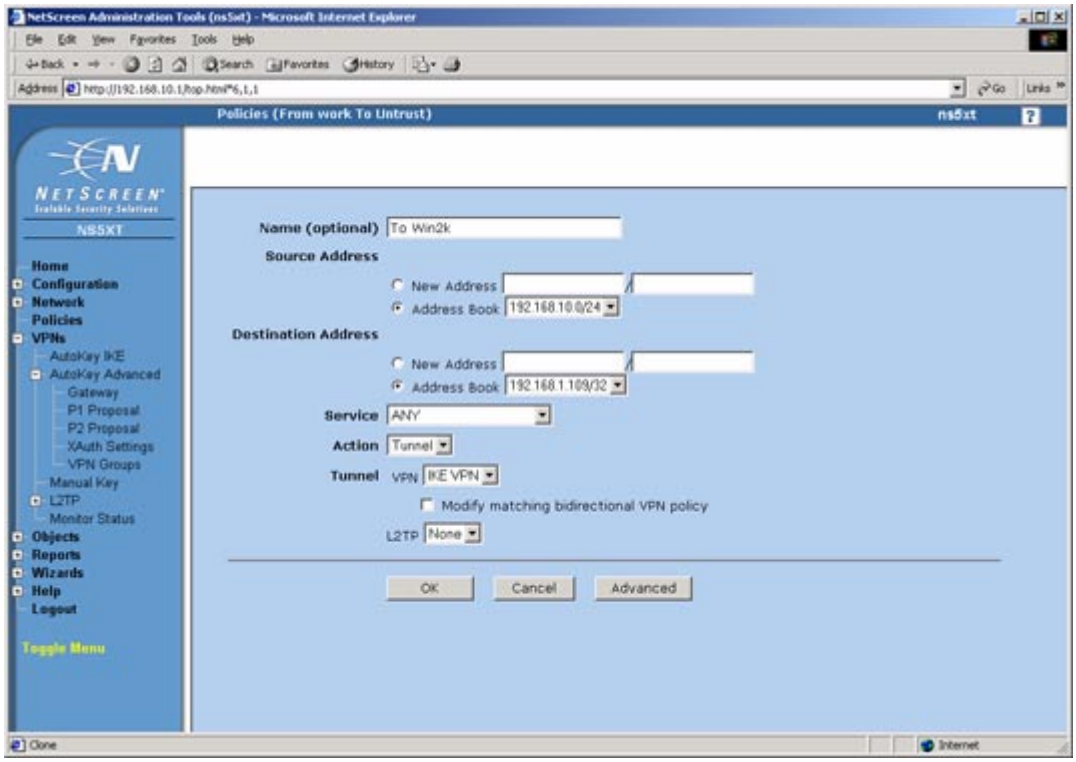


9. Scroll to the bottom, click Return, and then OK.

10. Select Policies, From: work To: Untrust, and click New.

11. Make the following settings on the screen.

Name = To Win2K
Source Address = 192.168.10.0/24
Destination Address = 192.168.1.109/32
Service = Any
Action = Tunnel
Tunnel = IKE VPN
Uncheck: Modify matching bidirectional VPN policy.
Check: Move to top.

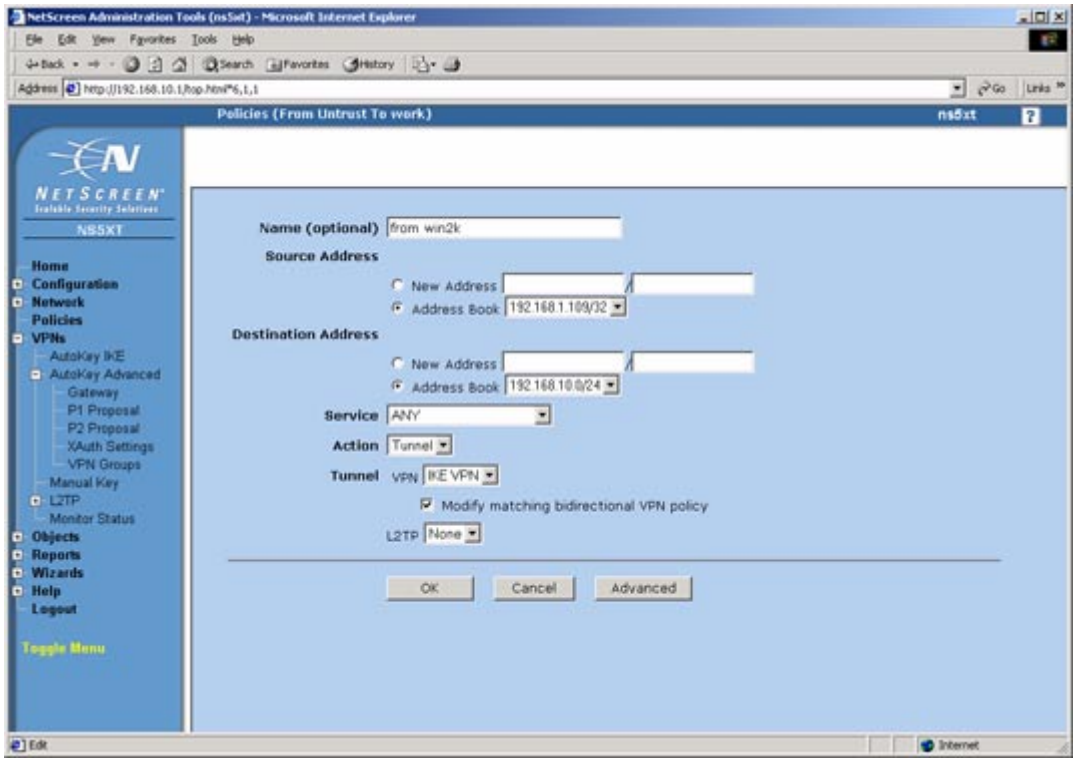


12. Click OK.

13. Select Policies, From: Untrust To: work, and click New.

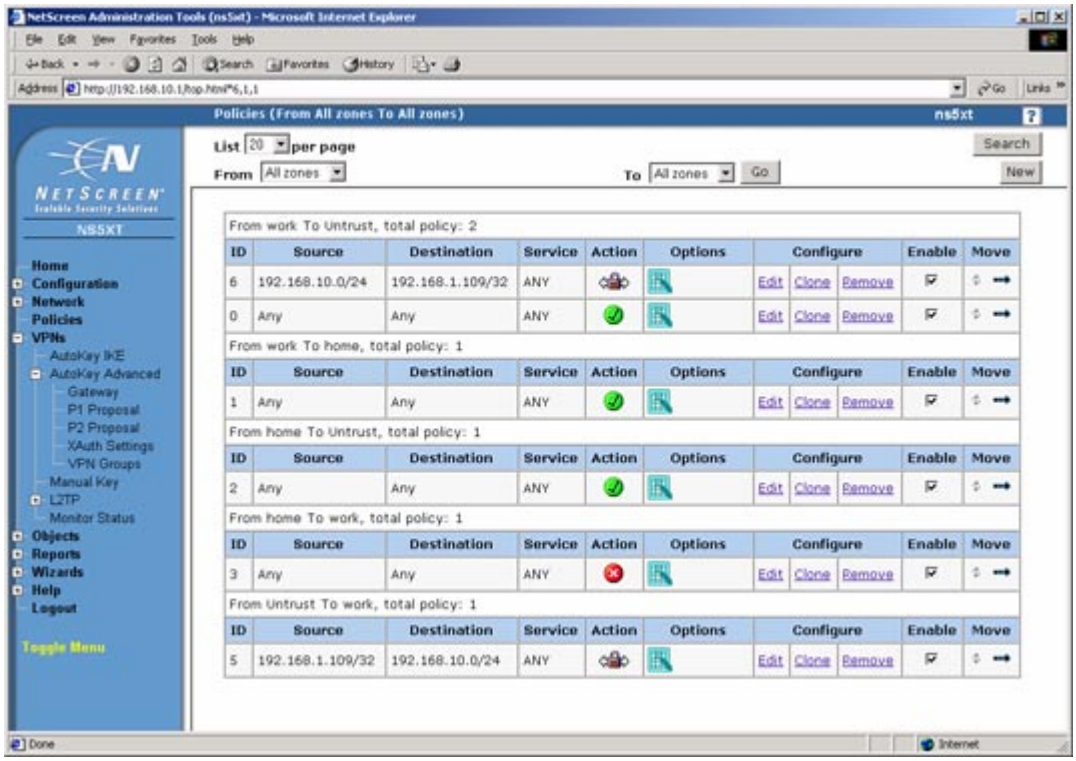
14. Make the following settings on the screen.

Name = From Win2K
Source Address = 192.168.1.109/32
Destination Address = 192.168.10.0/24
Service = Any
Action = Tunnel
Tunnel = IKE VPN
Uncheck: Modify matching bidirectional VPN policy.
Check: Move to top.



15. Click OK.

16. Select Policies so you can see them all.



This completes the configuration of the Netscreen firewall. You can now use the Remote Windows 2000 system to access machines on the inside of the Netscreen firewall. For example, you can access the management interface of the firewall. You can also go the other direction and access the Windows 2000 system from any system behind the Netscreen firewall which you could do before you made these settings, but the difference is that the communications all go through the encrypted tunnel instead of in the clear.

Below is the configuration file for the Netscreen created by making the settings in the web based screen OS. The VPN related commands are in bold.

```
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set clock "timezone" -8
set admin format dos
set admin name "netscreen"
set admin password nKVUM2rwMUzPcrkG5sWIHdCtqkAibn
set admin auth timeout 10
set admin auth server "Local"
set log module system level emergency destination console
set log module system level alert destination console
set log module system level critical destination console
set log module system level error destination console
set log module system level warning destination console
set log module system level notification destination console
set log module system level information destination console
set log module system level debugging destination console
```

```
unset log module system level emergency destination onesecure
unset log module system level alert destination onesecure
unset log module system level critical destination onesecure
unset log module system level error destination onesecure
unset log module system level warning destination onesecure
unset log module system level notification destination onesecure
unset log module system level information destination onesecure
unset log module system level debugging destination onesecure
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set zone "work" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "work" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "MGT" tcp-rst
set zone "home" tcp-rst
set zone Untrust screen tear-drop
set zone Untrust screen syn-flood
set zone Untrust screen ping-death
set zone Untrust screen ip-filter-src
set zone Untrust screen land
set zone V1-Untrust screen tear-drop
set zone V1-Untrust screen syn-flood
set zone V1-Untrust screen ping-death
set zone V1-Untrust screen ip-filter-src
set zone V1-Untrust screen land
set interface "ethernet1" zone "work"
set interface "ethernet2" zone "home"
set interface "ethernet3" zone "Untrust"
set interface ethernet1 ip 192.168.10.1/24
set interface ethernet1 nat
set interface ethernet2 ip 192.168.20.1/24
set interface ethernet2 nat
set interface ethernet3 ip 192.168.1.101/24
set interface ethernet3 route
unset interface vlan1 ip
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet2 ip manageable
set interface ethernet3 ip manageable
set interface vlan1 ip manageable
set interface ethernet1 dhcp server service
set interface ethernet2 dhcp server service
set interf ethernet1 dhcp server auto
set interf ethernet2 dhcp server enable
set interface ethernet1 dhcp server option gateway 192.168.10.1
set interface ethernet1 dhcp server option netmask 255.255.255.0
set interface ethernet2 dhcp server option lease 1440000
set interface ethernet2 dhcp server option gateway 192.168.20.1
set interface ethernet2 dhcp server option netmask 255.255.255.0
set interface ethernet1 dhcp server ip 192.168.10.33 to
   192.168.10.126
set interface ethernet2 dhcp server ip 192.168.20.33 to
   192.168.20.126
```

```
set flow tcp-mss
set hostname ns5xt
set address "work" "192.168.10.0/24" 192.168.10.0 255.255.255.0
set address "Untrust" "192.168.1.109/32" 192.168.1.109
   255.255.255.255
set snmp name "ns5xt"
set ike gateway "Win2kGate" ip 192.168.1.109 Main outgoing-
   interface "ethernet3" preshare "abc123" proposal "pre-g2-des-
   md5"
set ike policy-checking
set ike respond-bad-spi 1
set vpn "IKE VPN" id 1 gateway "Win2kGate" no-replay tunnel
   idletime 0 proposal "nopfs-esp-des-md5"
set ike id-mode subnet
set xauth lifetime 480
set xauth default auth server Local
set policy id 6 name "from win2k" from "work" to "Untrust"
   "192.168.10.0/24" "192.168.1.109/32" "ANY" Tunnel vpn "IKE
   VPN" id 5 pair-policy 5 log
set policy id 0 from "work" to "Untrust"  "Any" "Any" "ANY"
   Permit log
set policy id 1 from "work" to "home"  "Any" "Any" "ANY" Permit
   log
set policy id 2 from "home" to "Untrust"  "Any" "Any" "ANY"
   Permit log
set policy id 3 from "home" to "work"  "Any" "Any" "ANY" Deny log
set policy id 5 name "from win2k" from "Untrust" to "work"
   "192.168.1.109/32" "192.168.10.0/24" "ANY" Tunnel vpn "IKE
   VPN" id 5 pair-policy 6 log
unset global-pro policy-manager primary outgoing-interface
unset global-pro policy-manager secondary outgoing-interface
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set modem speed 115200
set modem retry 3
set modem interval 10
set modem idle-time 10
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
exit
```

APPENDIX B – AN IPSEC TUNNEL BETWEEN TWO FIREWALLS

One thing all of these home firewalls can do is to create VPN tunnels between similar devices. That is, between two home firewalls of the same brand and likely between two home firewalls of different brands. The same methods apply when creating a VPN tunnel between a home firewall and a corporate firewall. The corporate firewall is just bigger and faster.

One thing to keep in mind is licensing of VPN tunnel capability. Some brands have a different license for a client to a VPN tunnel and a server of a VPN tunnel. For example, the S-box has a different license for a firewall that can be a client to a VPN tunnel and an S-box that can be a client or server. The CISCO and NetScreen VPN capability can be either a client or a server with licenses controlling the strength of the encryption and the number of concurrent tunnels.

The setup of a connection between two firewalls is much like the connection between a workstation and a firewall. It is actually easier as the configuration of both ends of the tunnel are simply mirror images of each other. The following shows the configuration of an IPSec tunnel between a CISCO 501 and a CISCO 506 firewall.

Figure B1 shows the configuration of the network for this example. The VPN tunnel will go from one firewall to the other and connect the networks behind the two firewalls. Connections to systems elsewhere in the Internet do not go through the tunnels. The systems in the subnet behind the PIX 501 (10.10.10.x) are protected from the Internet by address translation while those behind the PIX 506 (192.168.10.x) are not. We will set this up so the addresses behind the PIX 501 are not translated when they are accessed from the network behind the PIX 506. We could also have translated those addresses into a subnet of the addresses behind the PIX 506.

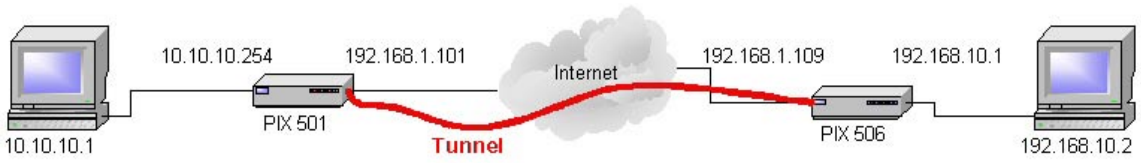


Figure B1. Configuration of the network for this example.

The CISCO PIX 506 we use in this example has only the command line interface for configuration. Below is the configuration file for that system with the commands related to the tunnel in bold.

```
Building configuration...
: Saved
:
PIX Version 5.2(5)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list acl_out permit icmp any any
access-list acl_icmp1 permit icmp any any
access-list 101 permit ip 192.168.10.0 255.255.255.0 10.10.10.0
   255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 10baset
icmp permit 192.168.10.0 255.255.255.0 outside
icmp permit any outside
mtu outside 1500
mtu inside 1500
ip address outside 192.168.1.109 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
arp timeout 14400
global (outside) 1 192.168.1.101
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-group acl_out in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
   h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
no floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set mytransform esp-des esp-md5-hmac
crypto map mymap 1 ipsec-isakmp
crypto map mymap 1 match address 101
crypto map mymap 1 set peer 192.168.1.101
crypto map mymap 1 set transform-set mytransform
```

```
crypto map mymap interface outside
isakmp enable outside
isakmp key ******** address 192.168.1.101 netmask 255.255.255.255
isakmp identity hostname
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
dhcpd address 192.168.10.2-192.168.10.10 inside
dhcpd lease 3600
dhcpd domain llnl.gov
dhcpd enable inside
terminal width 80
Cryptochecksum:9a9bdddd992b32fc18d85f0d8bf0d7f9
: end
```

Looking at the bold commands separately, you can see how they turn on the different parts of the IPSec tunnel.

Create a rule (access-list 101) that says the two networks behind the firewalls can talk to each other. This rule is used with other commands to specify who the commands apply to.

```
access-list 101 permit ip 192.168.10.0 255.255.255.0 10.10.10.0
   255.255.255.0
```

Allow an incoming connection from the PIX 501 (WAN address 192.168.1.101).

```
global (outside) 1 192.168.1.101
```

Do not do NAT on the addresses specified in address list 101 even though they appear behind the firewall. Connections coming through the tunnel will appear to be behind the firewall but we do not want to translate them. We could also translate them into a subnet of the addresses behind the PIX 506 to make them appear to be on that network instead of on a remote network.

```
nat (inside) 0 access-list 101
Turn on IPSec
sysopt connection permit-ipsec
```

The crypto commands set the configuration of the tunnel such as the type of encryption and authentication for phase 2 of the connection (DES and MD5 here), the address of the remote end of the tunnel (192.168.1.101), and the addresses to allow through the tunnel (access-list 101).

```
crypto ipsec transform-set mytransform esp-des esp-md5-hmac
crypto map mymap 1 ipsec-isakmp
crypto map mymap 1 match address 101
crypto map mymap 1 set peer 192.168.1.101
crypto map mymap 1 set transform-set mytransform
crypto map mymap interface outside
```

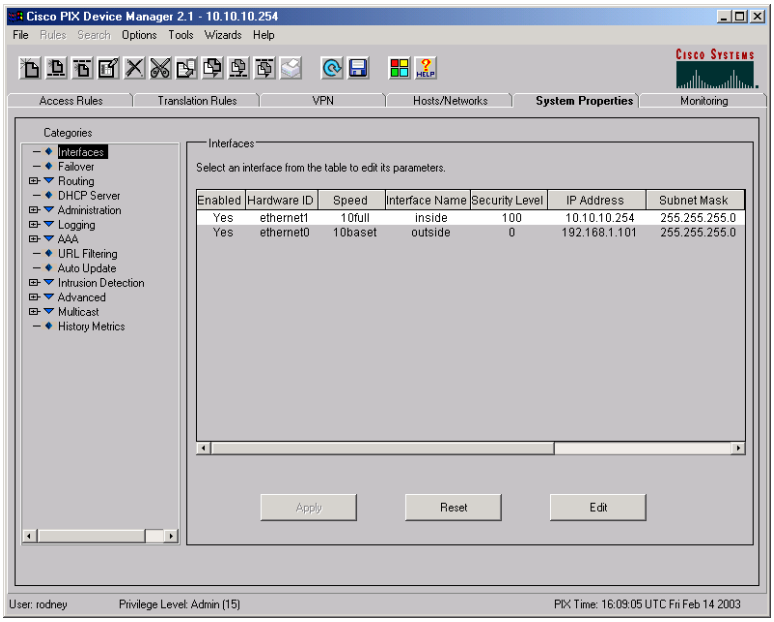
The isakmp commands turn on the authentication part of the IPSec tunnel (Phase 1) with the remote system. Here, we use a pre-shared secret which is hidden in the printout with *******. When a system is setup, the actual value of the shared secret would be used here. We also set the encryption and authentication for phase 1 of the tunnel setup.

```
isakmp enable outside
isakmp key ******** address 192.168.1.101 netmask 255.255.255.255
isakmp identity hostname
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 1000
```

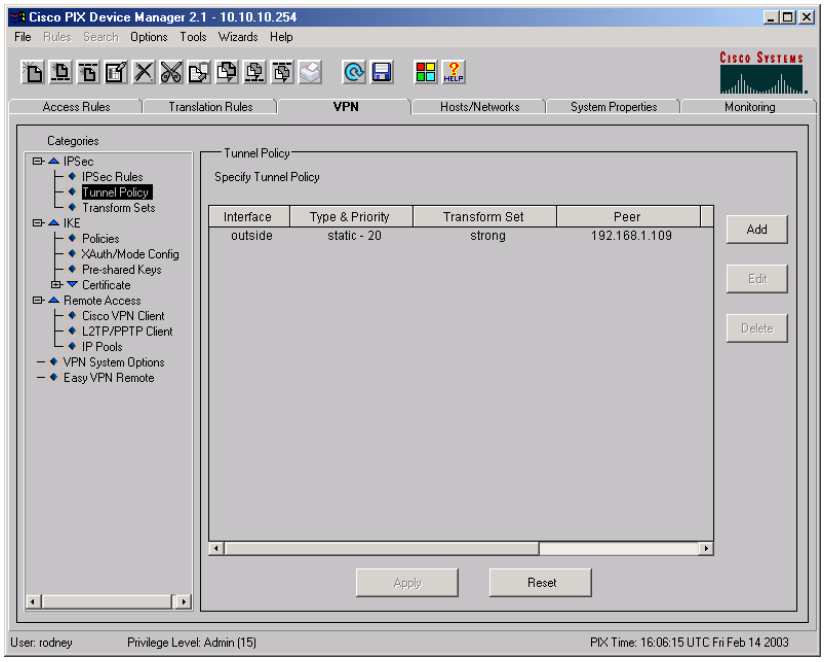
This completes the configuration of the PIX 506 now do the configuration of the PIX 501.

From the system 10.10.10.1, you can login to the inside, LAN port of the PIX 501 (10.10.10.254) using a web browser which starts the PIX Configuration Manager.

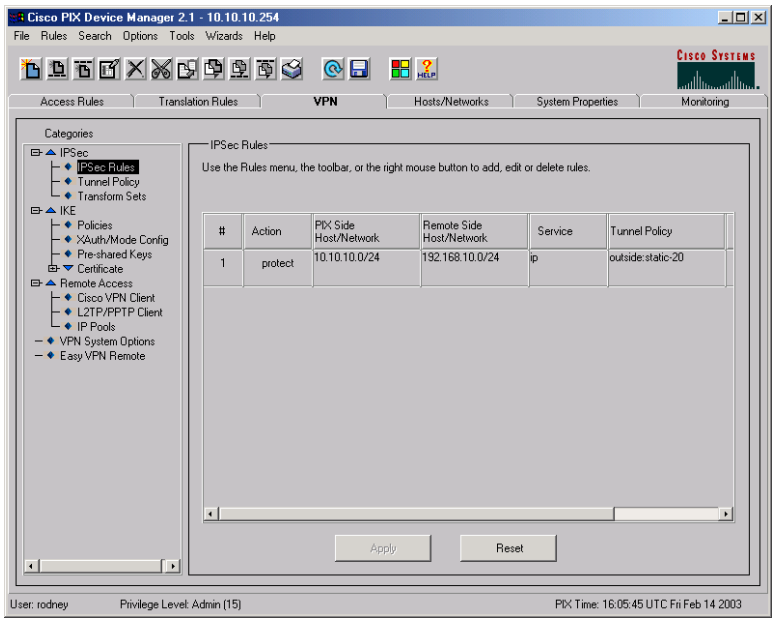
1. After logging in, check the configuration of the interfaces. Here you can see that the LAN and WAN interfaces are set as indicated in Figure B1.



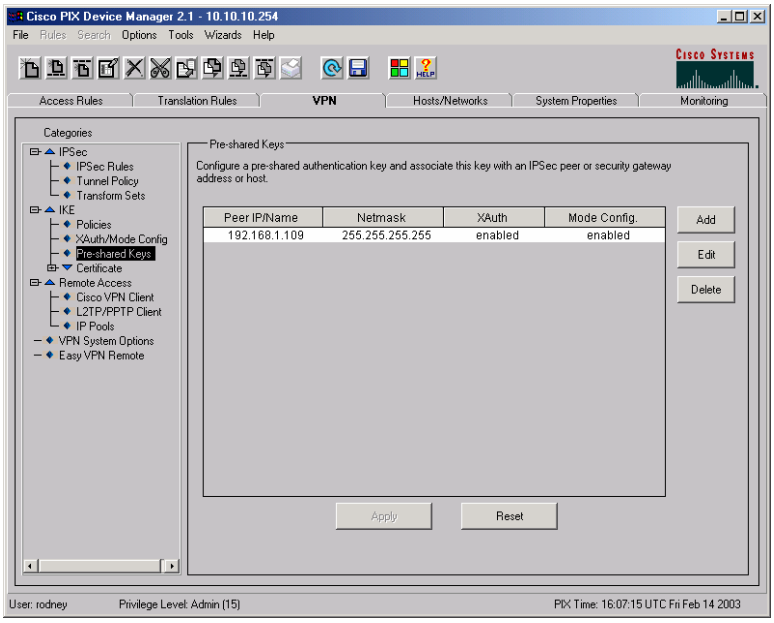
2. Select the VPN tab and Tunnel Policy category and add a new policy for the outside (WAN) interface with the settings below. The Peer is the external WAN address of the PIX 506 you are going to connect this tunnel to. The strong transform set is the name of the set that defines the encryption and authentication to use (DES and MD5) in Phase 2 of the IPSec tunnel.



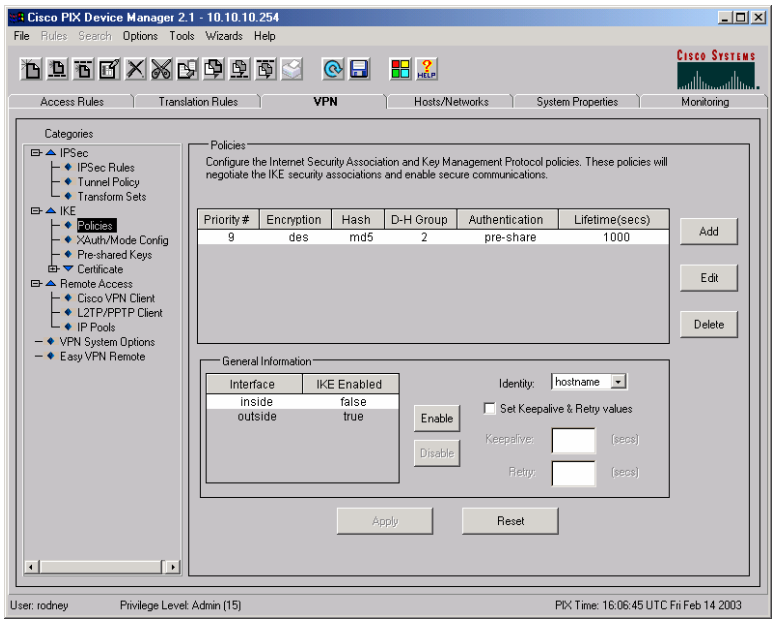
3. Select the VPN tab, the IPSec Rules category and add a new rule using the Rules menu. Set the options to protect IP connections from the 10.10.10.0/24 network to the 192.168.10.0/24 network using the policy specified in the last step.



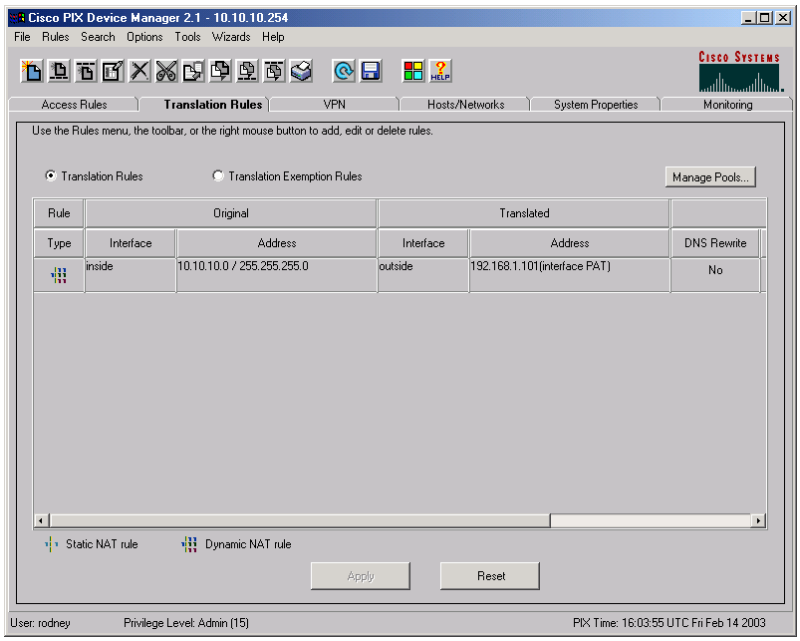
4. Select the VPN tab, Preshared Key category and create a pre-shared key for use with the authentication step of the IPSec tunnel. This should use the same key as was entered into the setup of the PIX 506.



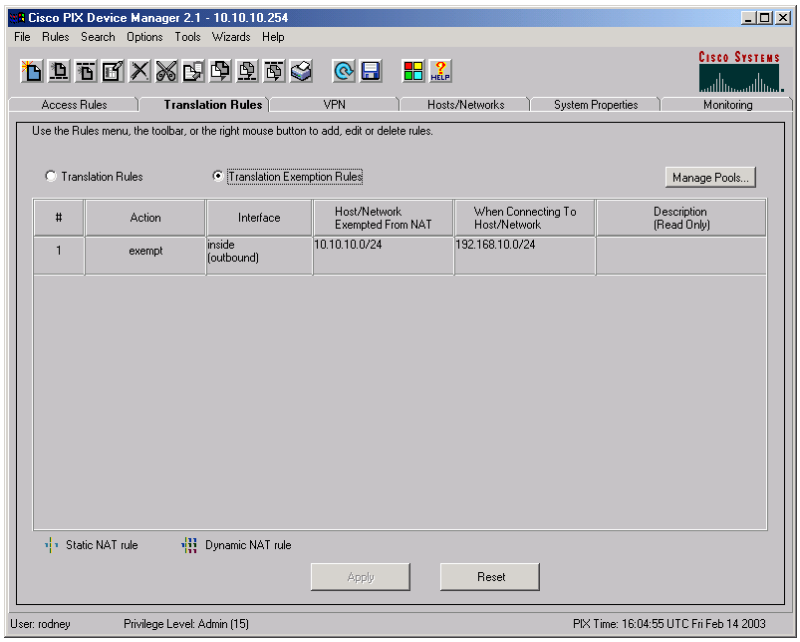
5. Select the VPN tab, Policies Category and create the authentication policy for Phase 1 of the IPSec tunnel. Here we use the pre-shared key created in the last step.



6. Select the Translation Rules tab and click the Translation Rules option. Create a rule that translates the addresses on the internal subnet to the outside address of the PIX 501 when connections are going to systems outside of the firewall.



7. Switch to the Translation Exception Rules option and create an exemption rule to leave alone connections that are going to the subnet behind the PIX 506.



8. Save these changes to the setup and update the system.

This completes the configuration of the PIX 501. The following command line interface result shows the current configuration of this system. The options related to the tunnel are in bold. Note that the bold items are the same as were used for the PIX 506. The options set in those items point in the opposite direction on the network or use different defined names.

```
: Saved
:
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname demopix
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list 90 permit ip 10.10.10.0 255.255.255.0 192.168.10.0
   255.255.255.0
access-list 91 permit ip 10.10.10.0 255.255.255.0 192.168.10.0
   255.255.255.0
pager lines 24
logging console debugging
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 192.168.1.101 255.255.255.0
ip address inside 10.10.10.254 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm location 10.10.10.1 255.255.255.255 inside
pdm location 192.168.1.101 255.255.255.255 outside
pdm location 192.168.1.109 255.255.255.255 outside
pdm location 192.168.1.106 255.255.255.255 outside
pdm location 192.168.1.106 255.255.255.255 inside
pdm location 192.168.1.109 255.255.255.255 inside
pdm history enable
arp timeout 14400
global (outside) 10 interface
nat (inside) 0 access-list 91
nat (inside) 10 10.10.10.0 255.255.255.0 0 0
access-group inside_access_in in interface inside
route outside 0.0.0.0 0.0.0.0 192.168.1.109 1
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
   h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa authentication enable console LOCAL
aaa authentication ssh console LOCAL
aaa authorization command LOCAL
http server enable
http 10.10.10.1 255.255.255.255 inside
http 192.168.1.109 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set strong esp-des esp-md5-hmac
crypto map toWin2k 20 ipsec-isakmp
crypto map toWin2k 20 match address 90
crypto map toWin2k 20 set peer 192.168.1.109
crypto map toWin2k 20 set transform-set strong
crypto map toWin2k interface outside
isakmp enable outside
isakmp key ******** address 192.168.1.109 netmask 255.255.255.255
isakmp policy 9 authentication pre-share
isakmp policy 9 encryption des
isakmp policy 9 hash md5
isakmp policy 9 group 2
isakmp policy 9 lifetime 1000
telnet timeout 5
ssh 192.168.1.106 255.255.255.255 outside
ssh timeout 5
dhcpd address 10.10.10.1-10.10.10.9 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
dhcpd enable inside
username rodney password TiWzUlj7GolYii.N encrypted privilege 15
privilege show level 0 command version
privilege show level 0 command curpriv
privilege show level 3 command pdm
privilege show level 3 command blocks
privilege show level 3 command ssh
privilege configure level 3 command who
privilege show level 3 command isakmp
privilege show level 3 command ipsec
privilege show level 3 command vpdn
privilege show level 3 command local-host
privilege show level 3 command interface
privilege show level 3 command ip
privilege configure level 3 command ping
privilege configure level 5 mode enable command configure
privilege show level 5 command running-config
privilege show level 5 command privilege
```

```
privilege show level 5 command clock
privilege show level 5 command ntp
terminal width 80
Cryptochecksum:0254ab217dc4756a259cd9f842871c63
: end
```

This tunnel can now be used. Whenever a system on the subnet behind the PIX 501 tries to connect to an address in the 192.168.10.x subnet, the packet is captured, the tunnel is opened, and the packet is sent through. The same thing happens when a system on the network behind the PIX 506 tries to send a packet to the 10.10.10.x subnet. When the tunnel opens, it stays open for communications in either direction or times out and closes if it is not being used.

APPENDIX C – A PPTP CONNECTION BETWEEN A WORKSTATION AND A FIREWALL

This appendix shows an example of how to connect a workstation to a firewall using a PPTP tunnel. In this case, we connect a Windows 2000 workstation to a CISCO PIX 501 firewall. The settings used here are similar to what you would use for other operating systems and firewalls.

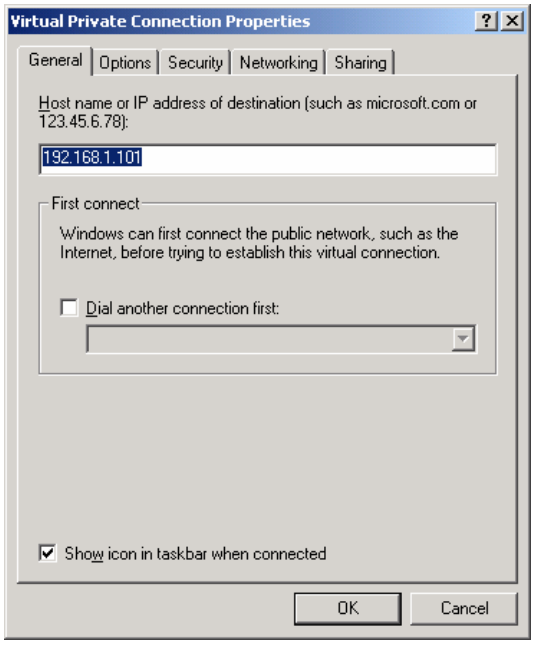
A PPTP tunnel is one of the easiest to set up as most systems have automatic configuration capabilities for PPTP.

1. Login to the PIX and open the PIX Device Manager.
2. Choose the Wizards, VPN Wizard command.
3. In the dialog box, choose Remote Access VPN.
4. Choose Outside as the interface. Click Next.
5. Choose the PPTP protocols to allow. PAP, CHAP, and MSCHAP are available. You could allow them all to have the most flexible server but PAP is a clear text login and should be unchecked unless it is absolutely necessary.
6. Choose Authenticate using local username/password database. This indicates that the user you are going to allow to connect must have a username and password stored on the PIX.
7. Click Finish to setup the server.
8. Create an account on the firewall for the remote user you are going to allow to connect this tunnel if you have not already done so.

This completes the configuration of the PIX. Now switch to the Windows 2000 system.

1. Login to the Windows 2000 system.
2. Start the Network and Dial-up Connections control panel.
3. Double Click Make New connection to start the wizard and click Next.
4. Choose, Connect to a private network through the Internet. Click Next.
5. For the Destination address, type the address of the WAN connection on the PIX. Click Next
6. Choose Create this connection only for myself. Click Next.
7. Type a name and click Finish.

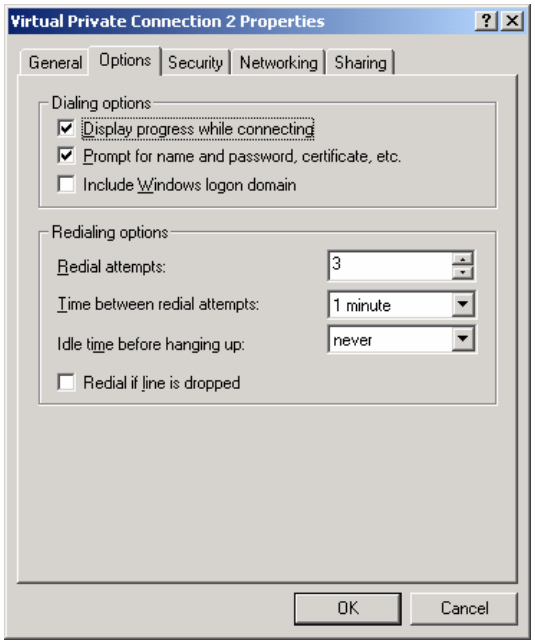
8. Right click on the newly created connection and choose Properties. The General tab should show the IP address of the external (WAN) interface of the firewall.



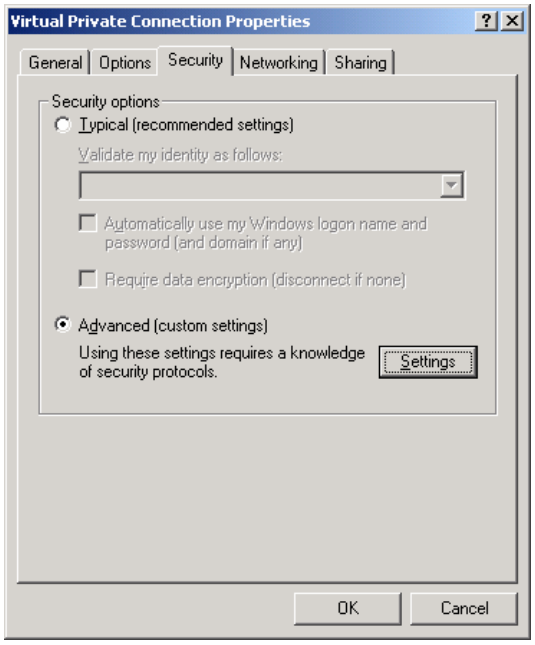
9. Click the Options tab. The settings should be,

   Display progress while connecting = Checked
   Prompt for name and password, certificate, etc. = Checked
   Include Windows login domain = Unchecked

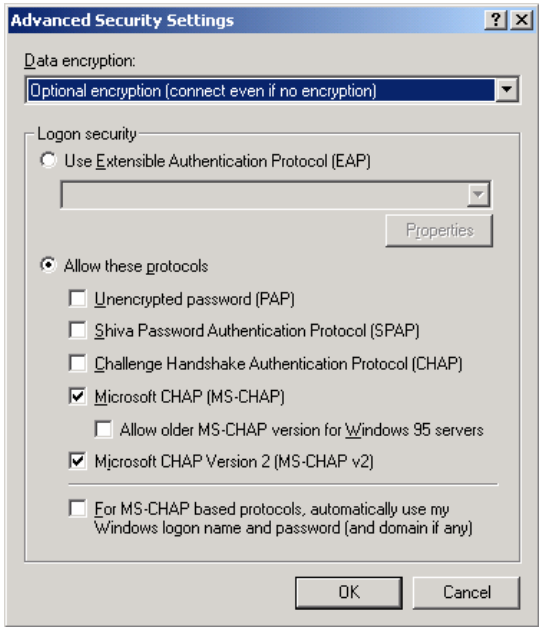
   Do not change the Redial options as they are not used here.



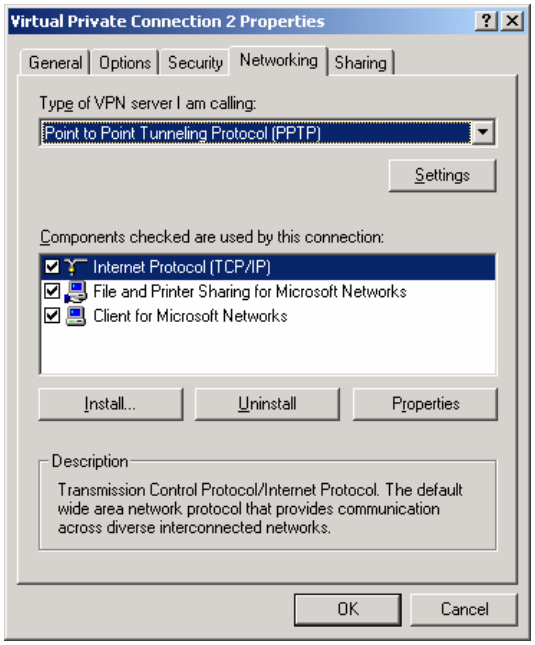
10. Click the Security tab, Click the Advanced option.



11. Click Settings. Make sure only MS-CHAP and MS CHAP version 2 are selected. Click OK

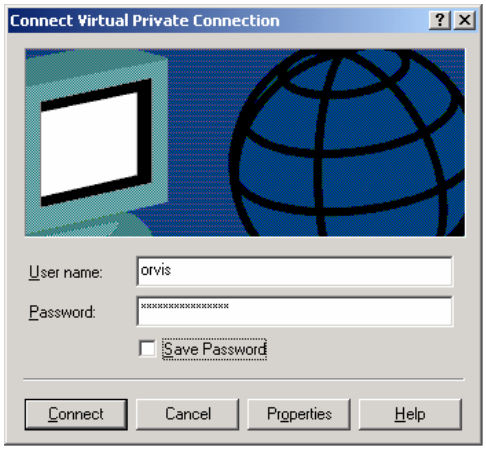


12. Choose the Networking tab and set the type of server to PPTP. In the components box, select those networking components that can use this VPN. At a minimum, you need TCP/IP.



13. Click OK.

The settings for the PPTP connection are done and the connection icon is now in the Network and Dial-up Connections control panel. To open the connection simply double click on it, type in the username and password for the firewall, click Connect, and the connection should open.



APPENDIX D – GLOSSARY

The following are definitions of computer related terms in this report. More computer related terms than you ever believed existed are available in *The Jargon File* (http://www.tuxedo.org/~esr/jargon/).

ACK Packet – A TCP/IP packet with the ACK (acknowledge) flag set. It is used to acknowledge the successful receipt of a packet.

AES – Advanced Encryption Standard. A fast, symmetric, block cipher. AES can use 128, 192, or 256 bit keys. See FIPS-197

AH – See Authentication Header.

Administrator – The highest level of access on a Windows system. Equivalent to root on a UNIX based system. The Administrator of a system can do anything on that system.

Adware – Software that displays ads on your computer and attempts to target the ads to your browsing habits. See also spyware.

Authentication Header – A VPN tunnel transport protocol where the packet contents are not encrypted. The AH header authenticates the message so that only the defined sender and receiver can use the tunnel. It prevents an outsider from taking over a tunnel. See also ESP.

Backdoor program – A hacker's version of pcAnywhere. That is, it allows a remote user to take control of a system, see what is on the desktop, capture keystrokes, move and click the mouse, and run any program on the system. Backdoor programs are distributed by viruses and worms and are sent to users via e-mail. The e-mail versions generally have a provocative title designed to get the user to run it. When a backdoor program is run once on a system, it installs and hides itself and makes settings that restart it whenever a system is rebooted. Some backdoor programs advertise their availability to specific sites or to IRC chat groups.

Blended Threat – Malicious code that is a combination of types. Blended threats combine the capabilities of viruses, worms, Trojans, and exploits to increase the likelihood that they can get to and take control of a system.

Broadband – High-speed, Internet access. In this paper it includes everything but dial-up modems. Most broadband connections are on all the time and includes, cable modems, DSL, and ISDN. ISDN is included here with Broadband connections even though it does require a dial-in.

Byte – A chunk of digital data consisting of eight binary bits. The amount of information needed to encode a single character.

Cable Modem – A modem for connecting a computer to a cable TV network and route digital data through that network. Cable networks currently operate at speeds of about 400k bits per second.

Challenge Handshake Authentication Protocol – A network authentication protocol that uses a challenge/response protocol so as to not send a password in the clear over the network. See also PAP and MSCHAP.

CHAP – See Challenge Handshake Authentication Protocol.

Class A subnet – See subnet and subnet mask. A subnet that reserves the first octet for the network address and the right three octets for the machine address. The network mask is 255.0.0.0. There are 255*255*255 = 16,581,375 addresses available for systems in this subnet. A class A subnet is usually further broken down into smaller subnets. See also subnet, subnet mask, class B subnet, class C subnet.

Class B subnet – See class A subnet. A subnet that reserves the left two octets for the network address and the right two for the machine address. The network mask is 255.255.0.0. There are 255*255 = 65,025 addresses available for machines. See also subnet, subnet mask, class A subnet, class C subnet.

Class C subnet – See Class A subnet. A subnet that reserves the left three octets for the network address and the right one for the machine address. The network mask is 255.255.255.0 and there are 255 addresses available for machines. See also subnet, subnet mask, class A subnet, class B subnet.

Command Shell – A text interface to an operating system. The shell is able to interpret and execute typed commands.

Cryptographic signing – Generating a security signature for a block of data such as the text of an e-mail message. The signature becomes invalid if the message is changed. It is extremely difficult to pad a message to make a certificate valid. That is, it is difficult to fake the signature of a signed message.

Daemon – A program that stays in memory and provides some service to other programs on a computer or to programs that connect to it through a network port.

DES, 3DES – Digital Encryption Standard. A high-speed, symmetric, block cipher. DES uses 56 bit keys. 3DES applies DES to the data 3 times with two different keys to create an effective 168 bit encryption. See also AES. See FIPS 46-3

Dynamic Host Configuration Protocol (DHCP) – A method of sharing IP addresses. When systems first connect to the network, they request an IP address from the DHCP server. The server returns the address along with other network configuration data.

Dial-up modem – A method of sending digital data using analog (voice) telephone lines at a rate of up to 56k bits per second. Digital data is converted into a series of tones that are sent

over the analog lines and converted back into digital data by another modem at the other end.

Domain – A Windows networking term for all the machines that participate in a single grouping for networking and authentication services. Login credentials are stored on a Domain server and a user need login only once to get access to all the machines he is allowed access to within the domain.

Domain Administrator – The administrative account for domain level logins In a Windows Domain. Domain Administrators generally have administrative access to all the machines in the domain.

Domain Server – The main administrative server in a Windows domain. It stores the login credentials for all the machines and users in the Domain.

DoS – Denial of Service (note the lower case "o"). An attack where a server is overwhelmed in some way to prevent it from accepting connections from legitimate users. Bogus connection attempts are often used to overwhelm a system.

DoS Master – The controlling machine in a Denial of Service (DoS) attack. The Master machine controls multiple Zombies that perform the actual attack. See also Zombie.

DOS – Disk Operating System (note the upper case "O"). Microsoft's older, pre-windows, command line operating system.

Drone – See Zombie.

DSL – Digital Subscriber Line. A high-speed data connection that uses telephone wires to send digital data at rates up to 1.5m bits per second. A user must be within 1.5 miles of the telephone substation.

Dumpster Diving – Digging through the trash to find usernames, passwords, and other information to use to compromise a system.

Encapsulating Security Payload – A VPN transport protocol where the contents of the transported packets are encrypted. The encryption prevents the packets from being viewed and authenticates the packets so the tunnel cannot be taken over. See also AH.

Encryption – A method of changing a message in such a way that only specific entities can read it. Modern encryption involves algorithms that make the data look like random numbers. Only people with the key can decrypt the information and read the message. See also symmetric encryption and public key encryption.

ESP – See Encapsulating Security Payload.

ESSID – The network name of a wireless network.

Exploit Scripts – See Scripts.

Exploits – See Scripts.

FAT, FAT16, FAT32 – File Allocation Table type of file system. This type of file system is used on DOS and the DOS based Windows systems (Windows 3.2, 95, 98, ME). It has no file access protections. The number refers to the size (bits) of the block descriptors in the file allocation table. The bigger the descriptors, the more blocks a drive can be broken up into. A block of sectors is the smallest chunk of a disk drive that can be allocated to a file. FAT (=FAT12) file systems had too few blocks for new, larger disk drives, hence the creation of FAT16 and FAT32. See also NTFS.

File Authorization – See Program Authorization.

File Transfer Protocol (FTP) – A protocol and program for transferring files between two computers via a network.

FIN Packet – A TCP/IP packet with the FIN (finished) flag set. Tells a remote system that no more data is coming. Used to close a properly opened session.

Firewall – A hardware or software device that controls access in and out of a subnet. Using a set of rules, a firewall examines (filters) every packet attempting to enter or leave a network and decides if the packet can continue or not. Firewalls can be simple, packet filters, or may do stateful packet inspection.

FTP – See File Transfer Protocol.

Gateway – A networking device that is the path out of the local network. This is where packets are sent that have a destination that is not on the local network.

Guest – An account on most systems that allows unauthenticated access to a system. This can be an extremely bad security hole if it is not carefully controlled.

GUI – Graphical user interface. A computer interface that uses a mouse, windows, and menus to control a computer. See also Command shell.

Hacker – A computer user who is extremely knowledgeable and interested in the details about how a computer system works. This term has been misused as a name for computer intruders who break into systems and perform malicious acts.

Hardware firewall – A networking appliance that protects a subnet from attacks by a larger network. All connections to the protected subnet must pass through the firewall, be inspected, and be selectively blocked according to a set of rules. See also software firewall.

Hub – A network device for sharing a 10-baseT Ethernet connection among several systems. Packets that go in any port come out all the other ports. See also switch.

ICQ – Short for “I Seek You.” An instant messaging service owned by AOL.

Internet – An internet is a collection of interconnected networks. The Internet (capital I) refers to the international collection of public networks that grew out of the Arpanet.

Integrated Services Data Network – A high-speed data connection that uses telephone wires to send digital data at rates up to 64k bits per second. ISDN is a dialed network like analog phones but is digital end to end. It can be connected to the Internet or directly connected to a company's internal network.

Intruder – A computer user who breaks into other people's systems.

IPSec – See IP security.

IP security. A protocol for setting up and encrypting all IP communications between two systems.

ISDN – See Integrated Services Digital Network.

ISP – Internet Service Provider. A person or company that provides a connection to the Internet.

Kerberos – An authentication scheme developed at MIT that uses cryptographic certificates to give access to objects such as systems.

L2TP/IPSec – See Level 2 Tunneling Protocol over IPSec.

LAN – Local Area Network. The network on the inside of a router or firewall. The local network where all your machines are. See also WAN.

LanMan – The old Windows network authentication protocol. This protocol is used by Windows 95, and 98. Se also NTLM.

Level 2 Tunneling Protocol over IPSec – An encryption protocol that uses UDP packets. Originally developed for serial connections, it is combined with IPSec to assure delivery.

Local Compromise – A type of attack on a system where an intruder with a normal user's account on that system is able to get root access to that system.

Logic bombs – Programs that wait for some trigger (date, user action, etc.) and then destroy files on a computer.

Login session – All the packet traffic associated with a single login to a networked resource. Also called a session. Communications between two computers is done with packets that contain one or more characters of data. To start a session, the two computers exchange three packets. All packets following the three are data packets. A single packet closes the session. All of the data in the data packets combined together is the session.

Malware – See malicious code.

Malicious code – Malicious software. Computer code that is specifically written to do destructive or inappropriate things. For example, damaging or compromising a computer and its

files. Includes: viruses, worms, Trojans, logic bombs, and exploits. See also virus, worm, Trojan horse.

MD5 – Message Digest number 5. A cryptographic checksum used for validating data. Changing the data makes the checksum invalid. It is extremely difficult to pad some data to make it get a specific checksum. That is, it is extremely difficult to fake.

Media Access Control (MAC) Address – The built-in hardware address of an Ethernet card.

Middleware – Software that resides between a server and your data files. For example, an indexing program that generates a web index or a search engine that is executed by a web server in response to a web page and that returns data via the web server to the user.

Microsoft Challenge Handshake Authentication Protocol – A network authentication protocol that uses a challenge/response so as to not put the password on the network. This is the Microsoft version. See also PAP and CHAP.

MSCHAP – See Microsoft Challenge Handshake Authentication Protocol.

NAT – Network Address Translation. A method to reduce the need for more IP addresses by allowing one address to be shared among several machines. It is also used to block access to the sharing machines by allowing only outgoing connections from the sharing machines and blocking incoming connections.

Network connection – A connection between two computers that is shared among many computers. Whichever computer needs to communicate with another puts packets on the network addressed to the receiver. All computers on the network listen for packets addressed to them. This is in opposition to a point-to-point connection.

NTFS – NT File System. The file system introduced with Windows NT. This file system has intrinsic file access control. See also FAT.

NTLM and NTLM2 – The newer Windows network authentication protocols. These have much better security than the older LanMan protocol.

One-time password – A method for authenticating with a remote system that uses a password that works for only one login. To make a second login requires a new password.

Packet – The smallest chunk of digital data sent as a unit over a network. A packet may contain a single keystroke or several pages of text plus all the source, destination, and routing information needed to get the data to its intended recipient. Maximum packet sizes are normally around 1500 bytes.

Packet Filtering – A method of filtering packets based on the contents of the packet stream. Packet Filtering must also employ stateful packet inspection in order to be able to look at the contents of the whole stream and not just a single packet. This is different from a simple packet filter.

PAP – See Point-to-Point Protocol.

Password Cracking Program – A program for determining the value of encrypted passwords by encrypting a possible password and comparing that to the encrypted password it is trying to determine. Password cracking programs have access to whole dictionaries (including foreign) of encrypted passwords so if a password is a word in a dictionary, it can be easily cracked.

Point-to-Point connection – A connection between two computers that is not shared with other computers. It appears to be a single wire connecting the two systems. All information sent down the connection is assumed to only be directed to the system at the other end of the connection. A telephone call is a point-to-point connection. This is in opposition to a network connection.

Point-to-Point Protocol – An authentication scheme that sends clear text passwords over the network. See also CHAP and MSCHAP.

Point to Point Tunneling Protocol – An extension of the PPP protocol used over serial links to it can be routed over a network. PPP allows packets to be passed from a system over a serial link to appear on a remote network. To allow it to be used over a network instead of a serial cable it was combined with an IP tunneling protocol.

Port – A connection between an application program and a network. Port numbers are used to connect a program running on one machine with the appropriate program running on another. A network packet contains routing information that includes both the address of the machine the packet is being sent to and the port number of the running program on that machine. The routing information also includes the source address and source port so the program that received a packet knows where to send any reply.

Port Forwarding – Mapping of a port on a server host inside a firewall to a port on the outside interface of the firewall so the service can be accessed by users outside of the firewall.

PPTP – See Point to Point Tunneling Protocol.

Program Authorization (File Authorization) – A filtering method where only specific files or programs on a computer are allowed to connect to the Internet. This is primarily used to block outgoing connections by viruses and worms.

Proxy server – A mechanism in a firewall where a service or port on a protected system is made to appear to be on the outside of the firewall. Connections to the port on the outside of the firewall are passed to a designated system and port on the inside and connections from the system on the inside are passed to the outside.

PSTN – Public Switched Telephone Network. The phone company.

Public key encryption – A nonsymmetric encryption method that employs two keys, a secret key and a public key. Encryptions made with one key can be decrypted by the other. Knowing the public key, it is extremely difficult to create the secret key. You keep and

protect the secret key and give everyone the public key. If someone wants to send you an encrypted message, they encrypt it with your public key and send it to you. You can decrypt it with your secret key. The encryption is not symmetric so knowledge of the public key will not allow you to decrypt the message encrypted with it.

Rcp – Remote copy. A program for copying files between two machines.

Remote Compromise – A type of attack where an intruder somewhere on the Internet attacks and gets root access to a system. The intruder does not need any access to the system other than the network connection to be able to compromise it. That is, he does not need a user account on the system (Local Compromise) or to have physical access to the system.

Rlogin – Remote login. A program for connecting to another system and opening a command shell there.

Root Access – A term describing the highest level of access on a system. A person with root access (equivalent to Administrator on a Windows system) on a system can do anything on that system. What an intruder wants most.

Routing – The act of determining where the destination of a packet is and sending it there. See router.

Router – A router is a networking device that determines through which of its ports a packet needs to go in order to get to its destination.

Rsh – Remote shell. A program for connecting to another system and opening a command shell there.

RST Packet – A TCP/IP packet with the RST (reset) flag set. Tells a remote system to reset the connection. Its primary use is to reset a connection when the connection has not been setup correctly.

Runlevel – Unix based operating systems have different runlevels numbered from 0 through 6 which determine which services are running for a particular situation. When you change runlevels, the system starts up and shuts down different services. The following lists the most common use for the different runlevels.

Runlevel – Use
0 – Halt, turn off all services and shut down
1 – Single-user mode, used for maintenance
2 – Not used (user-definable)
3 – Full multi-user mode, command line interface
4 – Not used (user-definable)
5 – Full multi-user mode, with an X-windows user interface
6 – Reboot, turn off all services and restart the system

Scanning – A method of determining what ports are open on what machines by sending packets to those ports to see how they respond. Scanning programs usually scan many ports on a single machine or single ports on many machines.

Scripts – This term applies to all automated processes. Originally these were interpreted programs written in the command language of the system being used or in a common interpreted language like Perl. Current scripts can be fully compiled programs. Scripts that automate security compromises are also called exploit scripts or exploits.

Secure Shell (SSH) – A program for creating an encrypted connection between two machines. SSH opens a command shell (command line interface) on the remote machine that a user can use to run programs and transfer files on the remote machine. SSH is available in both commercial and public license versions.

Secure Sockets Layer (SSL) – A method of encrypting network sessions between two machines that resides at the socket layer. Applications that use this kind of encryption do not need to know how it works, they only need to use the appropriate network port or socket. It is mostly used by web servers (https connections) but can be used by other communication protocols.

Security certificate – A block of data that contains security information such as a user's name and the user's allowed access. The block is cryptographically signed and may be encrypted to protect it from change and from viewing by unauthorized personnel. The security certificate is used to access resources and to initialize encryptions such as tunnels.

Service – A program running on a system that provides data or an action to another program or system. Services generally listen to network ports, waiting for requests for the service they provide. A web server service provides web pages to remote clients.

Session – See Logon Session.

Session key – An encryption key used to encrypt a network session. A network session is initially opened using a user's key, password, or certificate using public key cryptography. Public key cryptography is too slow for most sessions so a faster, secret key cryptography such as DES is used. A session key is generated, encrypted with public key cryptography, and sent to the other end of the tunnel. There it is used as the secret key to encrypt/decrypt packets for the rest of the session. The session key may be changed often during a session to make it more difficult to break the encryption.

SHA-1 – Secure Hash Algorithm revision 1. A cryptographic checksum used for validating data. Changing the data makes the checksum invalid. It is extremely difficult to pad some data to make it get a specific checksum. That is, it is extremely difficult to fake.

Shell – See Command Shell.

Simple Packet Filter – A packet filtering mechanism that filters single packets based only on the routing information in that packet. This is different from Packet filtering.

Sniffer – A program that puts your network interface into promiscuous mode so it can capture copies of all packets on the attached network. Sniffer programs thus "listen in" to communications between other systems.

Social Engineering – A method intruders and malicious codes use to get access to information and systems by fooling a human user of that system. For example, an intruder might pose as a computer repairman to talk a user out of a password.

Software firewall – A firewall program that runs on the protected system. It watches incoming and outgoing connections to a protected system and selectively blocks connections depending on a set of rules. Software firewalls can also authorize applications on the protected system to connect to the network. See also hardware firewall.

Split Tunneling – A VPN setup option that routes packets destined for the VPN network through the VPN tunnel and packets destined for other destinations directly to the Internet. When split tunneling is disabled, all packets must pass through the VPN network including those destined for locations outside of the VPN network.

Spyware – Software that watches your browsing habits and sends that information to a marketing company's server. See also adware.

SSH – See Secure Shell.

SSL – See Secure Sockets Layer.

Stateful Packet Inspection – A firewall filtering method that maintains the state of a session so it can allow those packets belonging to a session to pass while blocking those that do not. Stateful packet inspection is especially needed in situations where a protocol uses more than one data connection such as FTP.

Subnet – A piece of an IP network address space. IP addresses are defined as four numbers (called octets) separated by periods. A subnet is a group of sequential addresses that are assigned to a contiguous computer network. For example, all the systems in a building or office or workgroup are assigned addresses from a single subnet. See also subnet mask, class A subnet, class B subnet, class C subnet.

Subnet mask – An IP address is defined as four numbers separated by periods. Each number can range from 0 to 255 (an eight bit byte) so there are a total of 32 bits that can be used to address a system. A subnet mask is used to break an IP address into two parts. The left side is the network address and the right side is the machine address within a subnet (see subnet). The subnet mask is also a 32 bit number. To break an IP address into two parts, place a 1 in each bit position on the left side that is part of the network address and a 0 in each bit position on the right side that is part of the machine address. For example, the IP address 192.168.1.10 with a mask 255.255.255.0 defines a network address of 192.168.1.x and a machine address of 10 within that subnet. Doing this with binary shows how the mask splits the address.

11000000 10101000 00000001 00001010 = 192.168.1.10

11111111 11111111 11111111 00000000 = 255.255.255.0

The subnet defined with this mask can have up to 254 machines in it (addresses 0 and 255 have special meanings). The subnet mask does not need to break the address space between two octets but can break it anywhere depending on the need for addresses. See also subnet, class A subnet, class B subnet, class C subnet.

Switch – A network device for sharing a 10-baseT Ethernet connection among several systems. Packets that go in any port are only routed to the port where the destination system exists. See also hub.

Symmetric encryption – An encryption method where applying the algorithm once to the data encrypts it and applying it a second time decrypts it. See also encryption, public key encryption.

SYN Packet – A TCP/IP packet with the SYN (synchronize) flag set. The first packet in a TCP/IP session, requesting a remote system to open a port and synchronize the packet sequence numbers.

TCP Stack – The software drivers that handle network connections and decode network packets. When a packet of information is received from a network, it is passed up the stack until the packet type matches the type of packet a layer knows how to handle. The layer then decodes the information and passes it up the stack for more decoding. Eventually the information reaches the application program that it was destined for.

Telephone Modem – A device for sending digital information over analog telephone lines with a maximum speed of around 33k bits per second.

Telnet – A protocol and program for remotely logging into a system and creating a command shell.

Transport mode – A VPN method for transporting packets from one network to another that leaves the original packet header in place and adds an AH or ESP header to authenticate the packet.

Trojan Horse – A malicious code that appears to be one thing while doing another. For example, the AIDS Trojan deleted the files on your hard disk while you read about AIDS. See also virus, worm, malicious code.

Tunnel – A networking analogy. Packets sent through a tunnel are actually encrypted at the source, sent over the network to the destination, and then decrypted. The packet contents cannot be seen (except in encrypted form) while they are traversing the network making it appear that they are hidden inside of a tunnel or pipe.

Tunnel mode – A VPN method for transporting packets that hides the original packet header in the tunnel. Only the endpoints of the tunnel can be gleaned from the AH or ESP header that transports the packet.

Unicode – A text encryption scheme that uses two bytes instead of just one to encode a single character. Unicode is needed for character sets that have more than 256 characters (such as Asian characters), which is the maximum number of characters that can be encoded with a single byte.

URL – Universal Resource Locator. A method for explicitely identifying a networked resource. The format is: *service*://*username*:*password@host*:*port*/*path*. Where *service* is the computer service that will handle the request such as http for a web server. *Username* and *password* fields are available to allow you to login to a protected resource. *Host* is the host name of the server computer that contains the resource. *Port* is the port number and is only needed if the service is not on the standard port. *Path* is the path to the resource within the server.

URL blocking – A firewall rule that blocks all connections to a specific URL.

Virtual Private Network (VPN) – A networking option that creates an encrypted pipe between a system and a remote subnet. The system is made to appear to be directly attached to that subnet and all network communications pass through the encrypted pipe to protect them from being intercepted.

Virus – A malicious code that travels from system to system by attaching itself to other programs and documents. See also Trojan horse, worm, malicious code.

VPN – See Virtual Private Network.

WAN – Wide Area Network. The network on the outside of a firewall or network that connects to the Internet. See also LAN.

Web client – A computer program for displaying web pages. Web pages are requested from a web server and displayed by a web client. Internet Explorer and Netscape Navigator are web clients.

Web server – A computer program that makes web pages available to others via a network. Web clients send page requests to a web server and the server returns the requested page. Netscape and Apache servers are web servers.

Windows Domain – See Domain.

Wired Equivalent Privacy (WEP) – An encryption method for protecting wireless communications. The original WEP specification contained flaws that allowed the encryption to be broken with little difficulty. New systems improve the security by increasing the size of the encryption key to 128 bits or by using the new WEP2 standard.

Wireless Access Point – A router that routes between wireless and wired networks. That is, it has an Ethernet connection on one side and a wireless antenna on the other. Most home wireless access points include basic firewall features such as NAT.

Wireless LAN (WLAN) – A computer network that uses radio communications (and occasionally infra-red) for networking.

Worm – A malicious code that transports itself from system to system, usually through some security hole including social engineering. See also virus, malicious code, Trojan horse.

Zombie – A computer used in a denial of service (DoS) attack. A DoS Master machine controls multiple zombies. The zombies send the packets that actually comprise the attack. See also DoS Master.

Department of Energy

CIAC

Computer Incident Advisory Capability

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551