Session ID 46CM

AS/400 IP Packet Filtering & NAT

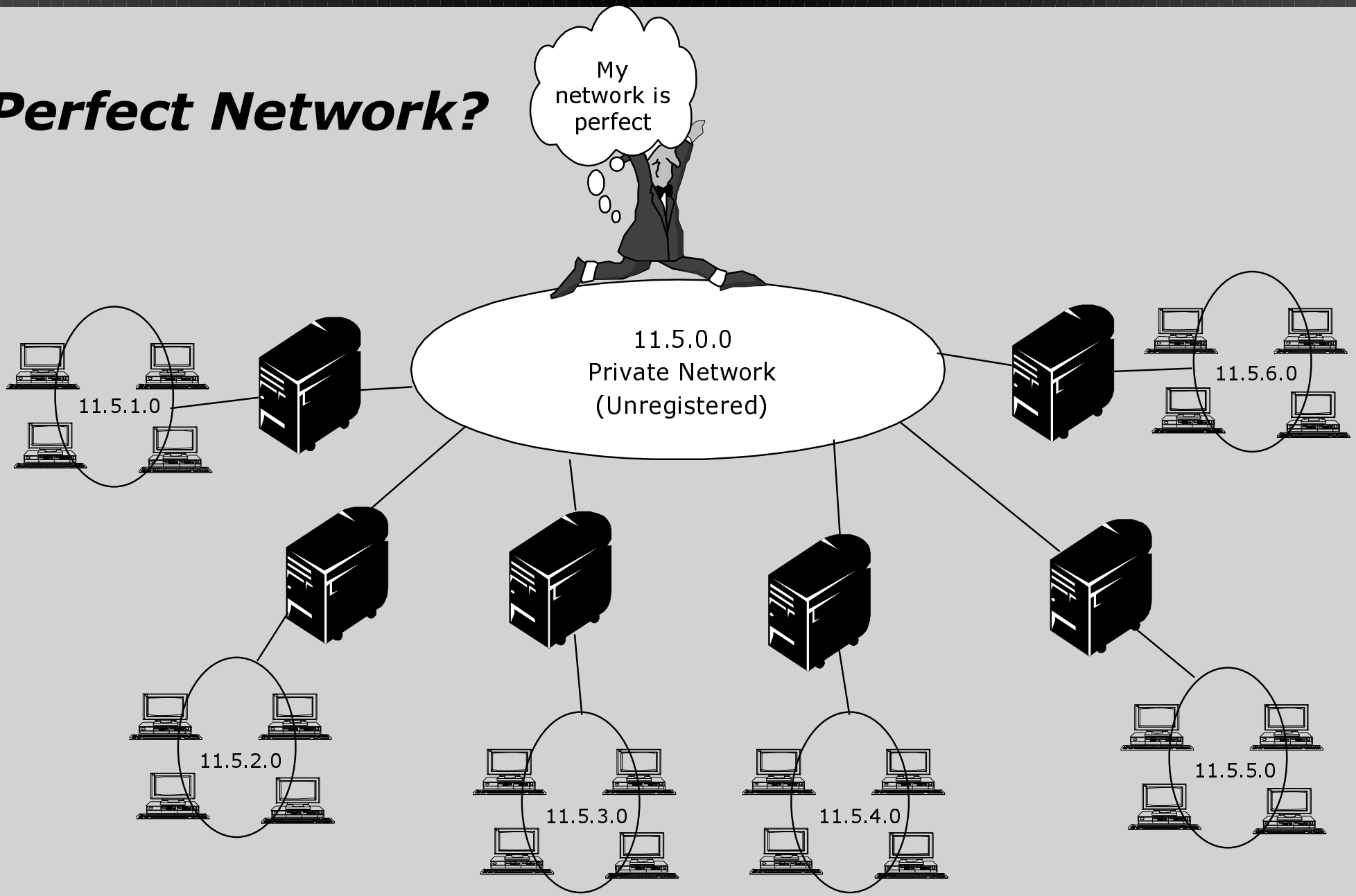
Ed Boden
AS/400 TCP/IP Development

Objectives

- Describe Network Address Translation (NAT)
- Describe IP Filtering
- Define the steps needed to configure NAT and filtering

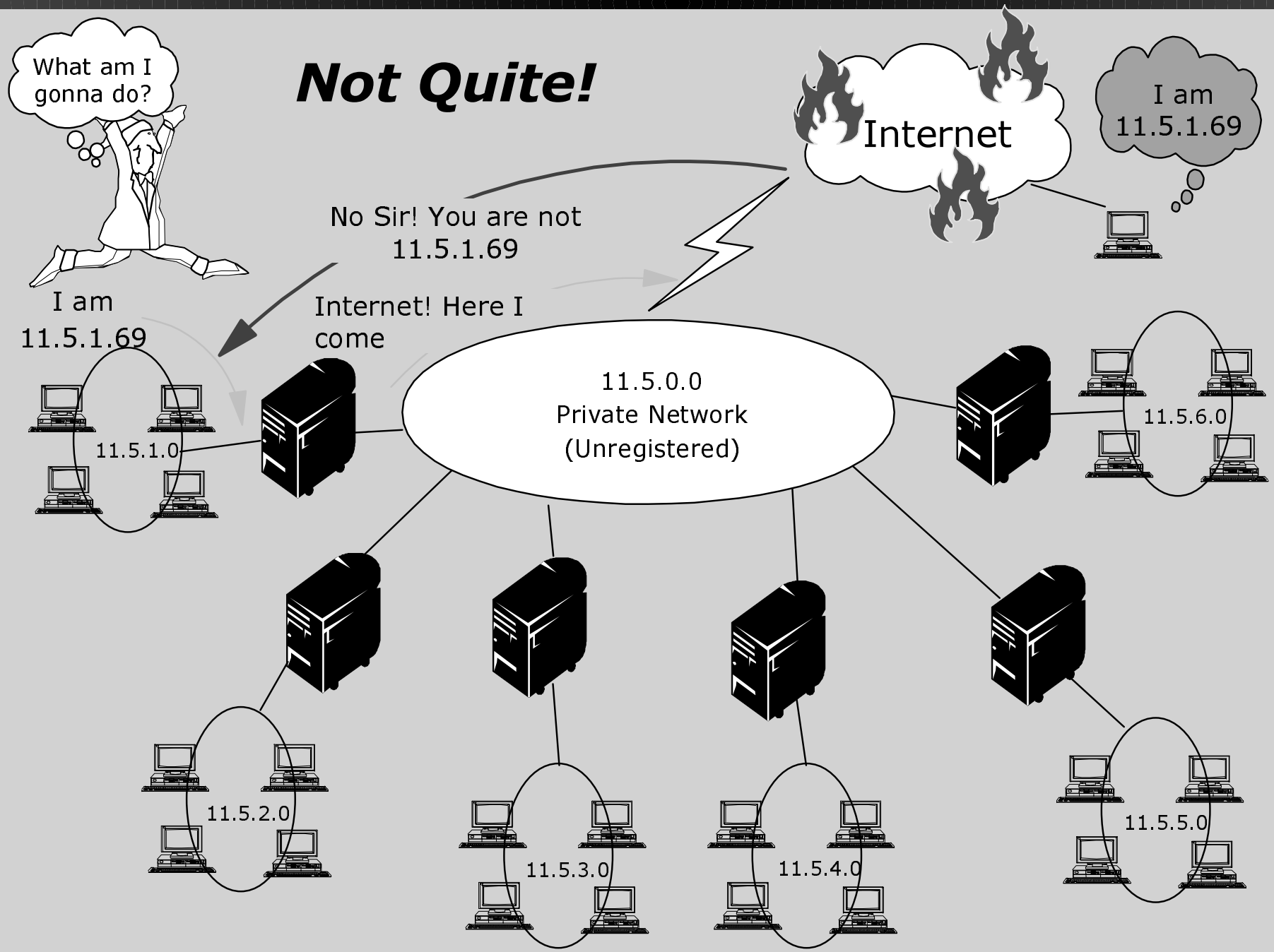
Network Address Translation (NAT)

Perfect Network?



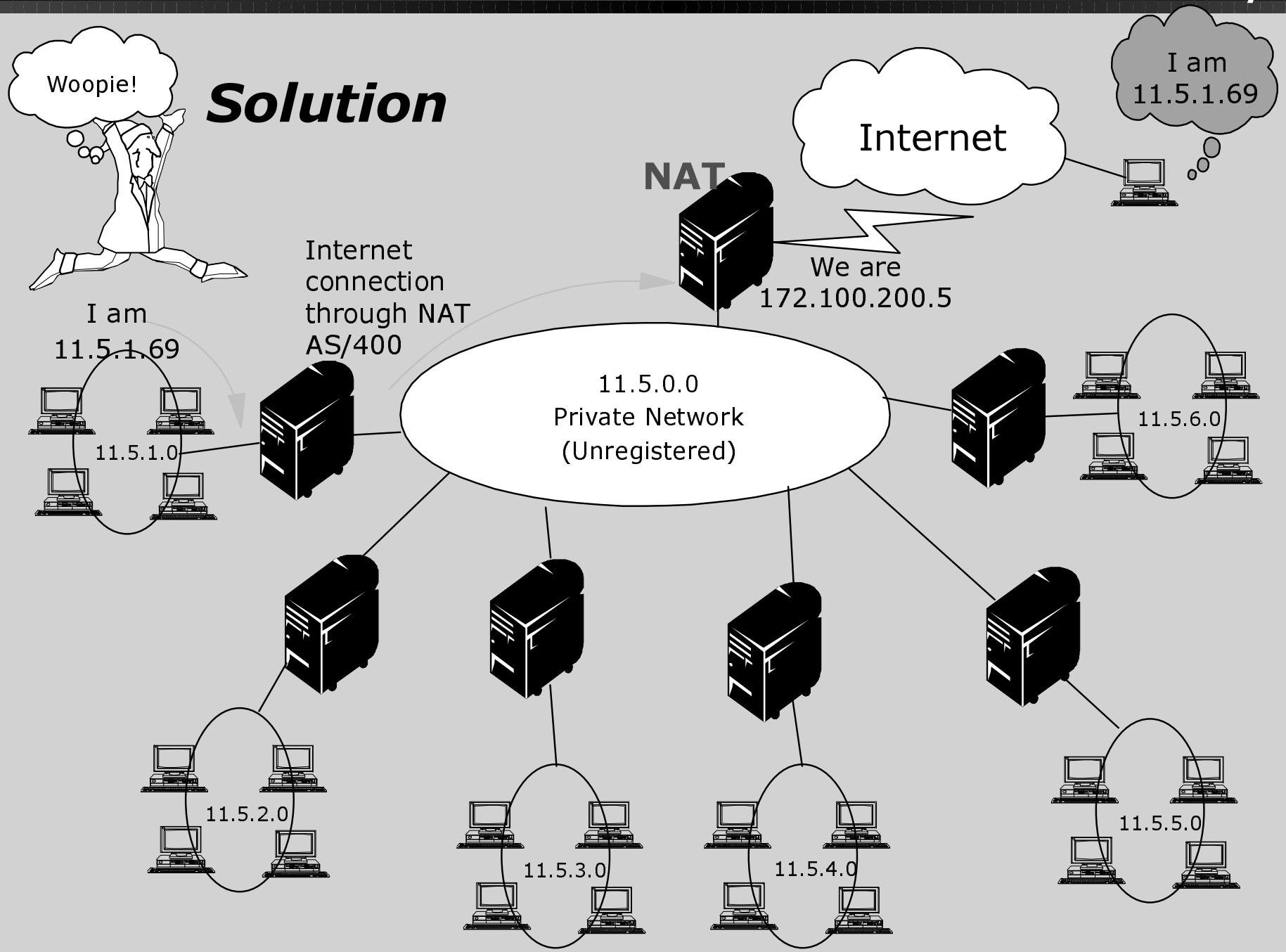
Perfect Network?

- Most of the organizations today, have started implementing private networks.
- These networks may be unregistered networks without proper authentication and permission of any international organization (IANA) and work fine as intranets as long as they are isolated from the rest of the world.
- This practice can have serious repercussions. Once we are out there on the internet, we might be using an address range owned and registered by others.
- This organization has implemented an excellent network, that works fine while they are restricted to their own networks.
- Everything seems to be in-place but ...!


What am I gonna do?
Not Quite!
Internet
I am 11.5.1.69
No Sir! You are not 11.5.1.69
I am 11.5.1.69
Internet! Here I come
11.5.0.0
Private Network
(Unregistered)
11.5.1.0
11.5.6.0
11.5.2.0
11.5.3.0
11.5.4.0
11.5.5.0

Not Quite!

- Here is the problem that might occur once we go out on the internet.
- Since we are using an address range that is owned and registered by someone else we are not able to operate with the current IP setup we have.
- Does this mean that we have to redesign our network and start from the point when we started to build our company's intranet?
- That effort had tremendous work involved.
- Is there no other way of going to the internet except to redesign our network and rework everything that has proven its creditability over several years?


Woopie!
Solution
I am
11.5.1.69
Internet
I am
11.5.1.69
NAT
We are
172.100.200.5
Internet
connection
through NAT
AS/400
11.5.0.0
Private Network
(Unregistered)
11.5.1.0
11.5.6.0
11.5.2.0
11.5.3.0
11.5.4.0
11.5.5.0

Solution

- **NAT (Network Address Translation)**
  - **Helps alleviate IP exhaustion**
  - **Allows private unregistered network to be represented in the Internet**
- **How?**
  - **By using a small set of valid (registered, globally routable) addresses**
  - **Function resides on the IP routing device providing the connection between the two networks**
  - **Shields the internal addresses from the world outside (enhances security)**
  - **Host providing NAT is an IP forwarding device connected to at least two different IP networks**

Solution

In V4r3 we introduced the concept of NAT (Network Address Translation).

This support will be provided as a part of the base operating system and can be considered as part of basic firewall functionality.

This means that we will have a native IP translator for Internet support and added security on the Internet. NAT will help the IP exhaustion problem. IP filtering will provide us the added security we need to shield our system from the outside world.

Network Address translation addresses the problem of IP depletion. NAT allows a private unregistered network to be represented by a small set of valid registered addresses. This function resides on the IP routing device providing the connection between the two networks, a boundary system.

In addition to the IP depletion problem, NAT can also be used to provide a certain level of network security.

- When connecting to another network, it is highly advisable to isolate the topology of the internal private network.
  - ***For example, the addressing (IP addresses, subnets and host names) of internal machines should not be known to the outside world .***
- NAT is able to hide the internal network topology by representing the internal hosts behind a small subset of publicly known addresses.

Network Address Translation is a mechanism which can be used to allow a private network which is not currently using registered address to connect to and communicate with a public, registered network.

Types of NAT

- **Masquerade NAT**
  - Provides a many-to-one mapping of IP addresses
  - Allows the private network to hide behind and be represented by one IP address assigned by an ISP
  - Each outbound request uses a different port assigned dynamically
  - Traffic must be initiated from the 'inside'.
- **Static NAT**
  - One-to-one mapping between private and public addresses
  - Traffic can be intiated in either direction
- **Port-mapped NAT**
  - One-to-one mapping of IP:port to IP:port
  - Traffic can be initiated in either direction

Types of Network Address Translation

Masquerade NAT

- Masquerading is used to allow the private network to hide behind and be represented by the address bound to the public interface of the NAT machine. In most situations, this will be the address that has been assigned by an ISP which may be dynamic in the case of a PPP connection. This type of translation can only be used for connections originating within the private network destined for the outside public network. Each connection out, is maintained by using a different source (client) IP port number. Provides a many-to-one mapping.

Static NAT

- Static NAT is a simple one-to-one mapping between private and public addresses. This is required to support inbound connections from the public network into the private network. For each local address defined, there must be an associated globally unique address.

Port-mapped NAT

- Port mapping might be used to allow multiple occurances of a HTTP server to execute on a AS/400 by mapping <internal IP>:5001 to <external IP>:80.
- This NAT rule would be placed on you external interface. The internalface would have no NAT rule.
- Then, configure one WEB server to use port 80 for internal clients, and the other WEB server to use port 5001, for the external clients.

Masquerading functions

- **Supports TCP and UDP, FTP**
- **Swaps actual**
  - **ports with Logical Port Numbers (LPN)**
  - **IP addresses with the public interface IP address**
- **A pool of ports for the same physical interface**
- **Port numbers for Masquerading:**
  - **55335 - 65335 (for TCP)**
  - **60001 - 65335 (for UDP)**
- **Re-computes checksums for TCP and UP headers**
- **Maintains tables of outgoing and incoming traffic**
  - **Cleans up inactive table entries**
- **Provides a primitive native firewall**
  - **Connection initiated by secure side Hosts only**
  - **Hosts cannot broadcast their addresses**

Masquerading functions

IP Masquerading is a method by which hosts which do not have InterNIC (Internet Network Information Center) registered IP addresses may communicate with the Internet through a router which does have an InterNIC registered IP address.

- The term "secure side host" is used to refer to all machines on an internal network regardless of the method of attachment (LAN, WAN, Ethernet etc.) and regardless of the distance of the connection.
- The term "external machines" is used to refer to machines located out on the Internet.

Masquerade will support TCP, ICMP and UDP protocols.

To the Internet, all of the secure side hosts appear to be contained within the AS/400; that is, there is only one IP address associated with both the AS/400 and these hosts.

- Each secure side host must be set up so that the AS/400 is its gateway, and also its default destination.
- The correspondence between a particular communication connection (port) and a host is set up when one of the hosts sends a packet to the AS/400 to be routed to the Internet.
- The masquerade NAT function saves the port number in a table of active connections so that when it receives responses to the host's packet over that connection, it can send the response to the correct host.
- When the router receives a packet intended for a host, it searches the table of active connections to determine what address on the internal ring should receive the packet and sends it there.

A record of active port connections and the last access time by either end of the connection is created/maintained by masquerade NAT. These records are periodically purged of all connections idle for a predetermined amount of time based upon the assumption that an idle link is no longer in use.

Masquerading functions

It should be noted that all communication between the secure side hosts and the Internet must be initiated by the secure side hosts. This is an enhancement to security. The Internet knows nothing of the existence of the hosts, and they cannot broadcast their addresses to the Internet.

Masquerading functions

Outbound traffic - secure side to external Internet

- Outbound masquerade processing assumes all IP packets it receives are bound for external IP addresses and so does not check to determine if a packet should be routed locally.
- Conflicting IP addresses must have static routes on the originating host to ensure only those bound for the Internet are routed to the masquerading boundary host.
- For outbound datagrams, the source port number is the port number of the originating host.
- At the transport layer, NAT searches the table of in-use Logical Port Numbers (LPN) entries looking for a source IP address and source port match. If found, the corresponding LPN is substituted for the source port. If no active matching LPN entry is found, a new one is created, a new LPN selected and substituted for the source port.
- NAT will save this combination of numbers in the In-Use table and replaces the port number in the transport header with the LPN.
- The source IP address is swapped with the Masquerading IP address in the IP datagram header and the header checksum value is recalculated.
- The packet is then processed as usual by IP, and will get sent to the correct external host.

The port numbers that will be used (v4r3 only) are in the range of:

- 55335 - 65335 TCP
- 60001 - 65335 UDP
  - ***This will affect the applications already using these port numbers.***
  - ***This was changed in v4r4; ports are obtained dynamically***

Masquerading functions

Inbound Masquerade processing (response & other)

- Response messages returning from the Internet bound for secure side hosts will have a Masquerade assigned Logical Port Number (LPN) as the destination port number in the transport layer header.

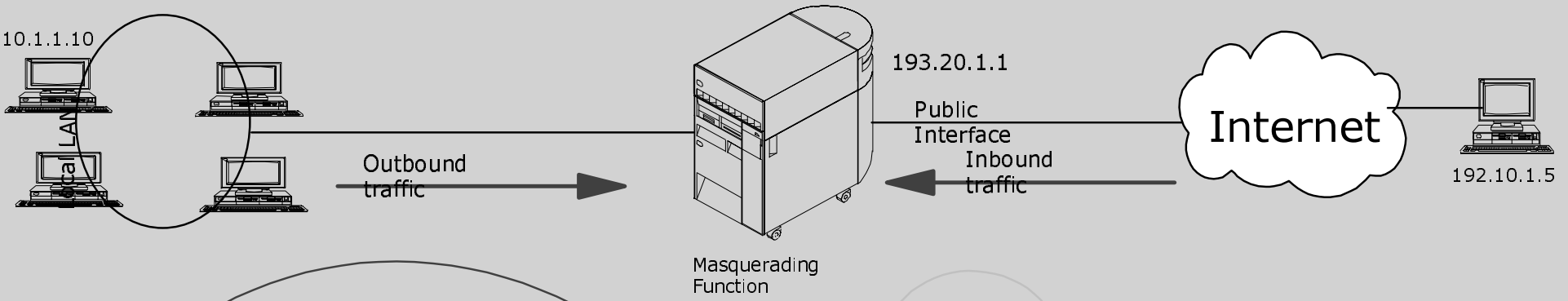
The Masquerade NAT inbound processing steps are;

- Masquerade will search the table of In-Use LPNs to see if this destination port matches an In-Use LPN port..
  - ***If not found, then the packet is assumed to be a unsolicited packet, and the packet is 'returned' to the caller unchanged. It will then be handled as a normal unknown destination.***
- If a matching LPN is found, a further check is made to determine that source IP address matches the destination IP address of the existing LPN table entry.
  - ***If it is OK, the original local machine's port number will replace the source port in the IP header.***
  - ***If this check fails, return the packet unchanged.***
- The source port listed in the table is placed in the packet transport layer header as the new destination port.
- The secure side host IP address from the table is placed in the packet header as the destination IP address
- The packet is then processed as usual and is routed to the secure side host.

Since Masquerade requires an LPN entry to determine the correct destination port and IP address, Masquerade is incapable of handling unsolicited datagrams from the Internet.

Masquerading NAT example

- Mapping table swap IP address and port numbers, hiding local LAN
- Translation is done for outgoing packets
- Incoming packets are translated back and redirected to original source



Dynamic Mapping

Source Address	Destination. Address.	LP	DP
10.1.1.10	192.10.1.5	1024	23

10.1.1.10	193.20.1.1
1024	55336

Source Address	Destination. Address.	LP	DP
193.20.1.1	192.10.1.5	55336	23

Source Address	Destination. Address.	LP	DP
192.10.1.5	10.1.1.10	23	1024

Source Address	Destination. Address.	LP	DP
192.10.1.5	193.20.1.1	23	55336

Masquerading NAT example

Telnet Client 10.1.1.10 wants to talk to a Server on the Internet at 192.10.1.5.

- The local host is trying to connect to the remote host through local port **1024** and remote port **23**.

The Masquerading gateway secure side address is "10.1.1.1"

The client routes the outbound packet to it's default route "10.1.1.1"

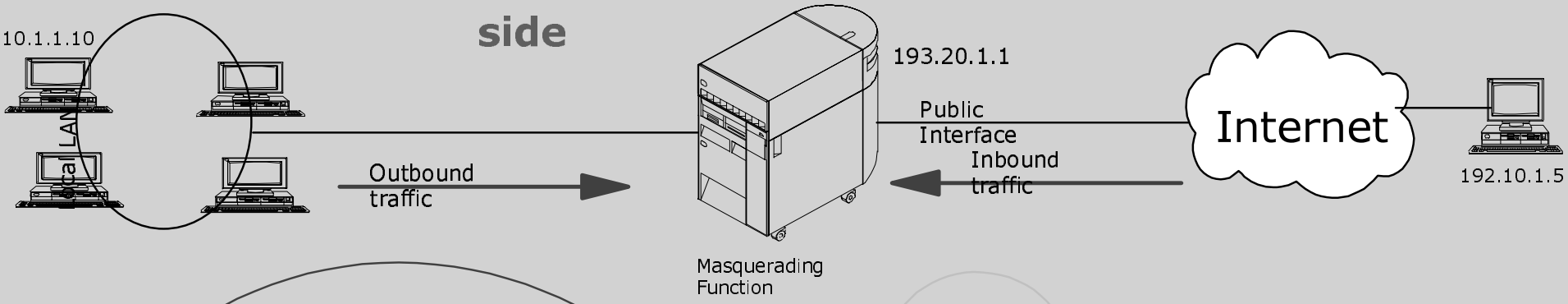
NAT does the following:

- Swaps the local port number with a random number from the available Logical Port Numbers
  - ***LPN assigned 55336***
- Records an entry in the dynamic mapping table
- Swaps the local IP address **10.1.1.10** with the masquerading IP address of **190.20.1.1**
- The packet is routed to the remote host with these changes
- The remote host sees a packet from **190.20.1.1** on port **55336** and opens port **23** for telnet.
- The return packets for **190.20.1.1** on port **55336** will be translated by NAT back to **10.1.1.10** on port **1024** and routed to the original telnet client.

Both the Telnet Server and Client are unaware masquerading is occurring

Static NAT example

- Provides one to one mapping
- Requires a registered IP address for each
- Port independent, remain unchanged
- Session can be initiated from either side



Source Address	Destination. Address.
10.1.1.10	192.10.1.5

Static Mapping

10.1.1.10	193.20.1.1
10.1.1.20	193.20.1.2
10.1.1.30	193.20.1.3

Source Address	Destination. Address.
193.20.1.1	192.10.1.5

Source Address	Destination. Address.
192.10.1.5	10.1.1.10

Source Address	Destination. Address.
192.10.1.5	193.20.1.1

Static NAT example

Each secure side IP address which is to be translated must be configured to an assigned Internet registered IP address.

This is a one-to-one mapping which remains static until reconfigured manually.

Only those IP addresses in the table will be routed through the Static NAT boundary host.

The internal LAN IP addresses are hidden behind the registered IP addresses.

- but

Since it is a static entry, the Internet hosts can learn the registered IP address of a specific secure side host and initiate conversations.

Which physical interface?

NAT rules are associated with a physical interface (e.g. PPP1, TRNLINE, ETH02, etc.)

For masquerade NAT rules (which use 'hide' statement) ...

- `HIDE <subnet a.b.c.*> BEHIND 203.14.57.198`
- physical interface is determined by the 203.14.57.198 address

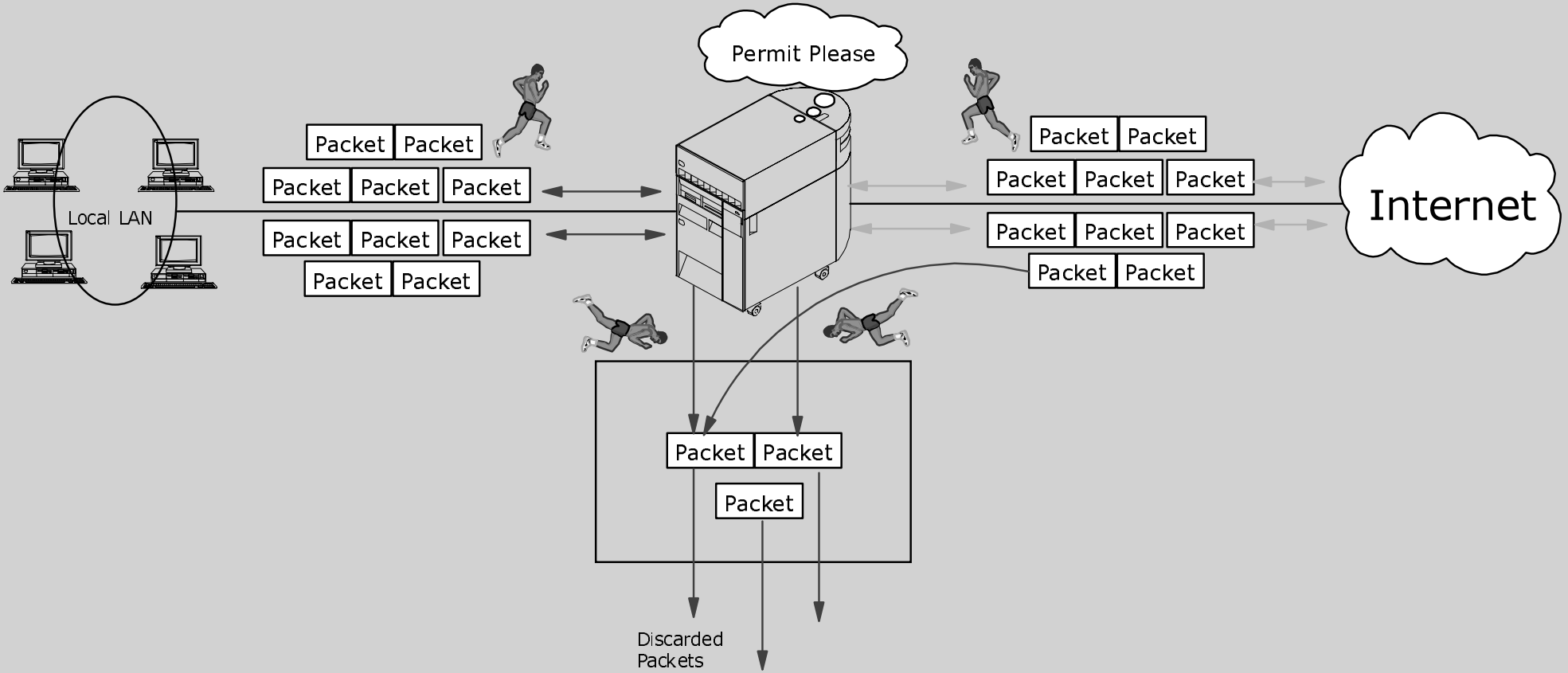
For static NAT rules (which use the 'map' statement) ...

- `MAP <internal IP addr> TO <external IP addr> LINE=ETH1`
- physical interface is ETH1

IP Filtering

IP Filtering

- Selectively lets some IP packets to go out and blocks others
- Works through predefined filter rules
- Actions are associated with each filter rule



IP Filtering

All the outbound and inbound IP packets have to pass through a set of rules.

Whenever an outbound connection is requested, the packet is compared against a set of predefined rules.

- If a condition is met and it has permission to go out, it will be allowed to go out onto the Internet, otherwise the packet will be discarded.
- This mechanism is applied for inbound traffic as well.

This provides a certain level of security from Internet traffic.

IP filtering can also be used in intranets to secure specific subnets from unauthorized access internally.

IP filtering, RIPv2 and NAT work together to provide entry level firewall function.

IP filter rules (like NAT rules) are associated with a particular physical interface (e.g. TRNLINE or PPP1)

IP Filtering Rules

- **Criteria**
  - source IP address
  - destination IP address
  - protocol (TCP, UDP, ICMP, FTP, etc.)
  - source Port
  - destination Port
  - direction (inbound, outbound or both)
  - fragments
- **Actions**
  - permit
  - deny
  - IPsec (for VPN)
- **Scope**
  - specific
  - universal

IP Filtering Rules

The availability of dynamic routing protocols and NAT will allow the AS/400 to easily connect two or more disparate networks . These functions alone, however, don't provide adequate security, even for low end, entry level connections. IP filtering is the core protection mechanism behind security. The combination properly configured Routing, NAT and IP filtering can be considered entry level network firewall.

Packet filters are set rules that limit IP packet flow into or out of a network. We define policies that determine which packets are allowed access into or out of the network. If there is no matching rule, the default rules are used to deny access and discard the packets. We can filter packets based on the following criteria:

- We can limit a specific source address for the outbound traffic to be restricted to the local network only or we can scan for a restricted destination address. We can also restrict traffic for certain applications using a particular protocol e.g. TELNET using TCP protocol. We can restrict access to specific port numbers and all these rules apply for both inbound and outbound traffic.
- We can set up filtering rules for our physical interfaces as well, that will ensure a high level of security. There are two actions associated with the filtering rules. Either you allow/permit someone to enter your system or you deny the access.

The scope of the rules can be specific or it can be universal. You define specific rules for everything that you are aware of and want to prevent. Whenever an IP packet comes in you check the contents of the IP packet against the rules that you set up for packets filtering. Normally packets have predictable behavior and you have taken care of it. A rule table is maintained by the system which has all the entries that you define for your system. This table is scanned for all the packets coming in or going out. Whenever a rule is matched it is applied. If after scanning all the rules, there is no exact match a default rule exists which matchs any packet. This rule denies the packet and this action cannot be changed.

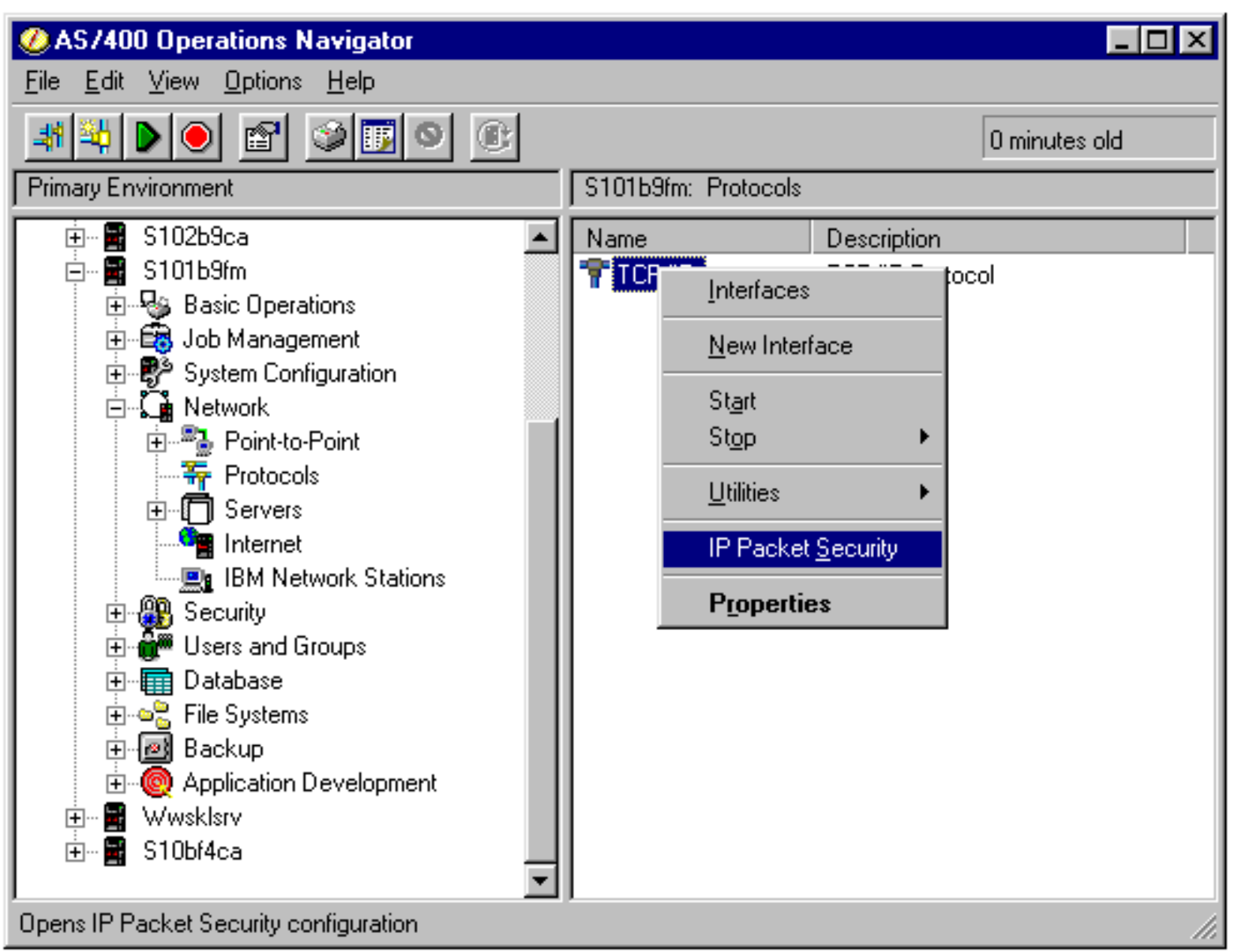
Configuration

Configuration

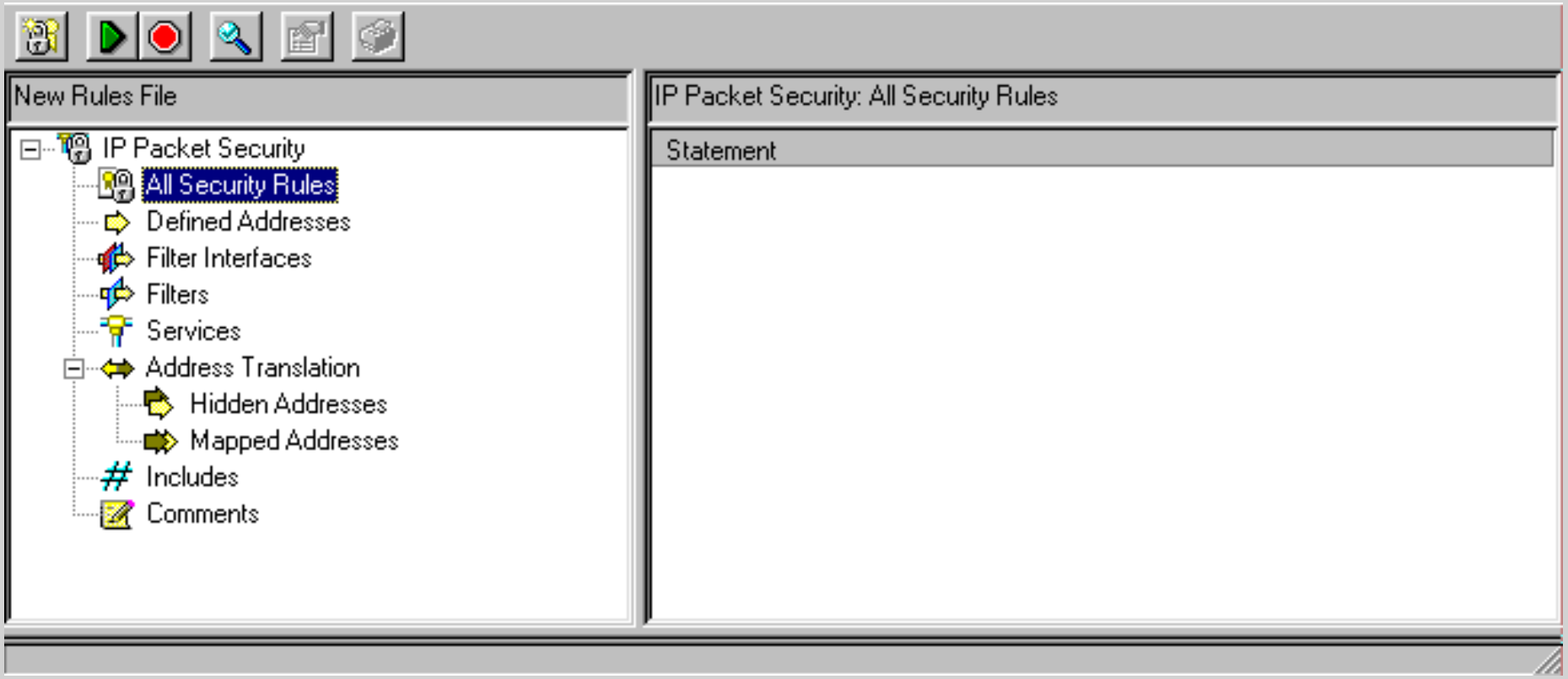
Select
Network
Protocols
TCP/IP

Right Click
TCP/IP

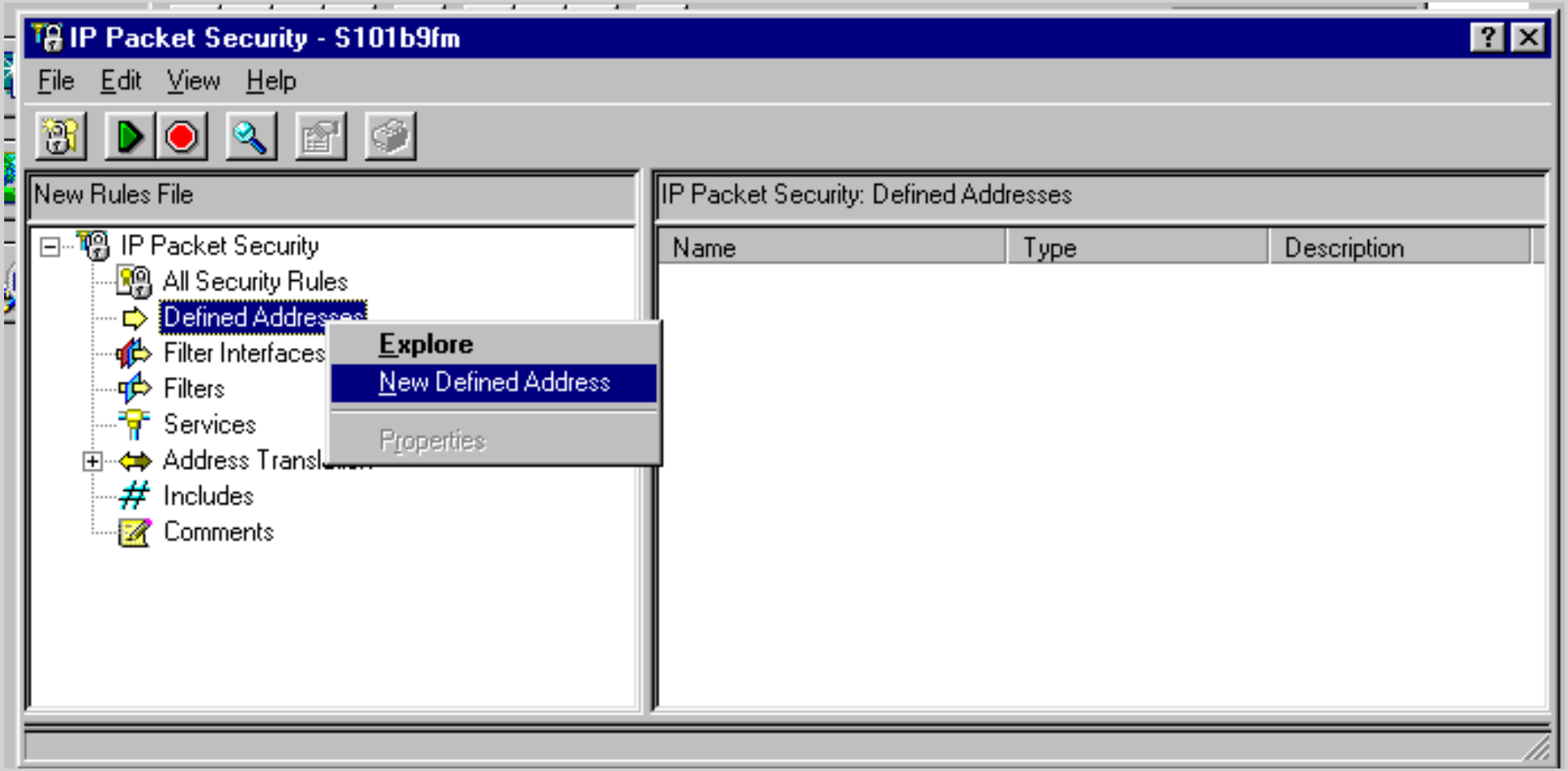
Select
IP Packet
Security



Main configuration screen



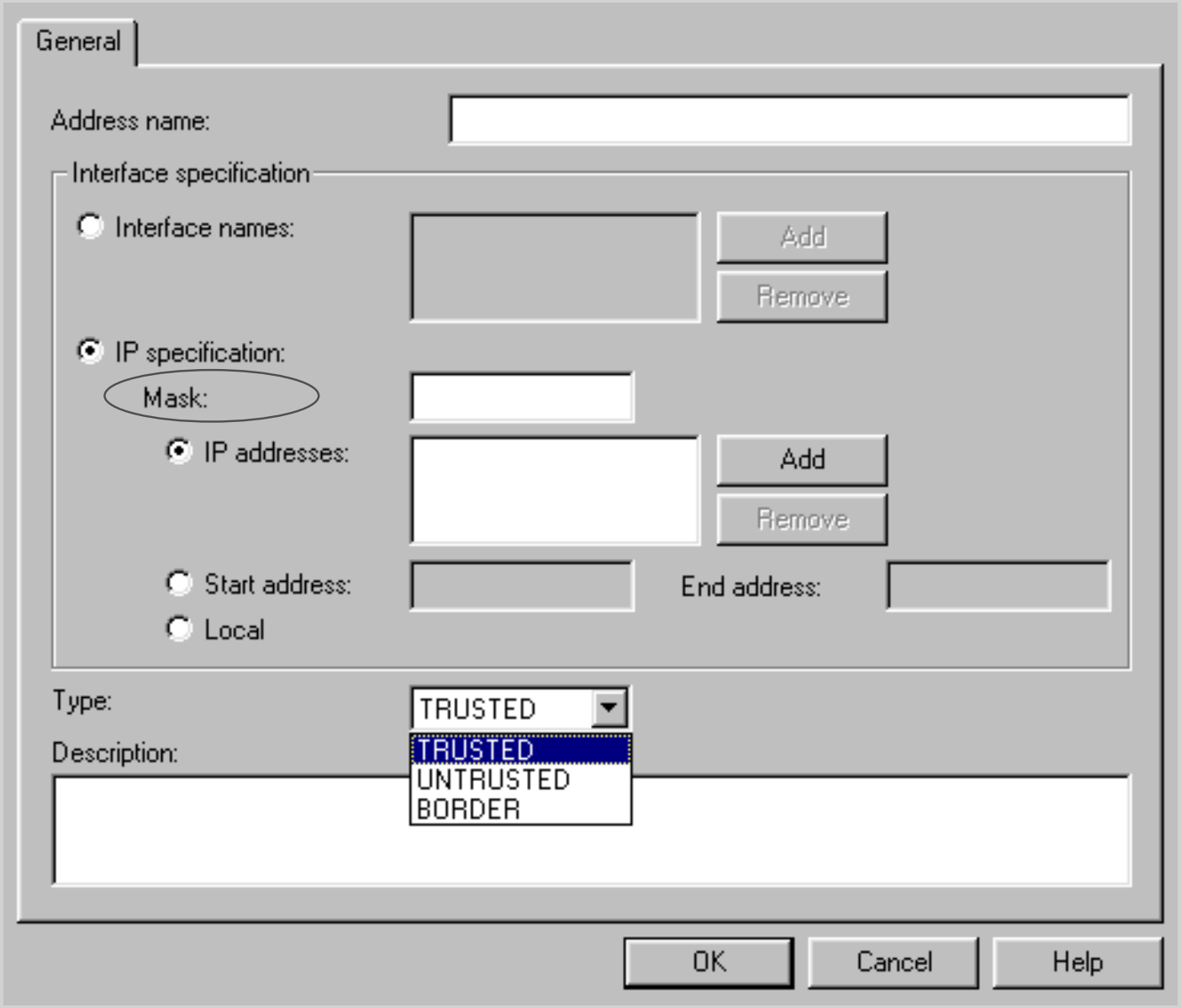
NAT Masquerade - Step 1



Add New Defined Addresses

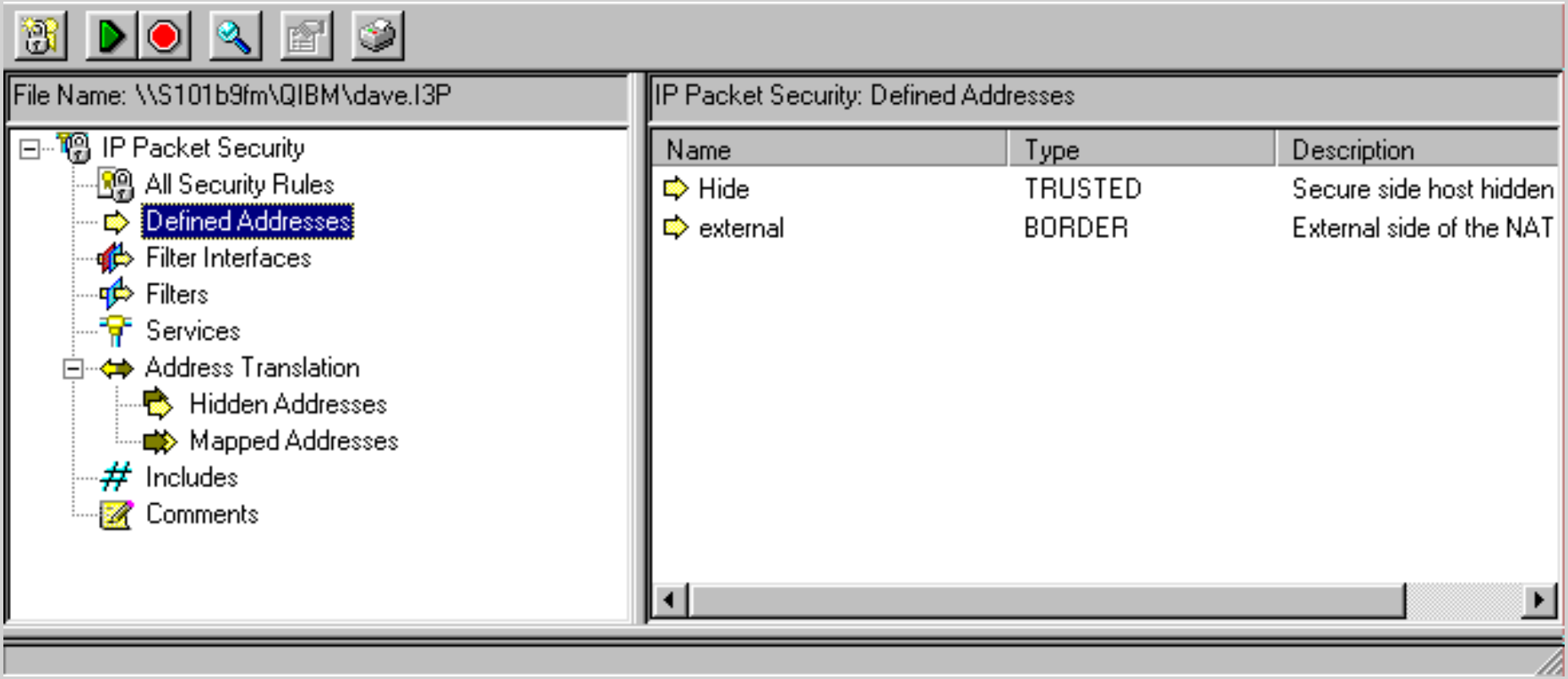
1. Ensure the rules are deactivated
2. Define each secure side IP address as TRUSTED
3. Define the external registered IP address as a BOUNDARY

Define Address window



Arbitrary Address name input here will be used in Step 2

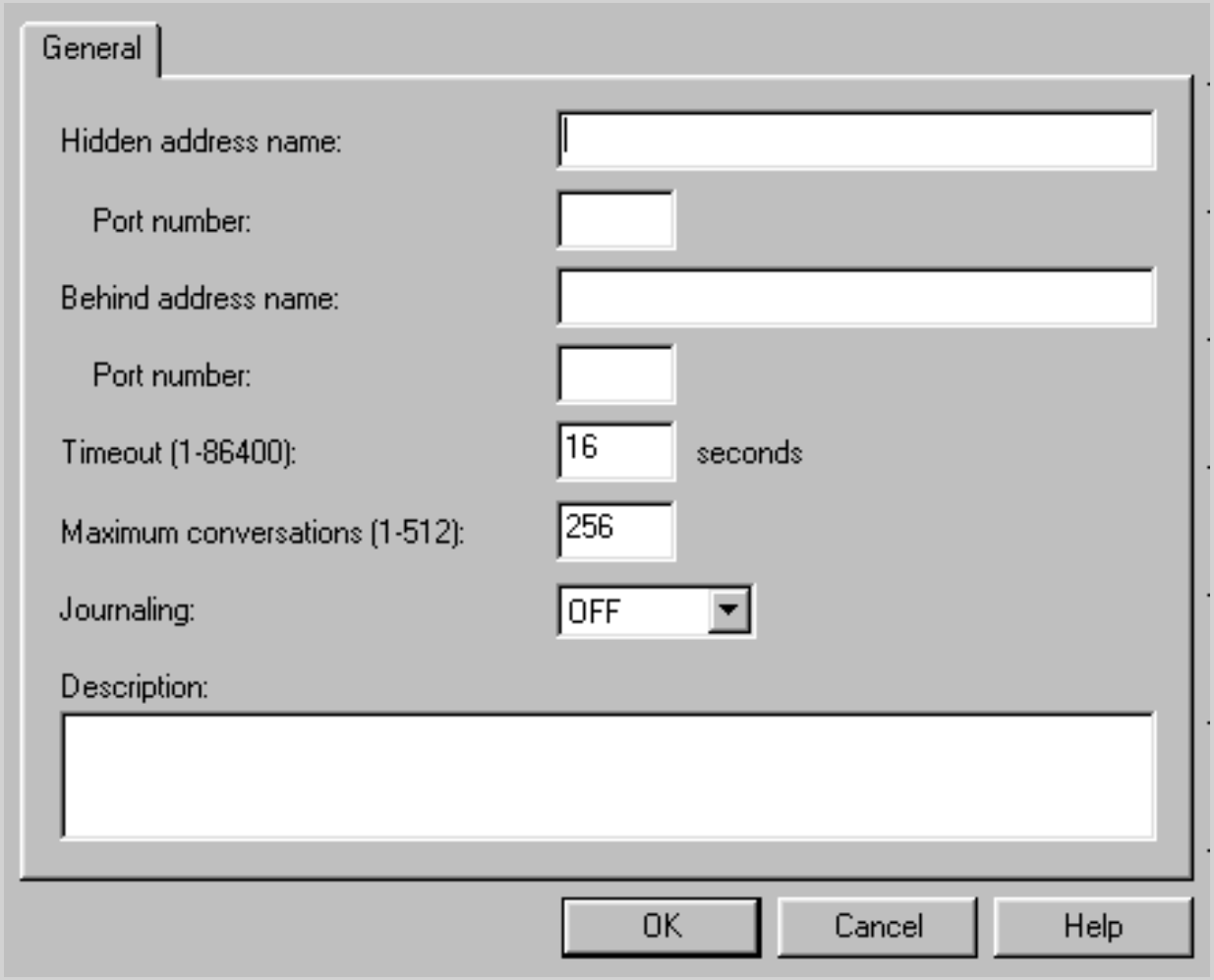
Nat Masquerade - Step 2



Tie the trusted address to the border address under Hidden

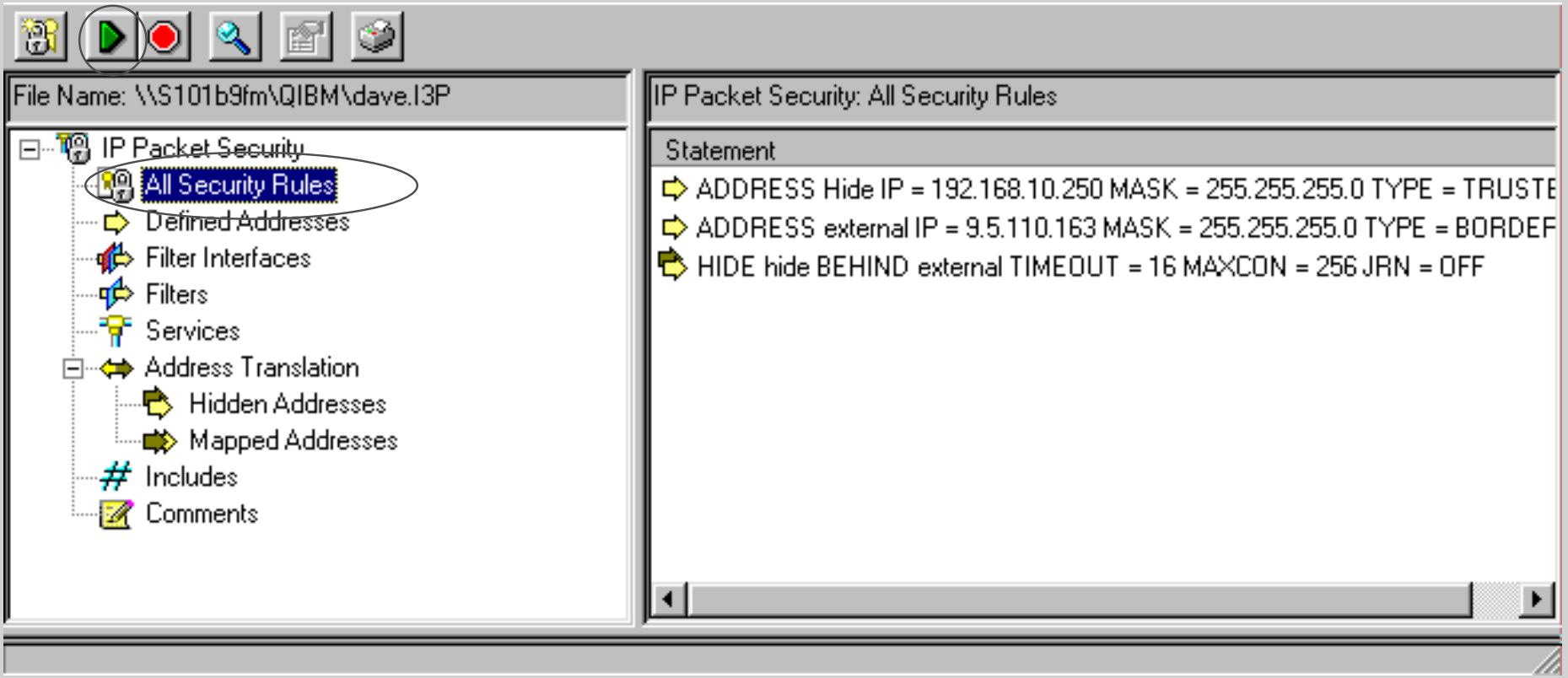
1. Select Address Translation Hidden address
2. Right click Hidden address, select New Hidden address

Hidden Address window



Use the names from Step 1 to tie the Hidden address to the Border address

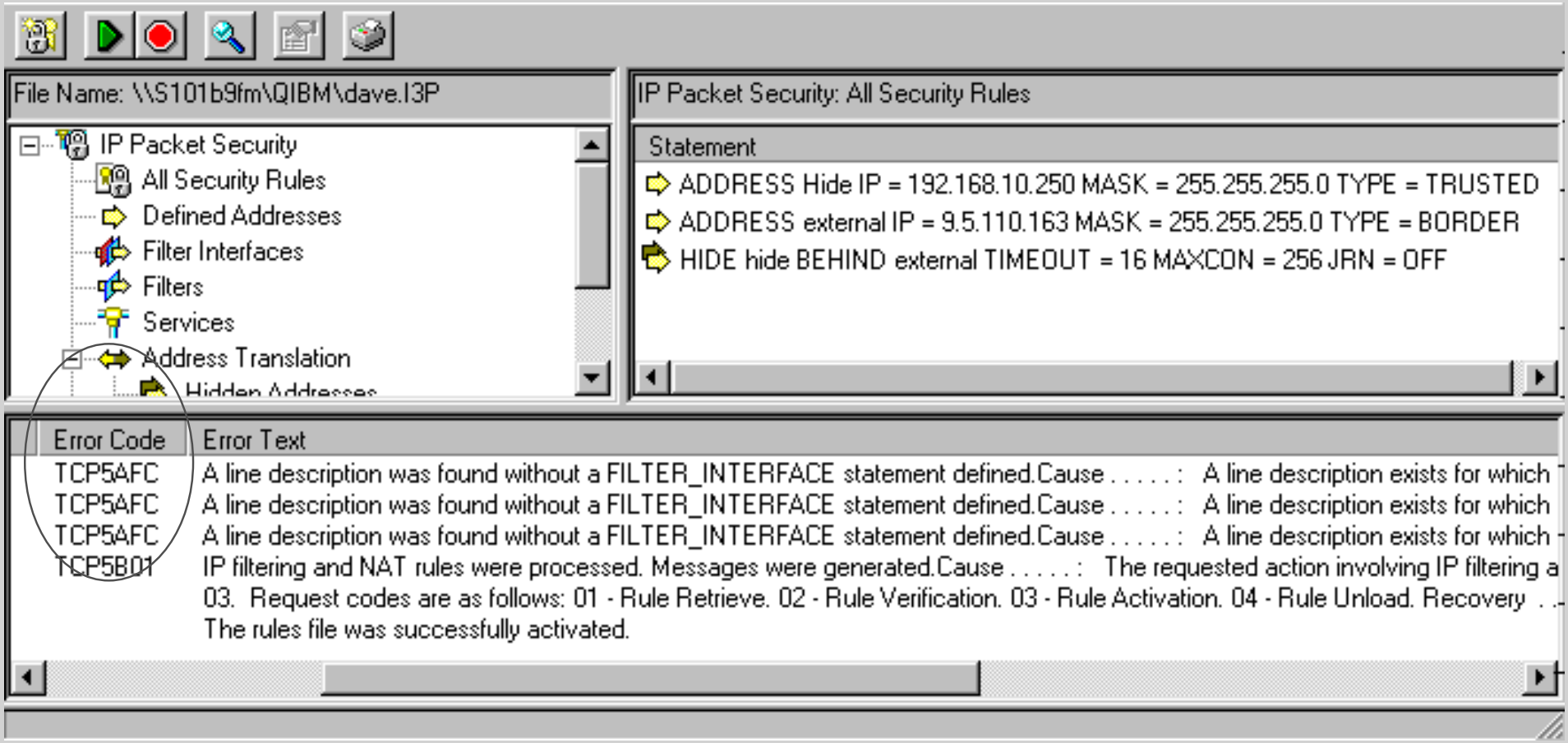
NAT Masquerade - Step 3



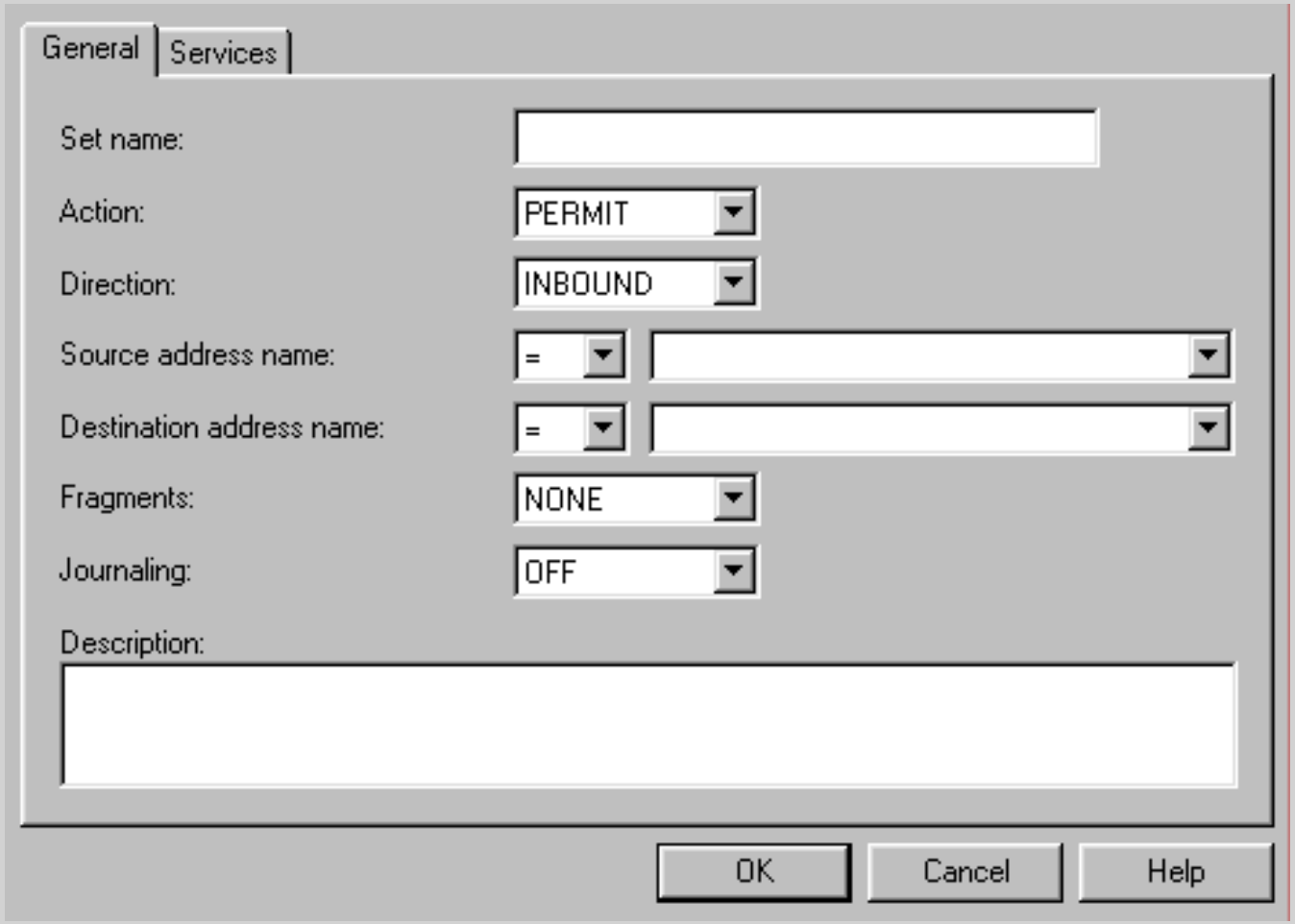
Use the All Security Rules function to see all the work done

1. Push the green arrow to activate the rules
2. You will be given a chance to save the rules to a file. This is a standard Windows file save dialogue. You can save the file under any name in any IFS directory

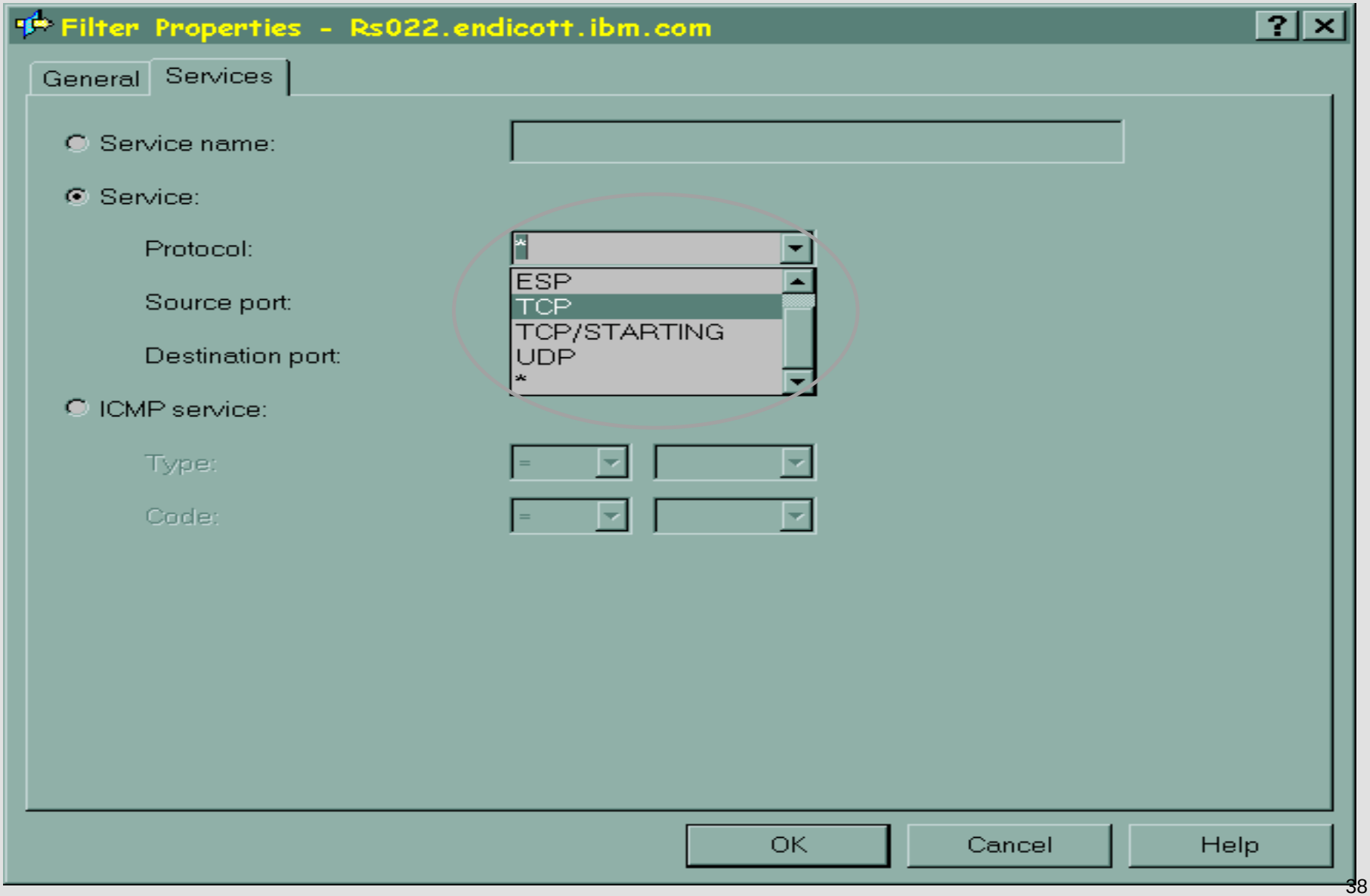
Message window



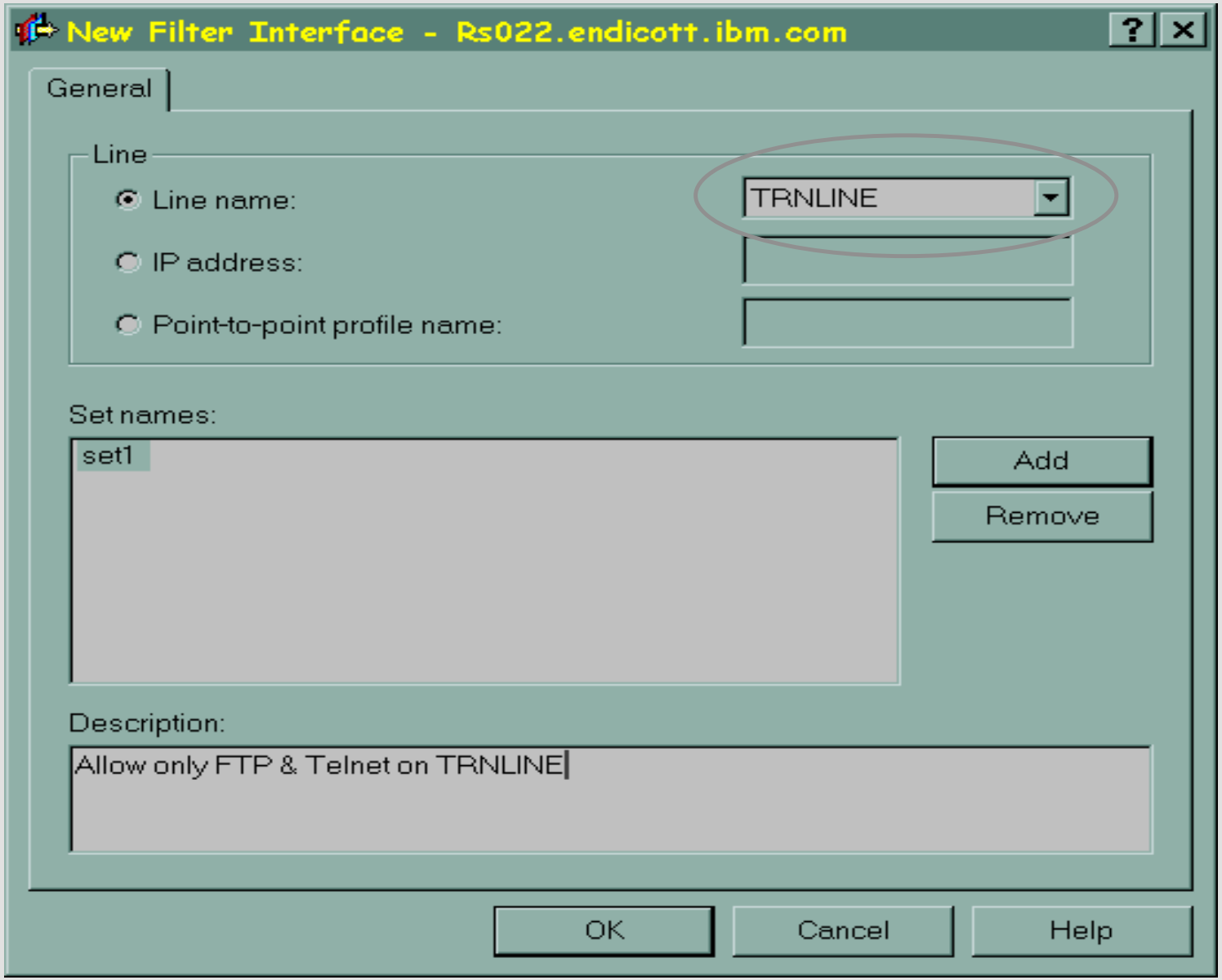
New Filter rule window



Service tab for filters



Associating filters with an interface



Things to consider when writing filter rules

A 'deny all' rule is always, automatically, the last rule (on any physical interface that has 1 or more filters).

So, generally, you only have to write 'permit' rules for the traffic you want to occur.

Group filters by protocols; FTP, Telnet, SMTP, etc.

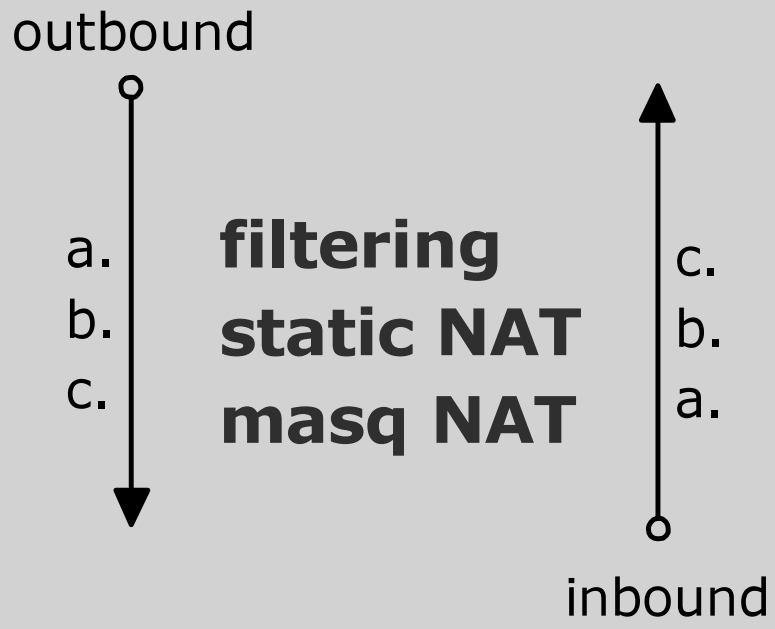
Include statements are supported; allows simple reuse of common rules across different interfaces or systems.

When testing new rules, don't forget RMVTCPTBL *ALL CL command.

Activated Rules

- **When the rules are activated, they are loaded as part of the IP protocol stack implementation in SLIC**
- **Activated rules persist across TCP/IP stop or start, interface state changes, and across IPLs**
- **When rules are activated, they completely replace all previously loaded rules on all physical interfaces**
- **The only AS/400 job associated with these functions is when journaling is selected**

Relationship between filter & NAT rules



Key points: - write filter rules for 'internal' traffic
- NAT rules are automatically mutually exclusive

Summary

- **Network Address Translation provides:**
  - **Public Internet access for existing private networks**
  - **Minimize the number of registered IP addresses required**
  - **Private network isolation from public networks**
- **IP Filtering provides:**
  - **Packet level security**
  - **Wide range of packet selection criteria**
  - **Rules for both inbound and outbound packets**

This publication may refer to products that are not currently available in your country.