IAC4000 - NAT Pool for VPN Packet

1. Introduction

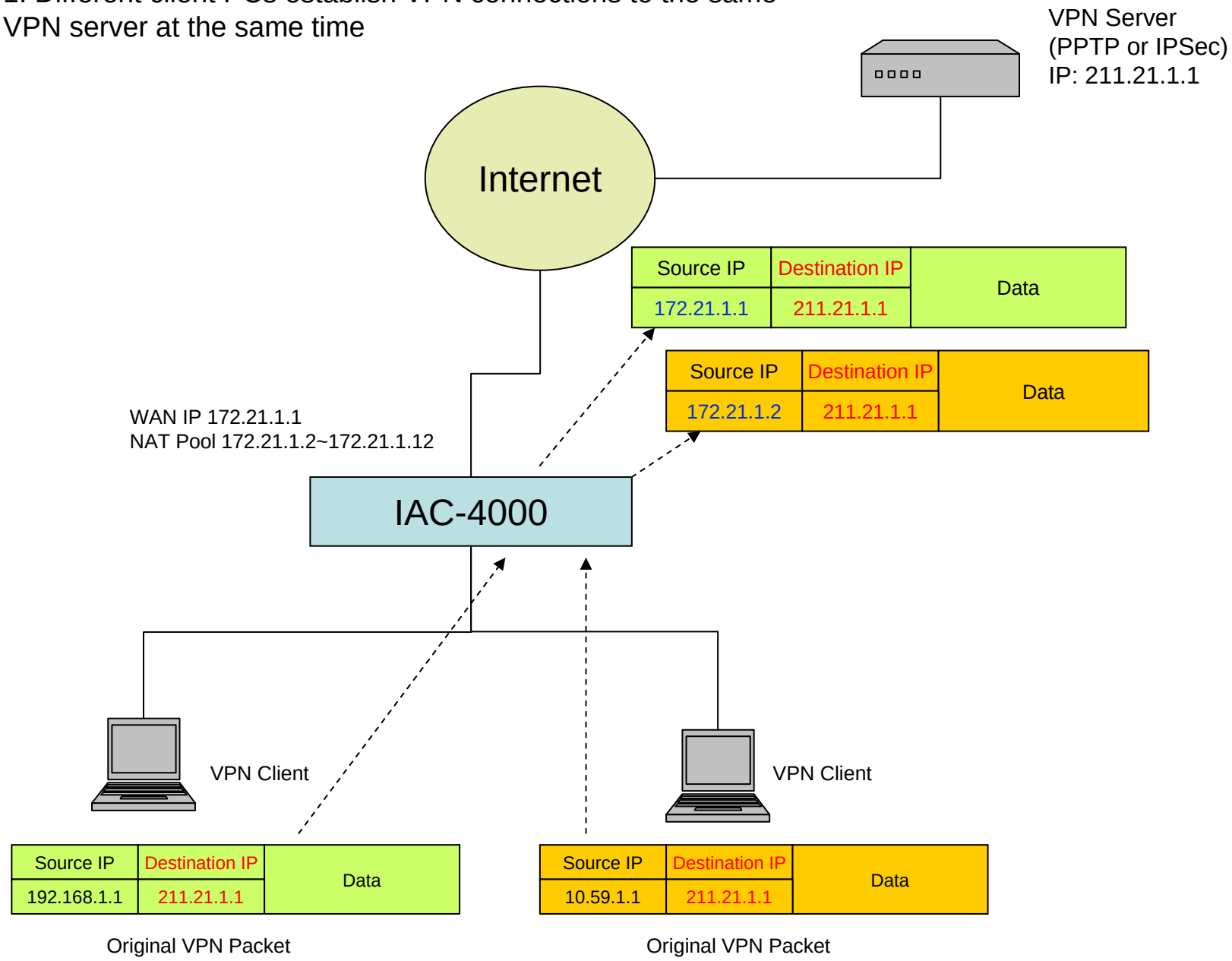
Some VPN servers have some limitations for clients. The server may only accept one client with the same source IP address. This means that if there are 2 client PCs behind a normal NAT router and they try to access the same VPN server at the same time, one of the clients may not succeed. The “NAT Pool for VPN packet” function is implemented to overcome this problem. When “NAT Pool for VPN packet” is enabled, the source IP of the PPTP and IPSec packets from client PCs will be translated to more than one global IP and forwarded to the VPN server.

2. Specification

a. With NAT, when the IAC4000 receives the VPN packets from LAN, it will replace the original source IP address with another global reserved IP address.
b. When the IAC4000 receives the VPN packets from WAN, it will check the mapping table to restore the original IP address. If it can’t find this in the table, the packet will be dropped.
c. Because this function may effect the performance of the IAC4000, the administrator can enable or disable this function. The default is disabled.
d. The administrator needs to enter the global IP pool: those IP addresses will be used on NAT automatically. The maximum number is 50.
e. This feature only supports IPSec and PPTP packets.
f. If the global addresses are exhausted, the IAC4000 will drop the packets automatically and will not give any information to this user.
g. If the destination IP addresses of some VPN packets are different, the IAC4000 uses the same global IP addresses on these packets whether the source IP addresses are different or not. Because the IAC4000 can distinguish each session by the destination IP address and the VPN server can accept this situation
h. If the destination IP addresses of some VPN packets are the same and the source IP addresses are different, the IAC4000 will only use different global IP addresses to replace the original source IP addresses.
i. The user can connect to one VPN server per session.
j. On the status page, we provide the mapping table for VPN packets. The administrator can view and analyze the information when some guests can’t connect to their VPN server.
k. The IAC4000 uses the N-1 mapping policy to process the packets as normal except VPN (IPSEC & PPTP) packets.
l. About IPSEC, the IAC4000 only supports tunnel mode, not the AH protocol.

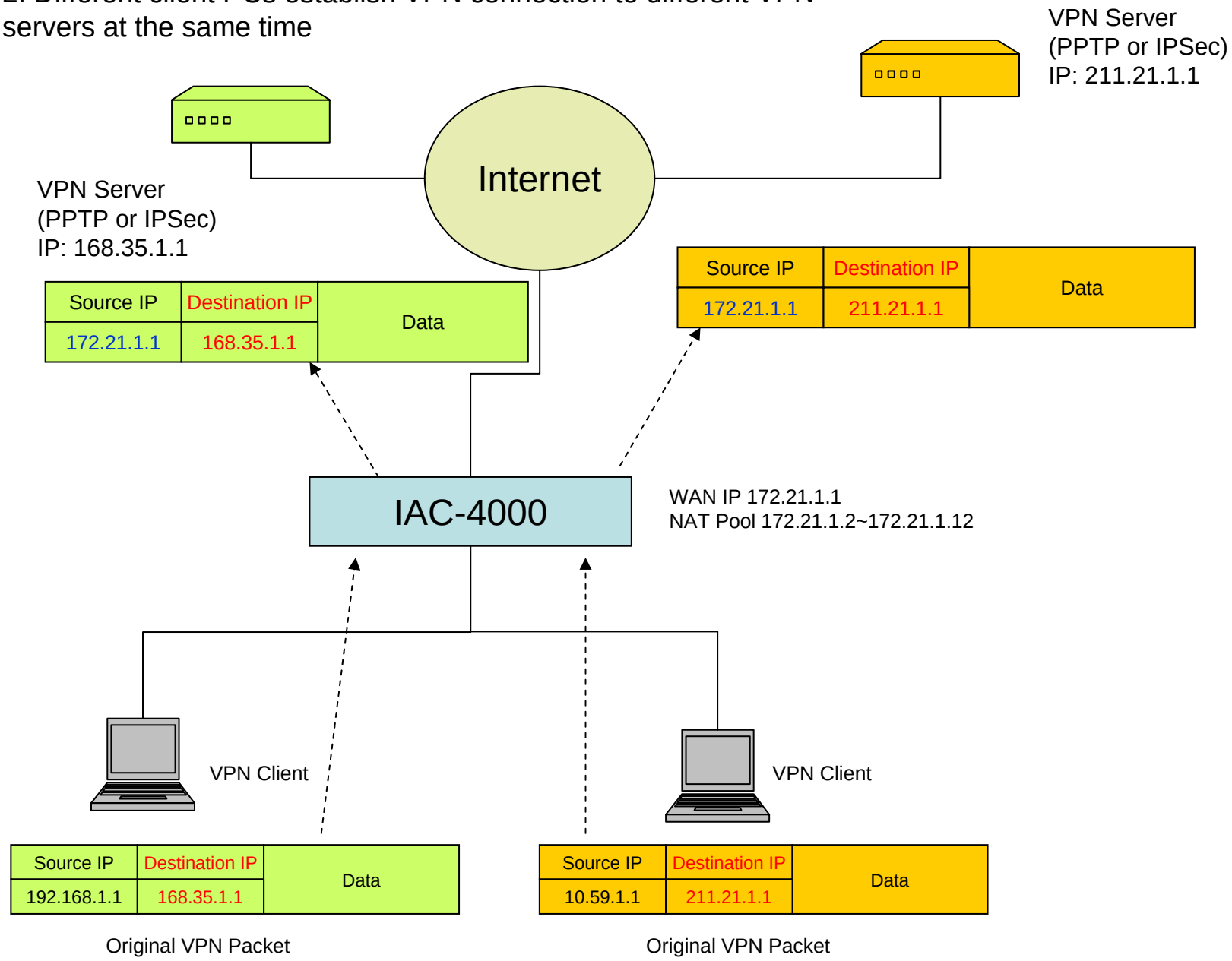
NAT Pool for VPN Packet

1. Different client PCs establish VPN connections to the same VPN server at the same time



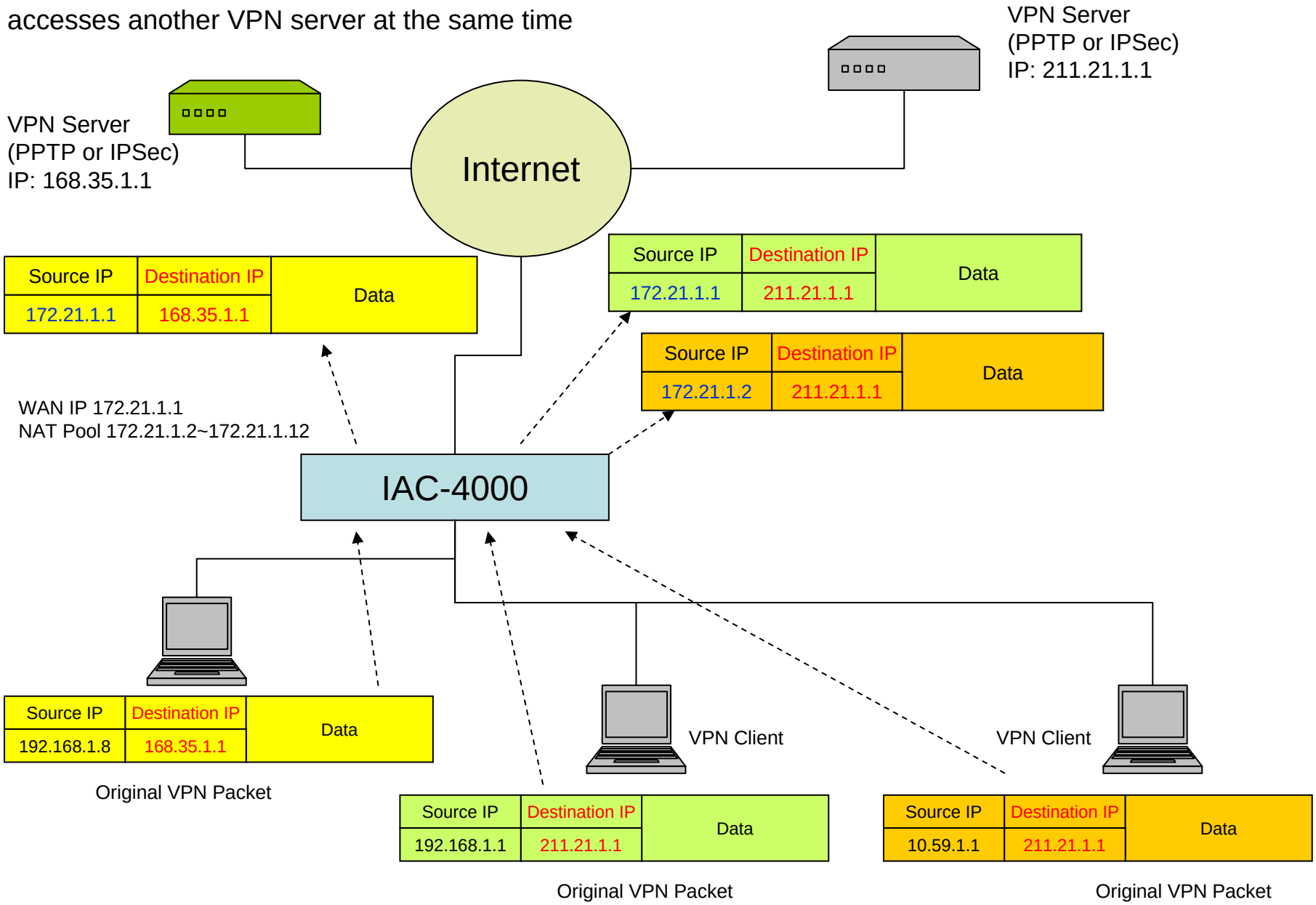
NAT Pool for VPN Packet

2. Different client PCs establish VPN connection to different VPN servers at the same time



NAT Pool for VPN Packet

3. Three different client PCs establish VPN connection. Two client PCs access the same VPN server and one client PC accesses another VPN server at the same time



NAT Pool for VPN Packet

NAT Pool

- (•) Disable
- ( ) Enable

Start IP: [ ] End IP: [ ] (Max. 50 IPs) [Add to List]

No.	Address List	Delete
01	210.66.37.242	☐
02	210.66.37.243 ~ 210.66.37.250	☐
03	211.12.1.1~211.12.1.10	☐

Idle Time : [5] Min.(1~60) [Delete]

NAT Pool for VPN Packet

NAT Pool Table

NAT Pool information. Source IP address, Source MAC address and Translated IP address

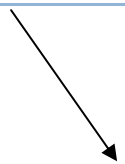
No.	Source IP Address	Source MAC Address	Translated IP Address	VPN Type
1	192.168.100.1	OE-90-80-90-EE-12	211.21.185.240	PPTP
2	192.168.100.2	OE-90-80-90-EE-13	211.21.185.241	PPTP
3	192.168.100.3	OE-90-80-90-EE-14	211.21.185.242	PPTP
4	192.168.100.4	OE-90-80-90-EE-15	211.21.185.243	IPSec
5	192.168.100.5	OE-90-80-90-EE-16	211.21.185.244	IPSec
6	192.168.100.6	OE-90-80-90-EE-17	211.21.185.245	IPSec
7	192.168.100.7	OE-90-80-90-EE-18	211.21.185.246	IPSec
8	192.168.100.8	OE-90-80-90-EE-19	211.21.185.247	IPSec
9	192.168.100.9	OE-90-80-90-EE-20	211.21.185.248	PPTP
10	192.168.100.10	OE-90-80-90-EE-21	211.21.185.249	IPSec

New page

NAT Pool for VPN Packet

Alert

Syslog	Syslog Name	Description	Interval Time	Type
☐	Administration access Fail	A log would be sent when someone failed to access the administration web server	When someone failed to access the system web server	161
☐	NAT Pool exhausted (IP / Port)	A log would be sent when IP or Port mapping exhausted	When NAT Pool exhausted	161



Add NAT Pool exhausted log in Syslog

NAT Pool exhausted (IP/ Port)
A log will be sent when IP mapping for NAT Pool VPN connection is exhausted or NAT Port mapping is exhausted
Format:
(**Id**, Mac Address)(**NAT Pool exhausted**, type)
Type: IP / Port