Character and GUI forwarding approaches

David Morgan


```
iptables -t filter -A OUTPUT -o eth1 -p tcp --sport 23 --dport 1024:65535
 -s 192.168.4.0/24 -d 0.0.0.0/0 –j ACCEPT
```

- Table for this rule
- Rule action
  - -A add rule to chain/list
  - -D delete rule from chain/list
  - -P default policy for chain/list
- Rule chain/list (tables contain chains)
  - INPUT
  - OUTPUT
  - FORWARD
  - PREROUTING
  - POSTROUTING
- Packet qualifiers
  - By interface and direction
  - protocol
  - source port number(s)
  - destination port number(s)
  - source address (range)
  - destination address (range)
- Packet disposition
  - ACCEPT
  - DROP
  - REJECT
  - SNAT
  - DNAT

Functions of iptables command

- firewall –drops undesired packets
- masquerading (NAT) – changes source address of outgoing packets
- port forwarding – changes dest address of incoming packets

IP masquerading

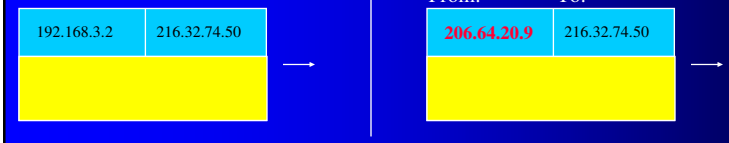
- Machines browse web w/o internet connection
- Gateway/translation service by linux machine
- Implemented as a function of firewalling

  iptables –t nat –A POSTROUTING –j SNAT –to <gateway addr>
- Clients designate linux machine as gateway
- Is a kernel component – must be compiled in

IP masquerading

iptables -t nat -A POSTROUTING
-o eth1 -s 192.168.3.0/24 -j SNAT --to 206.64.20.9

Outbound packet:



Reply:

IP masquerading

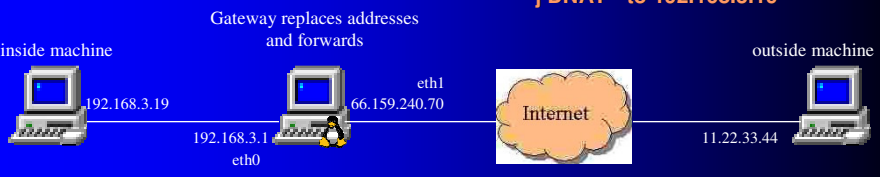
- Also known as
  - Network Address Translation (NAT)
  - Internet Connection Sharing (ICS)
- Gateway must have “forwarding” turned on
  - echo 1 > /proc/sys/net/ipv4/ip_forward

Three kinds of forwarding

- packet-rule “regular” forwarding (by iptables)
- ssh port forwarding (by ssh)
- ssh X11forwarding (by ssh)

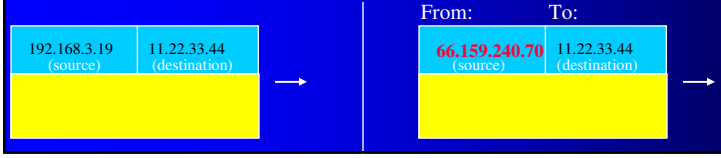
Packet-rule “regular” forwarding

iptables -t nat -A PREROUTING
-i eth1 -d 66.159.240.70/32 -p tcp --dport 5631
-j DNAT --to 192.168.3.19

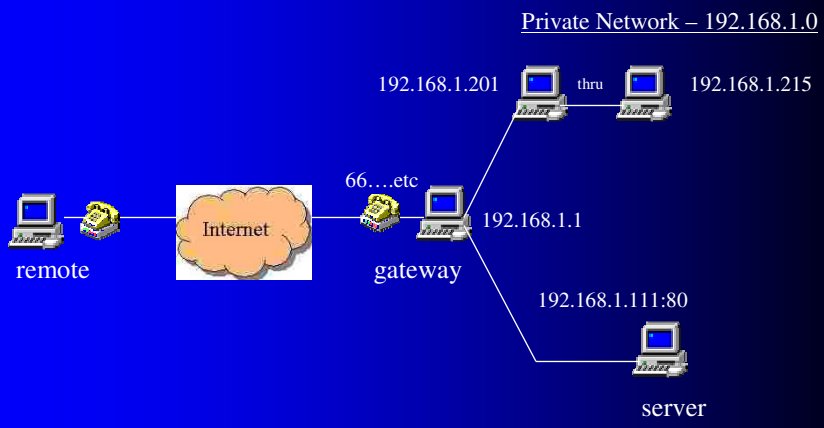


Inbound contact:

Outbound (masq’d) reply:



packet-rule port forwarding



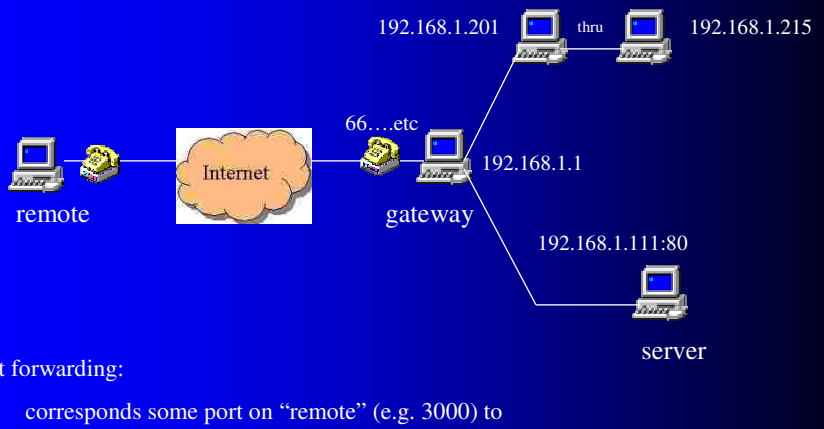
packet rule (firewall) forwarding:

corresponds some port on "gateway" (e.g. 12345) to
some port (e.g. 80) on a machine (eg, "server") reachable thru "gateway"

Example: http://66...:12345 in client's browser gets served from 192.168.1.111:80

ssh feature: port forwarding

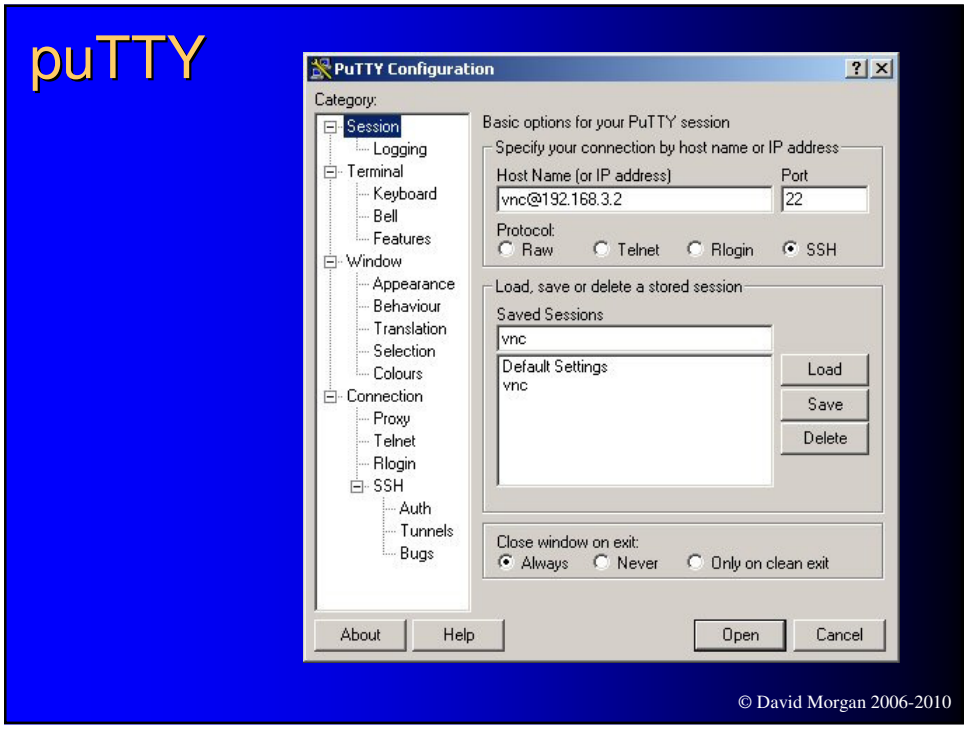
ssh -L 3000:192.168.1.111:80 66....

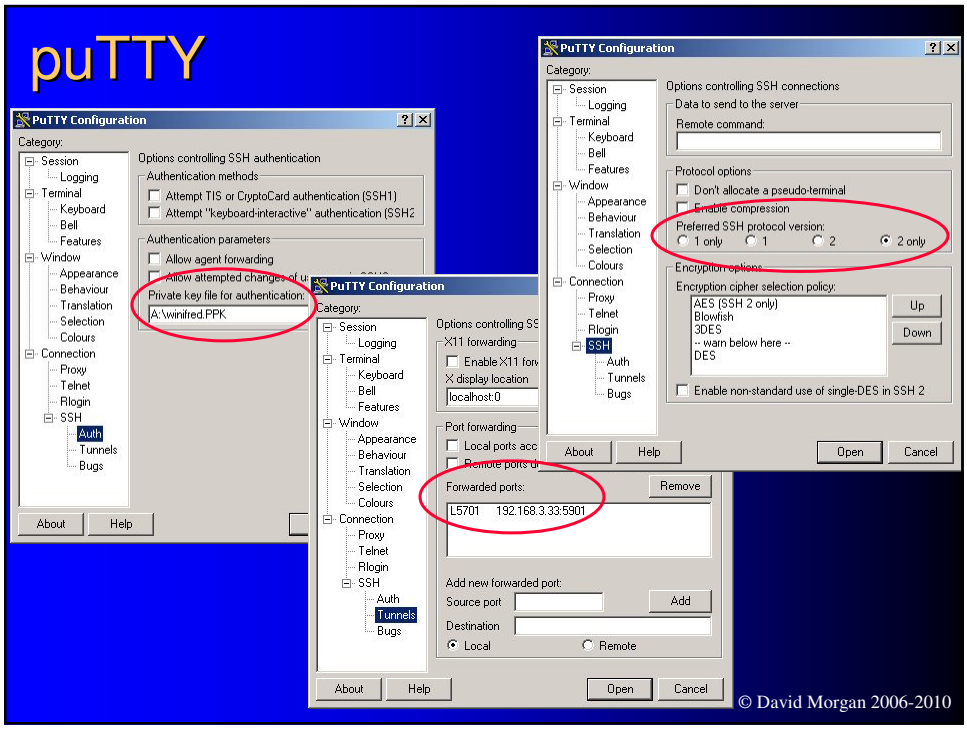


ssh port forwarding:

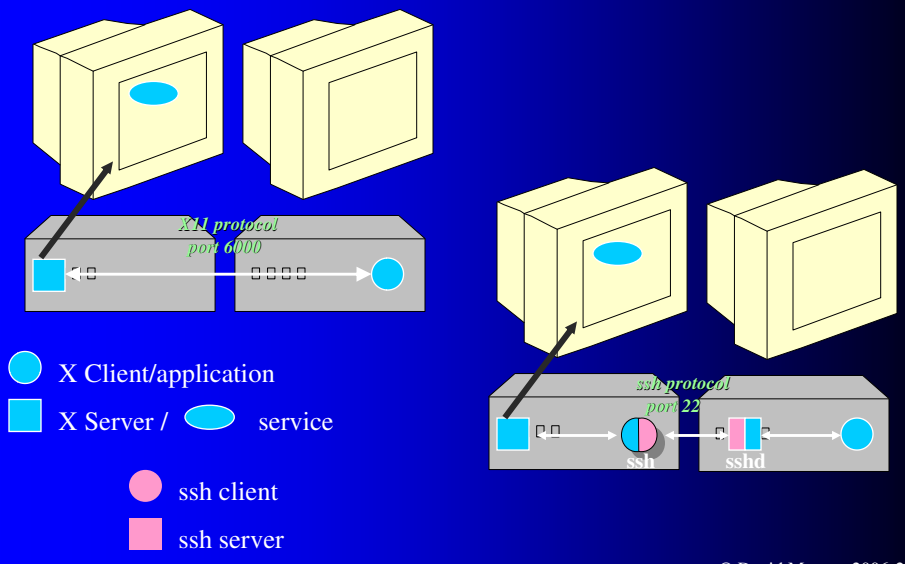
corresponds some port on "remote" (e.g. 3000) to
some port (e.g. 80) on a machine (e.g. "server") reachable from "gateway"

Example: http://127.0.0.1:3000 in client's browser gets served from 192.168.1.111:80


puTTY
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Proxy
Telnet
Rlogin
SSH
Auth
Tunnels
Bugs
Basic options for your PuTTY session
Specify your connection by host name or IP address
Host Name (or IP address)
Port
vnc@192.168.3.2
22
Protocol:
Raw
Telnet
Rlogin
SSH
Load, save or delete a stored session
Saved Sessions
vnc
Default Settings
vnc
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel
© David Morgan 2006-2010


puTTY
PuTTY Configuration
Options controlling SSH authentication
Authentication methods
Attempt TIS or CryptoCard authentication (SSH1)
Attempt "keyboard-interactive" authentication (SSH2
Authentication parameters
Allow agent forwarding
Private key file for authentication:
A:\winifred.PPK
Options controlling SSH connections
Data to send to the server
Remote command:
Protocol options
Don't allocate a pseudo-terminal
Enable compression
Preferred SSH protocol version:
1 only
1
2
2 only
Encryption options
Encryption cipher selection policy:
AES (SSH 2 only)
Blowfish
3DES
-- warn below here --
DES
Up
Down
Enable non-standard use of single-DES in SSH 2
X11 forwarding
Enable X11 for
X display location
localhost:0
Port forwarding
Local ports acc
Forwarded ports:
Remove
L5701 192.168.3.33:5901
Add new forwarded port:
Source port
Add
Destination
Local
Remote
About
Help
Open
Cancel
© David Morgan 2006-2010

ssh X11-forward vis-à-vis X

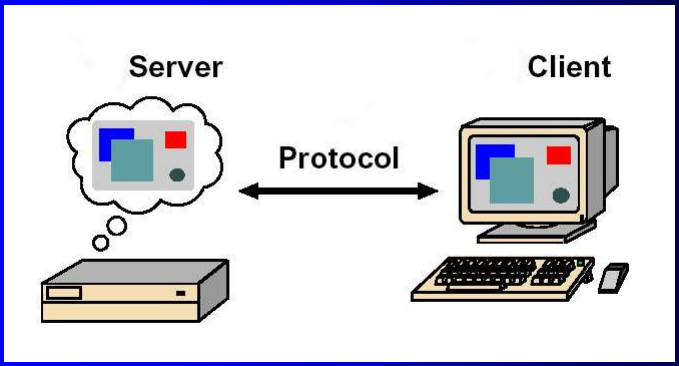


ssh man page excerpt

"If [appropriately configured] the connection to the X11 display is automatically forwarded to the remote side in such a way that any X11 programs started from the shell (or command) will go through the encrypted channel, and the connection to the real X server will be made from the local machine."

Accessing remote graphical I/O

-- with VNC or rdesktop



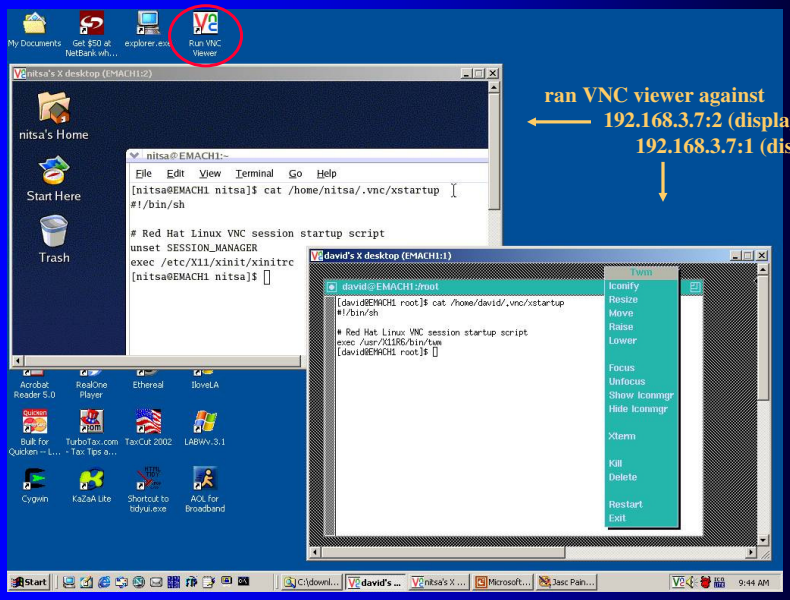
VNC

- RFB (Remote Frame Buffer) protocol
- by AT&T Laboratories, U.K. (defunct)
- server – ports 5900- for displays 0-
- plus http server – 100 ports lower
  - allows a browser as client

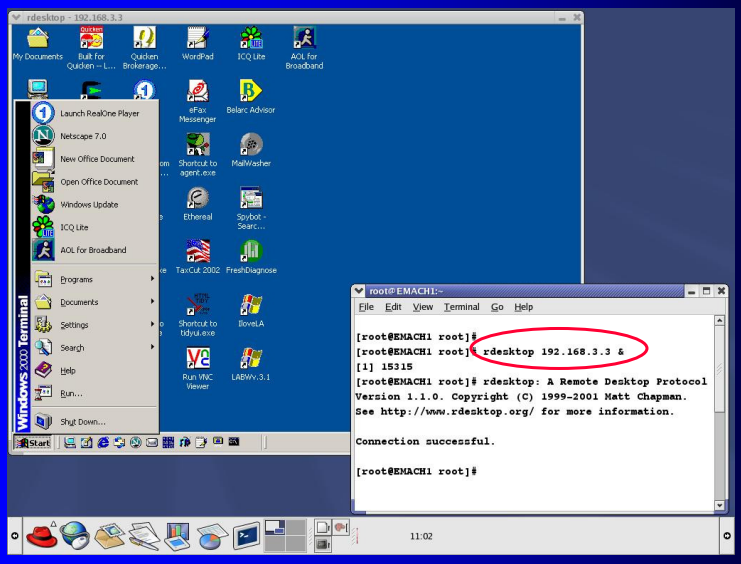
rdesktop

- RDP (Remote Desktop) Protocol
  - by Microsoft
- based on ITU T-120 family of protocols
  - "Data protocols for multimedia conferencing"
  - by International Telecommunications Union
- server - port 3389

lin desktop from win desktop (via vnc)



win desktop from lin desktop (via rdesktop)



VNC vis-à-vis X