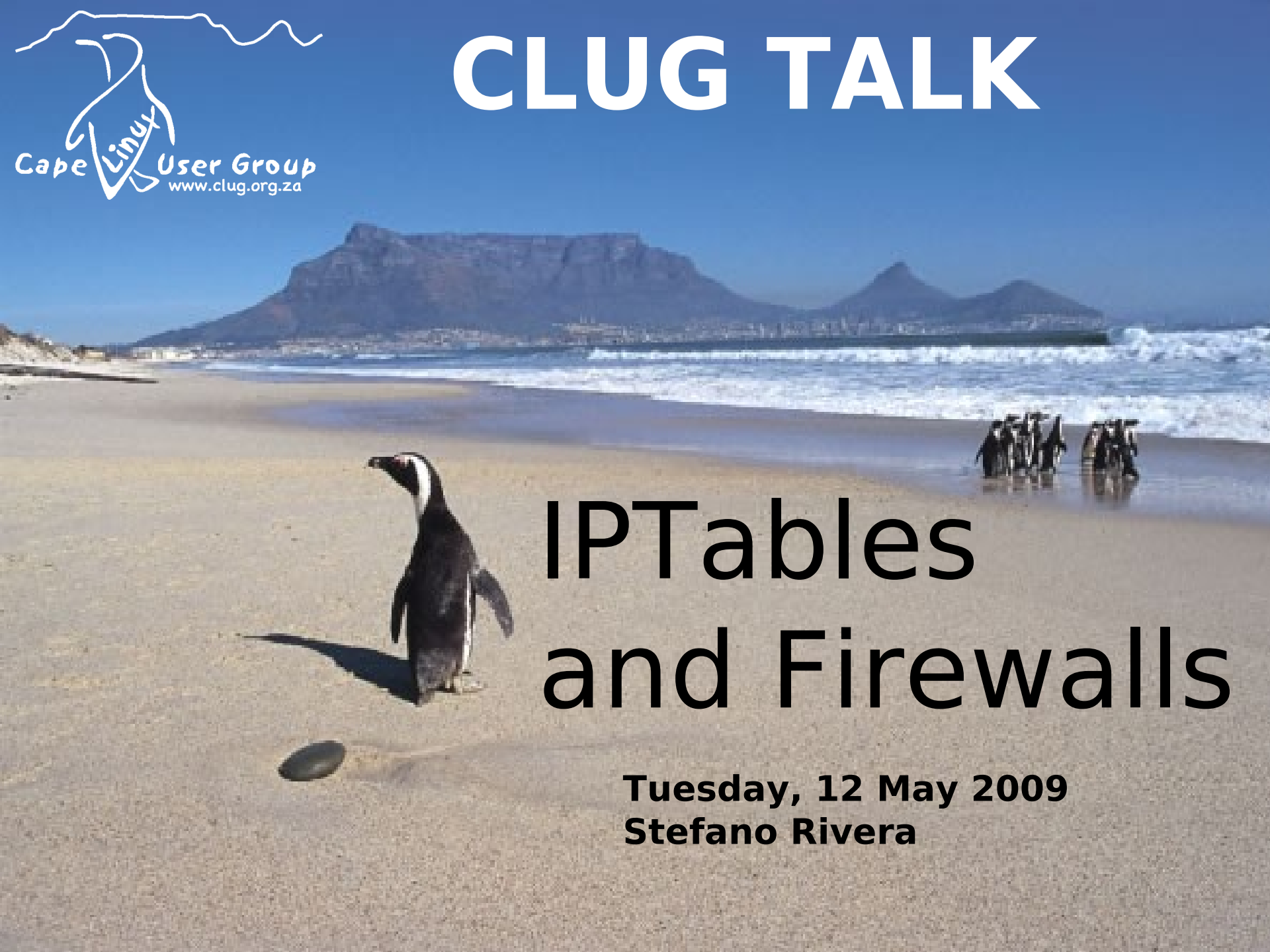
Cape Linux User Group
www.clug.org.za

CLUG TALK



IPTables and Firewalls

Tuesday, 12 May 2009
Stefano Rivera

Contents

- History
- Iptables
- Extensions
- Scary Diagrams
- No IPv6
- The end

What's the point?

- Security
- Naughty things (NAT)
- Accounting
- Debugging

History

- Nothing
- ipfwadm (1.1.1)
- ipchains (2.1.x)
- iptables (2.3.x)

Rules

```
# iptables -F INPUT
# iptables -A INPUT -i eth0 -p tcp --dport www -j ACCEPT
# iptables -A INPUT -i eth0 -s mypc.example.com -p tcp \
    --dport ssh -j ACCEPT
# iptables -A INPUT -i eth0 -j DROP
```

Chains

```
# iptables -N outgoing
# iptables -A outgoing -p tcp --dport www -j ACCEPT
# iptables -A outgoing -p udp --dport domain -j ACCEPT
# iptables -A outgoing -j DENY

# iptables -A FORWARD -o ppp0 -j outgoing
# iptables -A OUTPUT -o ppp0 -j outgoing
```

Rules

- ACCEPT
- DROP
- REJECT
- LOG
- RETURN

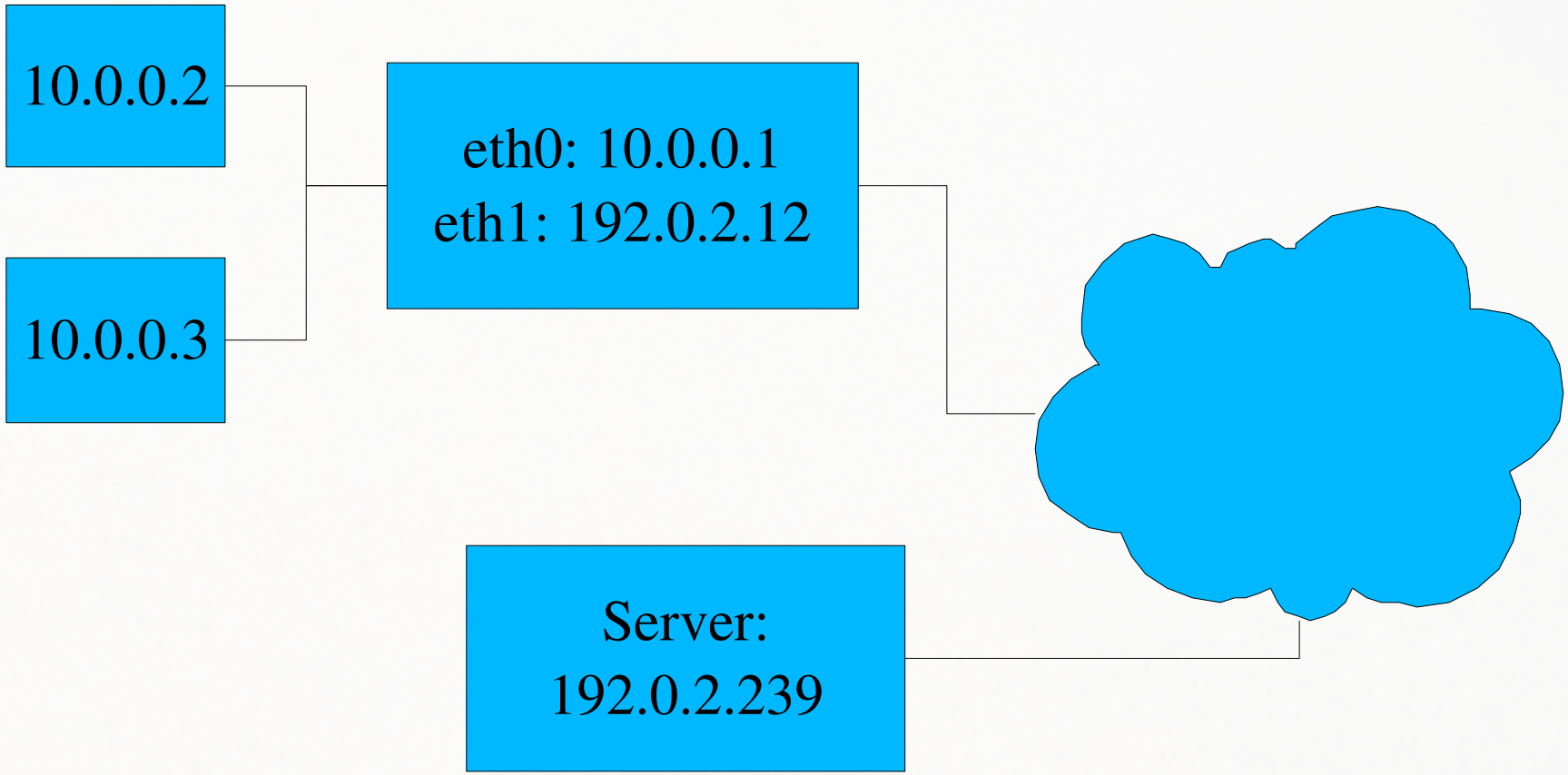
(and many more)

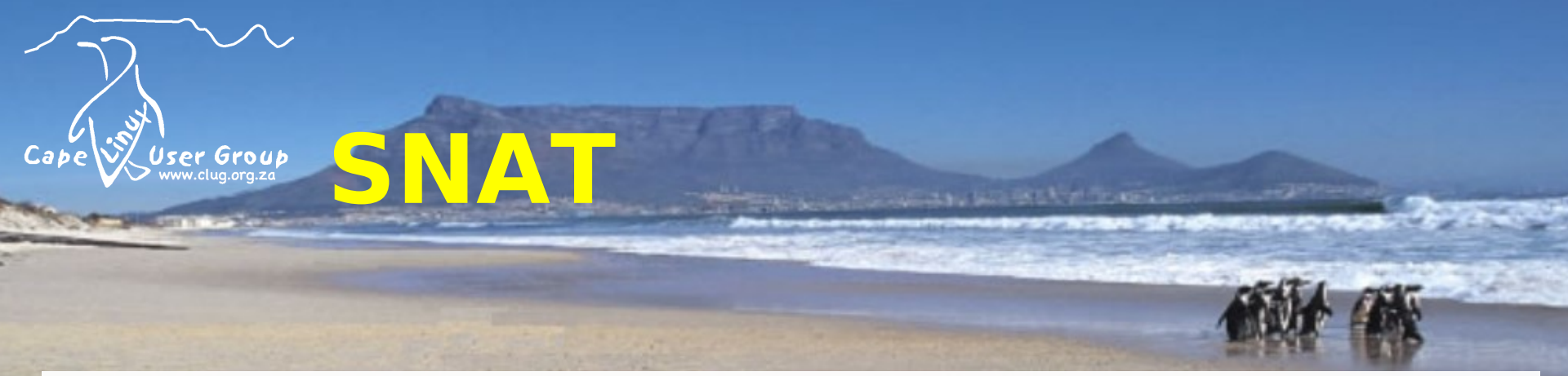
Tables

- filter
- nat
- mangle
- raw

Cape Linux User Group
www.clug.org.za

NAT





SNAT

```
# iptables -t nat -A POSTROUTING -i eth0 -o eth1 -j MASQUERADE
```

OR

```
# iptables -t nat -A POSTROUTING -i eth0 -o eth1 \
  -j DNAT –to 192.0.2.12
```

AND

```
# iptables -A FORWARD -j ACCEPT
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

DNAT

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 \
    -j REDIRECT --to localhost:8080
```

Diagrams

- Show off some scary diagrams

Netfilter Extensions

- Conntrack
- Iplimit
- Recent
- String / u32 / xor
- ulog
- Ipset
- L7 filtering

Other bits

- QoS
- iptables has “goto”

Future: nftables?

- Virtual machine

`-s 192.168.0.1` becomes

```
payload load 4 offset network header + 16 => reg 1
compare reg 1 192.168.0.1
```

Questions?

Cape Linux User Group
www.clug.org.za

More Information:

```
$ man iptables
```

netfilter.org

tldp.org

lartc.org