Scalable Operation of NATs with Per-Interface Bindings

or How I Stopped Worrying about NET10 Exhaustion and Learned to Love the NAT

http://tools.ietf.org/html/draft-arkko-dual-stack-extra-lite

Jari Arkko, Ericsson Research

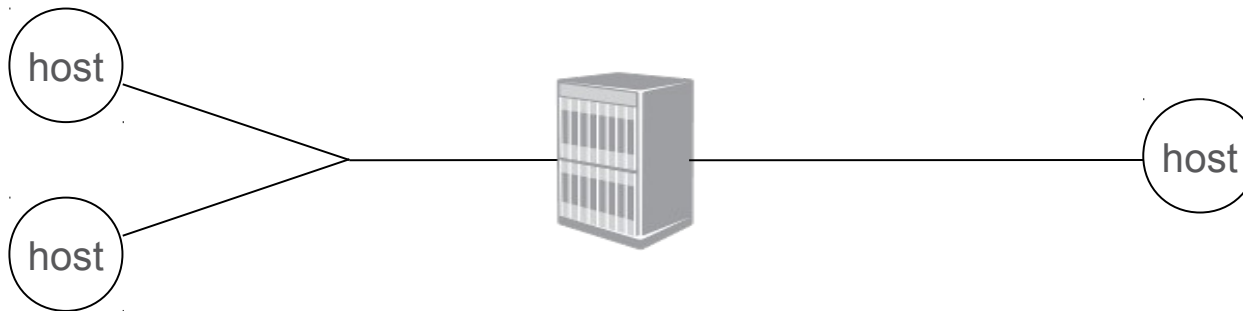Lars Eggert, Nokia Research Center

Original ideas are from Alain, Mark, and others

ERICSSON

Traditional NAT44 Architecture

hosts identified by
*a **private** address*

hosts identified by
*a **global** address*

host

host

host

flow from a private
address to a public
address

mapping

flow from a shared
public address to a
public address

10.0.0.1:5555 to 2.2.2.2:80
10.0.0.2:5555 to 2.2.2.2:80
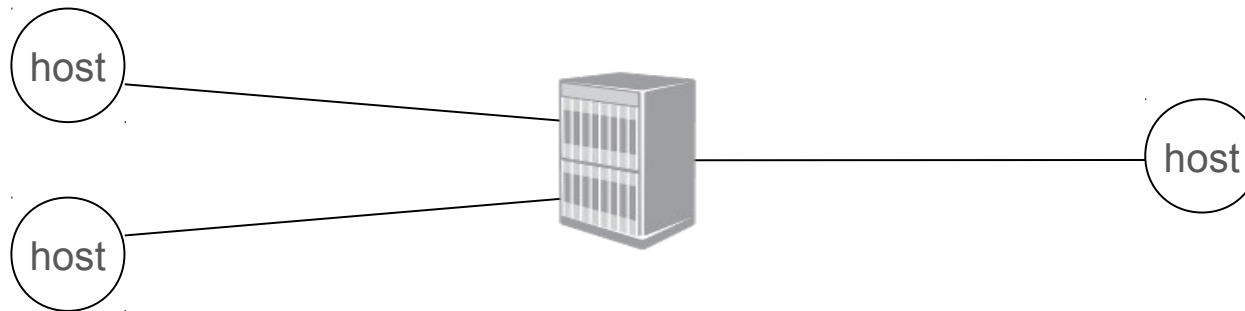
1.1.1.1:6666 to 2.2.2.2:80
1.1.1.1:7777 to 2.2.2.2:80

Per-Interface NAT44 Architecture

*hosts identified by an **interface** and a private address*

*hosts identified by a **global** address*

host

host

host

flow from an interface and a private address to a public address

mapping

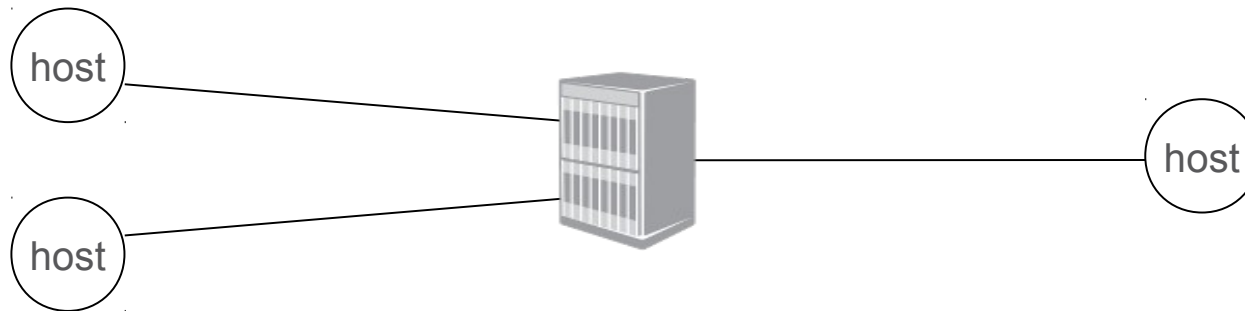*flow from a shared public address to a public address*

Eth0 10.0.0.1:5555 to 2.2.2.2:80
Eth1 10.0.0.1:5555 to 2.2.2.2:80

1.1.1.1:6666 to 2.2.2.2:80
1.1.1.1:7777 to 2.2.2.2:80

Per-Interface NAT44 Architecture

*hosts identified by an **interface** and a **private** address*

*hosts identified by a **global** address*

host

host

host

flow from an interface and a private address to a public address

mapping

flow from a shared public address to a public address

Eth0 10.0.0.1:5555 to 2.2.2.2:80
Eth1 10.0.0.1:5555 to 2.2.2.2:80

1.1.1.1:6666 to 2.2.2.2:80
1.1.1.1:7777 to 2.2.2.2:80

Applicability

› Allows reuse of RFC 1918 space for different users

› Applicable when the NAT has separate interfaces: GGSNs, home agents, tunnel servers

› Dual Stack Lite is one example of a tunnel server but the core idea can be applied even without introducing additional tunnels

› No new protocols, standards, or host impacts – just a local implementation technique

› Allows a near-infinite number of private addresses

› But does NOT avoid harmful side-effects of NATs or make it easy to address a host from the outside

› But there's always IPv6...

Recommended Deployment Model

Works well together with Dual Stack:

› NAT44 allows access to the IPv4 Internet

› Per-interface extension allows any number of hosts

› IPv6 avoids the harmful effects of NATs

    For instance, selected operator services can employ IPv6 and not suffer
    from the consequences of NATs or overlapping address space

Questions? Comments?