
Subject: no access to domain names

Posted by [goeldi](#) on Fri, 06 Nov 2009 12:49:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

I cannot ping a domainname from CT. Pinging to IP address works.

Node kernel: 2.6.18-128.2.1.el5.028stab064.7ent

Node is CentOS 5.4

On node: # cat /etc/resolv.conf
nameserver 212.40.0.10

In CT: # cat /etc/resolv.conf
nameserver 212.40.0.10

ifconfig on node:

```
eth0  Link encap:Ethernet HWaddr 00:1D:0F:C0:E9:9D
      inet addr:192.168.2.238 Bcast:192.168.2.255 Mask:255.255.255.0
      inet6 addr: fe80::21d:fff:fec0:e99d/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:1073 errors:0 dropped:0 overruns:0 frame:0
      TX packets:644 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:96397 (94.1 KiB) TX bytes:85949 (83.9 KiB)
      Interrupt:225 Base address:0x2c00
```

```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

```
venet0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
      UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
      RX packets:90 errors:0 dropped:0 overruns:0 frame:0
      TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:4868 (4.7 KiB) TX bytes:6592 (6.4 KiB)
```

ifconfig in VE:

```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
```

UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

venet0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:127.0.0.1 P-t-P:127.0.0.1 Bcast:0.0.0.0 Mask:255.255.255.255
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
RX packets:17 errors:0 dropped:0 overruns:0 frame:0
TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1472 (1.4 KiB) TX bytes:1124 (1.0 KiB)

venet0:0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:192.168.2.149 P-t-P:192.168.2.149 Bcast:192.168.2.149 Mask:255.255.255.255
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1

Routing rule on node:

0: from all lookup 255

32766: from all lookup main

32767: from all lookup default

ip route list table all on node

192.168.2.149 dev venet0 scope link

192.168.2.148 dev venet0 scope link

195.141.118.148 dev venet0 scope link

192.168.2.0/24 dev eth0 proto kernel scope link src 192.168.2.238

169.254.0.0/16 dev eth0 scope link

default via 192.168.2.1 dev eth0

local 192.168.2.238 dev eth0 table 255 proto kernel scope host src 192.168.2.238

broadcast 192.168.2.255 dev eth0 table 255 proto kernel scope link src 192.168.2.238

broadcast 127.255.255.255 dev lo table 255 proto kernel scope link src 127.0.0.1

broadcast 192.168.2.0 dev eth0 table 255 proto kernel scope link src 192.168.2.238

broadcast 127.0.0.0 dev lo table 255 proto kernel scope link src 127.0.0.1

local 127.0.0.1 dev lo table 255 proto kernel scope host src 127.0.0.1

local 127.0.0.0/8 dev lo table 255 proto kernel scope host src 127.0.0.1

fe80::/64 dev eth0 metric 256 expires 21333881sec mtu 1500 advmss 1440 hoplimit
4294967295

unreachable default dev lo table unspec proto none metric -1 error -101 hoplimit 255

local ::1 via :: dev lo table 255 proto none metric 0 mtu 16436 advmss 16376 hoplimit
4294967295

local fe80::21d:fff:fec0:e99d via :: dev lo table 255 proto none metric 0 mtu 16436 advmss
16376 hoplimit 4294967295

ff00::/8 dev eth0 table 255 metric 256 expires 21333881sec mtu 1500 advmss 1440 hoplimit
4294967295

```
unreachable default dev lo table unspec proto none metric -1 error -101 hoplimit 255
```

```
# iptables -t nat -L && iptables -t filter -L && iptables -t mangle -L on node:
```

```
Chain PREROUTING (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain POSTROUTING (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain INPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
RH-Firewall-1-INPUT all -- anywhere anywhere
```

```
Chain FORWARD (policy ACCEPT)
```

```
target prot opt source destination
```

```
RH-Firewall-1-INPUT all -- anywhere anywhere
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain RH-Firewall-1-INPUT (2 references)
```

```
target prot opt source destination
```

```
ACCEPT all -- anywhere anywhere
```

```
ACCEPT icmp -- anywhere anywhere icmp any
```

```
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
```

```
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
```

```
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ndmp
```

```
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited
```

```
Chain PREROUTING (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain INPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain FORWARD (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain POSTROUTING (policy ACCEPT)
```

```
target prot opt source destination
```

CT Routing:

```
192.0.2.0/24 dev venet0 scope host
169.254.0.0/16 dev venet0 scope link
default via 192.0.2.1 dev venet0
broadcast 127.255.255.255 dev lo table 255 proto kernel scope link src 127.0.0.1
local 192.168.2.149 dev venet0 table 255 proto kernel scope host src 192.168.2.149
broadcast 192.168.2.149 dev venet0 table 255 proto kernel scope link src 192.168.2.149
broadcast 127.0.0.0 dev lo table 255 proto kernel scope link src 127.0.0.1
local 127.0.0.1 dev lo table 255 proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev venet0 table 255 proto kernel scope host src 127.0.0.1
local 127.0.0.0/8 dev lo table 255 proto kernel scope host src 127.0.0.1
unreachable default dev lo table unspec proto none metric -1 error -101 hoplimit 255
local ::1 via :: dev lo table 255 proto none metric 0 mtu 16436 advmss 16376 hoplimit
4294967295
unreachable default dev lo table unspec proto none metric -1 error -101 hoplimit 255
```

Routing rule in CT:

```
0: from all lookup 255
32766: from all lookup main
32767: from all lookup default
```

tcpdump -i venet0:0 when pinging to google.com from CT:

```
# tcpdump -i venet0:0
```

```
tcpdump: WARNING: arptype 65535 not supported by libpcap - falling back to cooked socket
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on venet0:0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
23:33:02.019896 IP test5.47612 > 212.40.0.10.domain: 39786+ A? google.com. (28)
23:33:02.062725 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin
prohibited, length 64
23:33:07.062866 IP test5.37160 > 212.40.0.10.domain: 39786+ A? google.com. (28)
23:33:07.062892 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin
prohibited, length 64
23:33:07.062906 IP test5.34840 > 212.40.0.10.domain: 27708+ A? google.com. (28)
23:33:07.062922 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin
prohibited, length 64
23:33:07.062936 IP test5.34565 > 212.40.0.10.domain: 27708+ A? google.com. (28)
23:33:07.062951 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin
prohibited, length 64
23:33:02.062538 IP test5.46799 > 212.40.0.10.domain: 47287+ PTR? 10.0.40.212.in-addr.arpa.
(42)
23:33:02.062561 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin
prohibited, length 78
23:33:02.062595 IP test5.54328 > 212.40.0.10.domain: 47287+ PTR? 10.0.40.212.in-addr.arpa.
```

(42)

23:33:02.062601 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin prohibited, length 78

23:33:02.062776 IP test5.53512 > 212.40.0.10.domain: 49993+ PTR?

238.2.168.192.in-addr.arpa. (44)

23:33:07.062768 IP test5.53512 > 212.40.0.10.domain: 49993+ PTR?

238.2.168.192.in-addr.arpa. (44)

23:33:07.062794 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin prohibited, length 80

the same as above when I ping to the IP of the nameserver 212.40.0.10:

tcpdump: WARNING: arptype 65535 not supported by libpcap - falling back to cooked socket

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on venet0:0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes

00:38:05.724786 IP test5 > 212.40.0.10: ICMP echo request, id 17452, seq 1, length 64

00:38:05.748579 IP 212.40.0.10 > test5: ICMP echo reply, id 17452, seq 1, length 64

00:38:05.769203 IP test5.46227 > 212.40.0.10.domain: 57462+ PTR? 10.0.40.212.in-addr.arpa.

(42)

00:38:05.769237 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin prohibited, length 78

00:38:05.769318 IP test5.42538 > 212.40.0.10.domain: 57462+ PTR? 10.0.40.212.in-addr.arpa.

(42)

00:38:05.769325 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin prohibited, length 78

00:38:05.769606 IP test5.33772 > 212.40.0.10.domain: 5261+ PTR? 238.2.168.192.in-addr.arpa.

(44)

00:38:05.769612 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin prohibited, length 80

00:38:05.769661 IP test5.48588 > 212.40.0.10.domain: 5261+ PTR? 238.2.168.192.in-addr.arpa.

(44)

00:38:05.769667 IP 192.168.2.238 > test5: ICMP host 212.40.0.10 unreachable - admin prohibited, length 80

00:38:06.725786 IP test5 > 212.40.0.10: ICMP echo request, id 17452, seq 2, length 64

00:38:06.749797 IP 212.40.0.10 > test5: ICMP echo reply, id 17452, seq 2, length 64

00:38:07.726687 IP test5 > 212.40.0.10: ICMP echo request, id 17452, seq 3, length 64

00:38:07.750301 IP 212.40.0.10 > test5: ICMP echo reply, id 17452, seq 3, length 64

00:38:08.727587 IP test5 > 212.40.0.10: ICMP echo request, id 17452, seq 4, length 64

00:38:08.749219 IP 212.40.0.10 > test5: ICMP echo reply, id 17452, seq 4, length 64

pinging to google.com when IPTables on node is stopped works:

tcpdump: WARNING: arptype 65535 not supported by libpcap - falling back to cooked socket

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on venet0:0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes

00:40:00.067823 IP test5.57627 > ns1.datacomm.ch.domain: 13803+ A? google.com. (28)

00:40:00.068188 IP test5.54413 > ns1.datacomm.ch.domain: 55300+ PTR?

10.0.40.212.in-addr.arpa. (42)

00:40:00.115625 IP ns1.datacomm.ch.domain > test5.57627: 13803 3/4/3 A
gw-in-f100.1e100.net,[[domain]
00:40:00.115914 IP test5 > gw-in-f100.1e100.net: ICMP echo request, id 50988, seq 1, length 64
00:40:00.123566 IP ns1.datacomm.ch.domain > test5.54413: 55300* 1/3/3 (169)
00:40:00.123886 IP test5.52523 > ns1.datacomm.ch.domain: 50168+ PTR?
100.67.125.74.in-addr.arpa. (44)
00:40:00.160345 IP ns1.datacomm.ch.domain > test5.52523: 50168 1/4/3 (208)
00:40:00.270733 IP gw-in-f100.1e100.net > test5: ICMP echo reply, id 50988, seq 1, length 64
00:40:00.270953 IP test5.60735 > ns1.datacomm.ch.domain: 6973+ PTR?
100.67.125.74.in-addr.arpa. (44)
00:40:00.272663 IP ns1.datacomm.ch.domain > test5.60735: 6973 1/0/0 (78)
00:40:01.116327 IP test5 > gw-in-f100.1e100.net: ICMP echo request, id 50988, seq 2, length 64
00:40:01.285608 IP gw-in-f100.1e100.net > test5: ICMP echo reply, id 50988, seq 2, length 64
00:40:02.116227 IP test5 > gw-in-f100.1e100.net: ICMP echo request, id 50988, seq 3, length 64
00:40:02.255560 IP gw-in-f100.1e100.net > test5: ICMP echo reply, id 50988, seq 3, length 64
00:40:03.116126 IP test5 > gw-in-f100.1e100.net: ICMP echo request, id 50988, seq 4, length 64
00:40:03.255745 IP gw-in-f100.1e100.net > test5: ICMP echo reply, id 50988, seq 4, length 64
00:40:04.116031 IP test5 > gw-in-f100.1e100.net: ICMP echo request, id 50988, seq 5, length 64
00:40:04.254865 IP gw-in-f100.1e100.net > test5: ICMP echo reply, id 50988, seq 5, length 64

Subject: Re: no access to domain names

Posted by [maratrus](#) on Fri, 06 Nov 2009 13:54:41 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello Goeldi,

I'm almost sure that the problem is in iptables rules.

This one

Quote:

```
REJECT    all -- anywhere          anywhere          reject-with icmp-host-prohibited
```

rejects the input traffic.

Could you please check it?