strongSwan - Issue #2112

Broadcast packets are not relayed from Lan to Vpn clilent

10.09.2016 12:30 - Alex Brew

Status:	New		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.5.0	**Resolution:**	

Description

Strongswan 5.5 installed at Ubuntu 14.04 LTS x64, built from sources.
Also forecast plug-in is enabled, set up and working.
There are some Lan clients and Ikev2 Vpn clients connected from time to time.

So, there are its settings:
portion from ipsec.conf

mark=%unique at ikev2 connection
broadcast address 255.255.255.255 is added to leftsubnet, and there is no rightsubnet at all

portion from strongswan.conf
forecast {
interface=lan
reinject=ikev2_cert_,ikev1_xauth_cert
}

Packets from Vpn clients with 255.255.255.255 as destination are relayed to lan, but from lan are not to ikev2 tunnel.

I added rightsubnet=%dynamic,255.255.255.255.

Looked at log and saw that packet from Lan client to 255.255.255.255 was intercepted and sent to 255.255.255.255/32, not to Vpn client in other words, not to Vpn net.

History

#1 - 10.09.2016 12:51 - Noel Kuntze

> portion from ipsec.conf

Full logs and config, please. And try to use the formatting commands in the help message of the wiki (click the question mark symbol for help) to format configurations and logs correctly. Also, "expand" can be used.

> I added rightsubnet=%dynamic,255.255.255.255.

Check if that TS is actually negotiated.

#2 - 10.09.2016 23:37 - Alex Brew

- File strongswan.conf added

- File ipsec.conf added

- File strongswan.log added

So, **ipsec status**:

```
Security Associations (1 up, 0 connecting):
ikev2_cert_eap-mschapv2[1]: ESTABLISHED 2 minutes ago, 95.245.95.95[CN=My CA Server Certificate for Vpn...]...
```

```
79.2451.35.195[10.20.0.1]
ikev2_cert_eap-mschapv2{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c14252df_i 24d3c43b_o
ikev2_cert_eap-mschapv2{1}:   192.168.0.0/24 255.255.255.255/32 === 192.168.0.202/32 255.255.255.255/32
```

Look at attached files.

#3 - 11.09.2016 00:32 - Noel Kuntze

Logs indicate it works:

```
Sep 10 23:58:40 07[NET] forecast intercepted packet: 192.168.0.70 to 255.255.255.255
Sep 10 23:58:40 07[NET] forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 255.255.255.255/32 (1
)
```

#4 - 11.09.2016 11:23 - Alex Brew

Noel Kuntze wrote:

> Logs indicate it works:
> [...]

So, if you look at log for opposite direction, you will see:
forecast intercepted packet: 192.168.0.202 to 255.255.255.255
forwarding a 255.255.255.255 broadcast from peer 192.168.0.202 to internal network

But regarding direction lan->vpn, there is
forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 255.255.255.255/32
not
forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 192.168.0.202/32
or some look like
forwarding a 255.255.255.255 broadcast from peer 192.168.0.70 to vpn clients

And I can not see any packets from lan to 255.255.255.255 at Vpn client are reached its.

In particular, speaking is about NetBios.

#5 - 11.09.2016 11:34 - Noel Kuntze

Alex Brew wrote:

> Noel Kuntze wrote:
>
> > Logs indicate it works:
> > [...]
>
> So, if you look at log for opposite direction, you will see:
> forecast intercepted packet: 192.168.0.202 to 255.255.255.255
> forwarding a 255.255.255.255 broadcast from peer 192.168.0.202 to internal network

Is that actually in the log of the remote side? Please attach the log to this issue.

> But regarding direction lan->vpn, there is
> forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 255.255.255.255/32
> not
> forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 192.168.0.202/32
> or some look like
> forwarding a 255.255.255.255 broadcast from peer 192.168.0.70 to vpn clients

The destination of a broadcast packet is 255.255.255.255 (all networks) or 192.168.0.255 (this network).
The forecast plugin duplicates packets to the registered IP addresses in its and sends them out over socket with the corresponding mark value.
The log message's format or formulation doesn't give you any indication of what exactly it does.
The to peer x/32 just uses the destination IP of the packet. It doesn't use the assigned IP of the remote peer.

> And I can not see any packets from lan to 255.255.255.255 at Vpn client are reached its.
>
> In particular, speaking is about NetBios.

#6 - 11.09.2016 11:41 - Alex Brew

Noel Kuntze wrote:

> Alex Brew wrote:
>
> > Noel Kuntze wrote:
> >
> > > Logs indicate it works:
> > > [...]
> >
> > So, if you look at log for opposite direction, you will see:
> > forecast intercepted packet: 192.168.0.202 to 255.255.255.255
> > forwarding a 255.255.255.255 broadcast from peer 192.168.0.202 to internal network
>
> Is that actually in the log of the remote side? Please attach the log to this issue.
>
> > But regarding direction lan->vpn, there is
> > forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 255.255.255.255/32
> > not
> > forwarding a 255.255.255.255 broadcast from 192.168.0.70 to peer 192.168.0.202/32
> > or some look like
> > forwarding a 255.255.255.255 broadcast from peer 192.168.0.70 to vpn clients
>
> The destination of a broadcast packet is 255.255.255.255 (all networks) or 192.168.0.255 (this network).
> The forecast plugin duplicates packets to the registered IP addresses in its and sends them out over socket with the corresponding mark value.
> The log message's format or formulation doesn't give you any indication of what exactly it does.
> The to peer x/32 just uses the destination IP of the packet. It doesn't use the assigned IP of the remote peer.
>
> > And I can not see any packets from lan to 255.255.255.255 at Vpn client are reached its.
> >
> > In particular, speaking is about NetBios.

No. The log is from server side only.
So, did I understand you right, that forecast inpercepted packet from lan node to 255.255.255.255 will be forwarded to Vpn client ?

May be some additional **iptables** settings are necessary. What one ?

#7 - 11.09.2016 11:47 - Alex Brew

If in simple words, I can not ping Vpn client from Lan by NetBios name, but van ping Lan client from Vpn by NetBios name.
NetBiosname of Vpn client is not resolved due to broadcast unreaching of Vpn client from Lan.

#8 - 11.09.2016 12:01 - Noel Kuntze

Alex Brew wrote:

> [..]
>
> No. The log is from server side only.
> So, did I understand you right, that forecast inpercepted packet from lan node to 255.255.255.255 will be forwarded to Vpn client ?

Yes.

> May be some additional **iptables** settings are necessary. What one ?

I don't think so. Check the traffic flow.

#9 - 11.09.2016 12:14 - Alex Brew

Noel Kuntze wrote:

> Alex Brew wrote:
>
> > [..]
> >
> > No. The log is from server side only.
> > So, did I understand you right, that forecast inpercepted packet from lan node to 255.255.255.255 will be forwarded to Vpn client ?

> Yes.
>
> > May be some additional **iptables** settings are necessary. What one ?
>
> I don't think so. Check the traffic flow.

How is the best way to check the traffic at the case ?

#10 - 11.09.2016 12:15 - Noel Kuntze

tcpdump, wiresharking, checking the traffic counter of the CHILD_SA in the output of ipsec statusall. Be creative and inventive.

#11 - 11.09.2016 14:12 - Alex Brew

Noel Kuntze wrote:

> tcpdump, wiresharking, checking the traffic counter of the CHILD_SA in the output of ipsec statusall. Be creative and inventive.

I made dumpig via nflog:group.

So, may be you will tell how packets from Lan to 192.168.0.255 is to forward to Vpn client ?
Or packet for 192.168.0.255 forward to 255.255.255.255 to tunnel ?
What settings and where are necessary ?

Or I understand something wrong...
But Vpn hosts are not resolved by NetBios names.

#12 - 12.09.2016 15:29 - Alex Brew

Noel Kuntze wrote:

> tcpdump, wiresharking, checking the traffic counter of the CHILD_SA in the output of ipsec statusall. Be creative and inventive.

Noel, by your knowlegde, or for your fresh eyes, does Vpn client with 192.168.0.202/255.255.255.255 (for example) have to answer for Lan directed broadcast packet forwarded from Lan to 192.168.0.255 ?
Or not ?
In other way, Lan client (192.168.0.15/255.255.255.0) answers for packet forwarded from Vpn client to 255.255.255.255.

#13 - 12.09.2016 18:20 - Noel Kuntze

Any host is free to respond to a packet or not. Did you check if the packets make it to the client?

#14 - 14.09.2016 14:18 - Alex Brew

Noel Kuntze wrote:

> Any host is free to respond to a packet or not. Did you check if the packets make it to the client?

It is broadcast NetBios UDP 137, 138 port packets.

For l2tpd/ipsec connection I use bcrelay daemon.
It forwards broadcasts to limited 255.255.255.255 address. I think it is regarding netmask of uped ppp interface.
That is whet l2tp connection is established, ppp0... interfaces are uped at servers side with netmask of 255.255.255.255.

But when ikev2 connections established, broadcasts are forwarded to directed net 192.168.0.225 address.

Is it possible to add to forecast plug-in setting, which would turn on/off reforwarding directed broadcast from 192.168.0.255 tolimited broadcast address 255.255.255.255 ?

Files

strongswan.conf	1.98 KB	10.09.2016	Alex Brew
ipsec.conf	2.02 KB	10.09.2016	Alex Brew
strongswan.log	3.51 MB	10.09.2016	Alex Brew