A server on my home network (10.1.1.32/24) is used to allow remote devices to connect to the network, and assigns road warriors an IP using DHCP from the router. This setup/config works on 5.5.3 and prior, but fails to work on 5.6.0 or 5.6.1dr3. Kernel version is 4.13.11, Arch Linux.

It's a pretty basic config where clients are configured with "leftsourceip=%config4 rightsubnet=10.1.1.0/24" and server is rightsourceip=%dhcp. Traffic from the road warrior makes it through the tunnel, but no responses are sent back to it. Pinging/accessing the client's IP from the server sends the packets off to the gateway/router instead of through the tunnel, and outgoing packet counters do not increase. Using a subnet that does not overlap (leftsourceip=10.1.2.0/24) works fine, as does IPV6. See attached for full configs, as well as ip route and ip xfrm state/policy dumps - the client is assigned 10.1.1.130 via DHCP.

5.5.3 loaded plugins: charon aesni aes des rc2 sha2 sha3 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp curve25519 agent chapoly xcb c hmac ntru newhope bliss curl sqlite attr kernel-netlink resolve socket-default connmark forecast farp stroke vici updown eap-identity eap-sim eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-reauth eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp radattr unity

5.6.0 loaded plugins: charon idap aesni aes des rc2 sha2 sha3 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp curve25519 agent chapoly xcb c hmac ntru newhope bliss curl mysql sqlite attr kernel-netlink resolve socket-default bypass-lan connmark forecast farp stroke vici updown eap-identity eap-sim eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-reauth eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp radattr unity

5.6.1dr3 loaded plugins: loaded plugins: charon idap aesni aes des rc2 sha2 sha3 sha1 md5 mgf1 random nonce x5 09 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp curve25519 9 agent chapoly xcb c hmac ntru newhope bliss curl mysql sqlite attr kernel-netlink resolve socket-default bypass-lan connmark forecast farp stroke vici updown eap-identity eap-sim eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-reauth eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp radattr unity

I guess then the issue is that the plugin's presence makes it impossible to host virtual IPs on any local networks, should the policy priorities be adjusted to prevent this from happening?
Hm looks like that's it, it was enabled recently on the arch package and is loaded by default:
https://git.archlinux.org/svntogit/community.git/commit/trunk?h=packages/strongswan&id=b23268cbc76a09bc2273e316ad50d8f5866d664c

OK.

I guess then the issue is that the plugin's presence makes it impossible to host virtual IPs on any local networks, should the policy priorities be adjusted to prevent this from happening?

The whole point of the plugin is to explicitly bypass IPsec tunnels for local traffic (and it's more intended for clients than for gateways). Just disable the plugin (via /etc/strongswan.d/charon/bypass-lan.conf or directly in strongswan.conf).

#4 - 09.11.2017 20:10 - arc xmncre
Tobias Brunner wrote:

The whole point of the plugin is to explicitly bypass IPsec tunnels for local traffic (and it's more intended for clients than for gateways). Just disable the plugin (via /etc/strongswan.d/charon/bypass-lan.conf or directly in strongswan.conf).

Yup disabling it does work. I can just edit/delete bypass-lan.conf. I did come across that plugin when trying to diagnose the issue but I incorrectly assumed it was harmless because a more specific virtual IP route/policy would take precedence over a blanket bypass - and also assumed that its default configuration would not prevent some basic functionality from working.

Part of the issue lies in that the recommended way to enable or disable plugins is during compile time and a distro will just provide precompiled packages with all plugins enabled by default (what's not clear to me is whether not enabling a plugin at compile time allows manual enabling by config later, or omits it from the build entirely). It seems like an invasive plugin that should not be enabled by default config in a generic distribution, although if disabling prevents anyone from using it then I suppose some documentation that it will conflict with server configurations would be the next best solution.

#5 - 10.11.2017 09:06 - Tobias Brunner

I did come across that plugin when trying to diagnose the issue but I incorrectly assumed it was harmless because a more specific virtual IP route/policy would take precedence over a blanket bypass

Bypass policies currently always have the highest priority.

(what's not clear to me is whether not enabling a plugin at compile time allows manual enabling by config later, or omits it from the build entirely).

Yes, anything not enabled via configure script won't be built. But distros are free to patch the config snippets (set load = no in them) if they don't want some of the plugins to get loaded by default (or if the plugin is shipped in a separate package also ship the config snippet with it, so it is only loaded when installed).

#6 - 18.04.2018 17:33 - Tobias Brunner
- Category set to configuration
- Status changed from Feedback to Closed
- Assignee set to Tobias Brunner
- Resolution set to No change required

Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>client.conf</td>
<td>279 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>policy-5.5.txt</td>
<td>608 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>policy-5.6.txt</td>
<td>975 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>routes-5.5.txt</td>
<td>842 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>routes-5.6.txt</td>
<td>899 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>server.conf</td>
<td>264 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>state-5.5.txt</td>
<td>745 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
<tr>
<td>state-5.6.txt</td>
<td>745 Bytes</td>
<td>08.11.2017</td>
<td>arc xmncre</td>
</tr>
</tbody>
</table>