9800 series phones using OpenVPN always use source port UDP 1194.

Last Modified on 04/23/2020 2:31 pm EDT

Products Affected:

9800 series IP phones configured for OpenVPN on Wave 4.0 and later.

Issue

At some remote locations with underline multiple OpenVPN phones, certain Firewalls (notably Cisco ASA) may have issues with these phones all sending from the same source port (UDP 1194).

Symptoms

Phones may not act as expected & may need

Logs from OpenVPN server (/var/log/openvpn.log) may show similar to that below:

```
Mar 12 13:39:46 openvpn 44820 b061c7ffffff/:1194 TLS Error: local/remote TLS keys are out of sync:
[AF_INET]:1194 [0]
Mar 12 13:39:44 openvpn 44820 b061c7ffffff/:1194 TLS Error: local/remote TLS keys are out of sync:
[AF_INET]:1194 [0]
Mar 12 13:39:43 openvpn 44820 b061c7ffffff/:1194 TLS Error: local/remote TLS keys are out of sync:
[AF_INET]:1194 [0]
Mar 12 13:39:43 openvpn 44820 b061c7ffffff/:1194 TLS Error: local/remote TLS keys are out of sync:
[AF_INET]:1194 [0]
Mar 12 13:39:42 openvpn 44820 b061c7ffffff/:1194 TLS Auth Error: Auth Username/Password verification
failed for peer
Mar 12 13:39:42 openvpn 44820 b061c7ffffff/:1194 TLS Auth Error: username attempted to change from
'b061c7ffffff' to 'b061c7ffffee' -- tunnel disabled
```

Cause

While Firewalls are setup to perform NAT, several may by default or configuration try to avoid PAT as well. This may be for performance or other reasons. The OpenVPN phones by default use the same source port, UDP 1194. The issue arises as since they're using
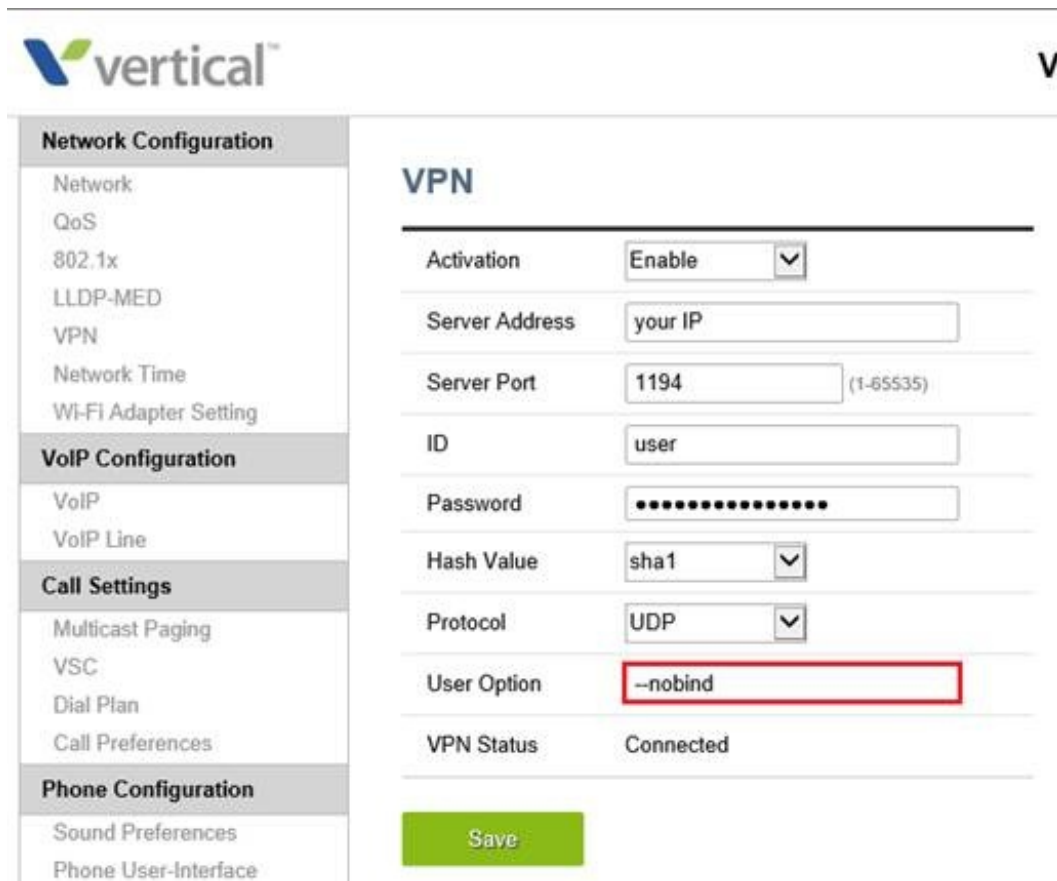
the same source port, mapped to the same external IP address and are sending traffic to the same destination port & IP address, the firewall loses track of which packets go to which phone.

Resolution

The configuration noted here can be done on a per phone basis via the web interface, or can be implemented via a custom configuration file per the phone model.

One off phone configuration via web interface:

Under the VPN section, set the 'User Option' to --nobind (pictures are not clear but it is two separate dashes with no space between them).

Custom file configuration per phone model:

Or this can be accomplished by setting up a custom file on the Wave as follows:

```
--nobind
```

Below is a screen capture of this:

```
sysconf_9x30_sip_custom.xml - Notepad
File   Edit   Format   View   Help
<?xml version="1.0" encoding="UTF-8"?>
<Settings>
        <Vpn>
              <UserOption>--nobind</UserOption>
        </Vpn>
</Settings>
```

Setting the custom file will necessitate the Vertical SIP service, or the Wave system, being restarted. **However please note as the VPN tunnel is already established when this setting is picked up, the phones will need to be rebooted a second time to actually make this change active.**