Fix for lost nat-t internal firewall rule in VNS3 4.0-4.3.5

Cohesive Networks
Problem Remediation
Feb 2018

Situation

- Cohesive Networks has identified an issue that can affect site-to-site IPsec connections using "nat-traversal" (IPsec encapsulated over UDP 4500).
- The situation manifests itself with working site-to-site connections configured for nat-t that are working, suddenly lose connection, and do not recover even when restarting the tunnel or restarting the IPsec subsystem.
- In the tunnel logs you will see one of the following messages:
  - No response (or no acceptable response) to our first IKEv2 message
  - No response (or no acceptable response) to our first IKEv1 message
- A reboot will fix the situation, and you will see the site-to-site tunnels connect. However, the issue could recur unless the remediation steps following are taken.

Situation

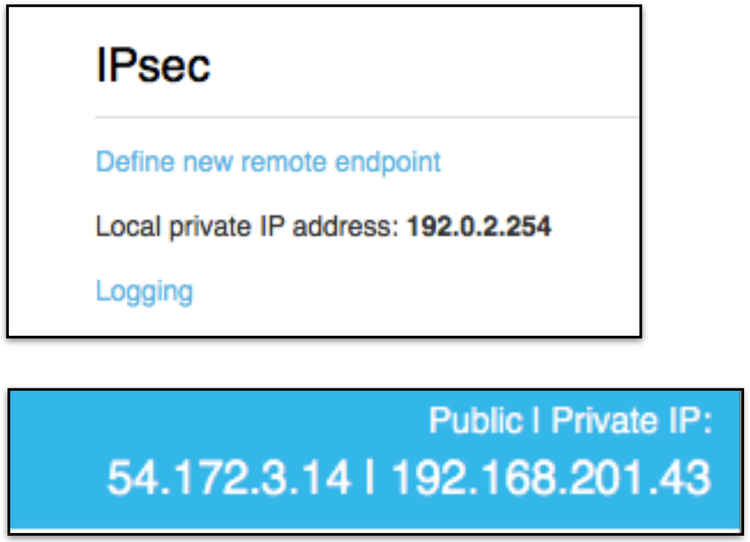
- The problem is caused by a bug that can cause the loss of an internal firewall rule used for nat-traversal configurations.
- The problem can occur when deleting NAT-T IPsec endpoints and/or editing the remote peer IP address of a NAT-T IPsec endpoint.
- Putting an equivalent rule to the one inadvertently lost into the VNS3 firewall for 4.0+ versions up through 4.3.5, solves the problem.
- VNS3 4.3.6+ does not have this issue.

FAQ

- **If all of my site-to-site connections are stable do I need to take any action?**
  No. If your connections are stable and you are not doing configuration modifications, you do not need to take action.
- **I just entered a new endpoint and am getting the error message "No response (or no acceptable response) to our first IKEv<1 or 2> message." Is this the problem you are describing?**
  Unlikely. If it is a new connection it is more likely that it is a "normal" initial configuration mismatch
- **Do I need separate firewalls rule for each of my endpoints defined?**
  No. The rule described supports all of your nat-t endpoints and replaces the missing internal rule.
- **Since you had a bug where the internal rule is lost, do I need to worry about the rule I enter into the customer firewall disappearing as well?**
  No. This rule is explicitly defined in the "customer" firewall and is not affected by any internal VNS3 processes.

Solution Detail: Controller Data Needed

- To create the firewall rule you will need two address values for your controller; "Local Private IP" and the "Private IP".
- The "Local Private IP" is found on the top of the "IPsec" page on the Web UI. The default value on a controller is 192.0.2.254, although it is often changed to the Controller's EIP, or another customer-defined value.
- The "Private IP" is on the top right of all of the Web UI pages. It corresponds to the cloud subnet IP of the VNS3 Controller. In this example it is 192.168.201.43.



Solution Detail: Firewall Rules Needed

- The "form" of the rules are:

  POSTROUTING_CUST -s <Controller Local Private IP> -p udp --sport 500 -j SNAT --to <Controller Private IP>:500
  and
  POSTROUTING_CUST -s <Controller Local Private IP> -p udp --sport 4500 -j SNAT --to <Controller Private IP>:4500

- In our example where the Local Private IP is 192.0.2.254 and the Private IP is 192.168.201.43, the rule is as shown below.

  POSTROUTING_CUST -s 192.0.2.254 -p udp --sport 500 -j SNAT --to 192.168.201.43:500
  POSTROUTING_CUST -s 192.0.2.254 -p udp --sport 4500 -j SNAT --to 192.168.201.43:4500

Solution Detail: Rules as entered in the VNS3 Firewall

Firewall

Custom firewall is activated.

Current firewall rules:

```
 pkts bytes target     prot opt in     out     source               destination
CHAIN POSTROUTING_CUST
    0     0 SNAT       udp  --  *      *       192.0.2.254          0.0.0.0/0           udp spt:500
to:192.168.201.43:500
    0     0 SNAT       udp  --  *      *       192.0.2.254          0.0.0.0/0           udp spt:4500
to:192.168.201.43:4500

Firewall SubGroup Display
```

Edit rules:

```
POSTROUTING_CUST -s 192.0.2.254 -p udp --sport 500 -j SNAT --to 192.168.201.43:500
POSTROUTING_CUST -s 192.0.2.254 -p udp --sport 4500 -j SNAT --to 192.168.201.43:4500
```

Save and activate

Conclusion

- Cohesive Networks regrets that this regression occurred as we transitioned to supporting native IPsec and NAT-T IPsec connections simultaneously on the same VNS3 Controller as part of the 4.x release.
- The firewall rule form provided in this document will fix a connection currently affected by this issue, and will prevent any future occurrence.
- VNS3 4.3.6 available the week of Feb 20th, 2018 does not have this issue. Release 4.3.6 also includes patches to protect against the Meltdown and Spectre exploits.

- If any additional questions or concerns please contact us at support@cohesive.net