Heitor Lessa

Random IT Tips

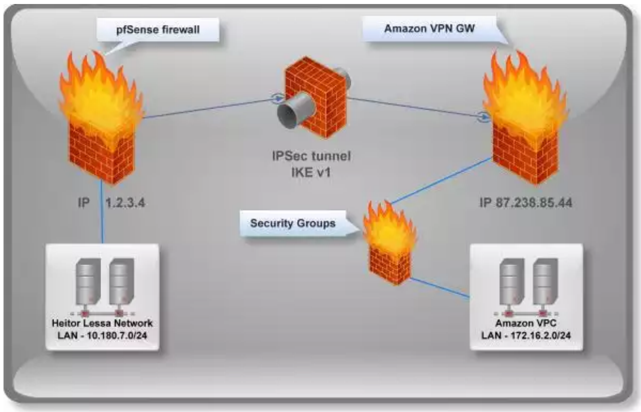
Site-to-site VPN pfSense and Amazon VPC

Posted by admin

*How to create a **Site-to-site VPN** between **pfSense** and **Amazon VPC** using **Virtual Private Gateway** feature.*

From here, I presume that you already know what is **pfSense** and **Amazon VPC**, however instead of creating an instance in **Amazon** and use an **IPsec** software, we will be using here a VPN Gateway in Amazon that can be created quite easily.

Basically, we will be setting up an **IPsec VPN** using **IKEv1** because IKEv2 its not supported by Amazon (learnt in the hardest way unfortunately), and this tunnel will share static routes. Follow below an image I created specifically for this article that will help you to have a better overview:

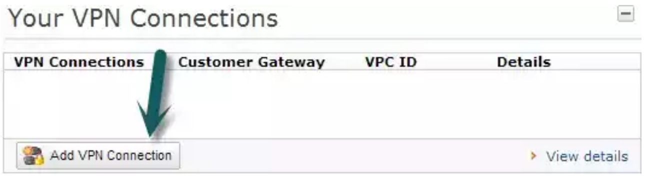


VPN overview

I would say this is a very straightforward and basic one which is really stable, however if you are looking for a **VPN** using **BGP** protocol with **pfSense –** check out this well written article.

Starting from scratch, we will need to create a **VPG in Amazon** as below:

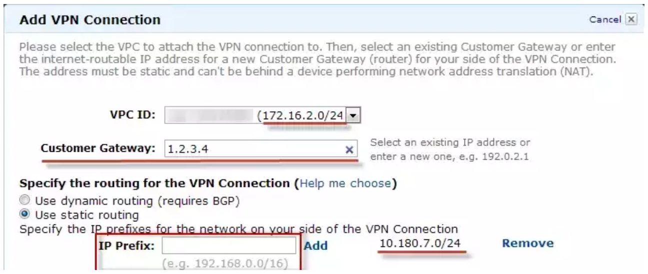
Go to your Amazon VPC dashboard and select the button **Add a VPN connection**


Your VPN Connections

VPN Connections	Customer Gateway	VPC ID	Details

pfSense Amazon VPC – New VPN connection

A new window will show up to fill out the a form as follow:



Add VPN Connection

Cancel ☒

Please select the VPC to attach the VPN connection to. Then, select an existing Customer Gateway or enter the internet-routable IP address for a new Customer Gateway (router) for your side of the VPN Connection. The address must be static and can't be behind a device performing network address translation (NAT).

VPC ID: [redacted] (172.16.2.0/24

Customer Gateway: 1.2.3.4 — Select an existing IP address or enter a new one, e.g. 192.0.2.1

Specify the routing for the VPN Connection (Help me choose)

○ Use dynamic routing (requires BGP)

● Use static routing

Specify the IP prefixes for the network on your side of the VPN Connection

IP Prefix: (e.g. 192.168.0.0/16) Add

10.180.7.0/24 Remove

pfSense Amazon VPC – Customer gateway and network

As you see, you firstly have to choose your VPC subnet (172.16.2.0/24 in this case), then **your external IP** in Customer Gateway, your LAN subnet (10.180.7.0/24) in **IP Prefix** and finally select **Add/Yes create** to finish the **VPN creation**.

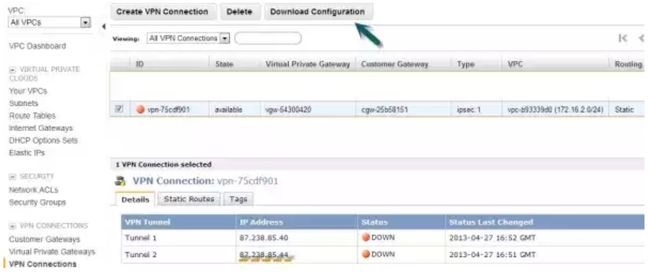
It will take few minutes to create the **VPN gateway** in Amazon and you should see the image below until complete.

Add VPN Connection

Creating your VPN Connection ...

pfSense Amazon VPC – Creating your VPN

Once completed, go to **VPN Connection** option in the left-side menu as shown:



	ID	State	Virtual Private Gateway	Customer Gateway	Type	VPC	Routing
☑	vpn-75cdf901	available	vgw-54300420	cgw-25b58151	ipsec.1	vpc-b93339d0 (172.16.2.0/24)	Static

1 VPN Connection selected

VPN Connection: vpn-75cdf901

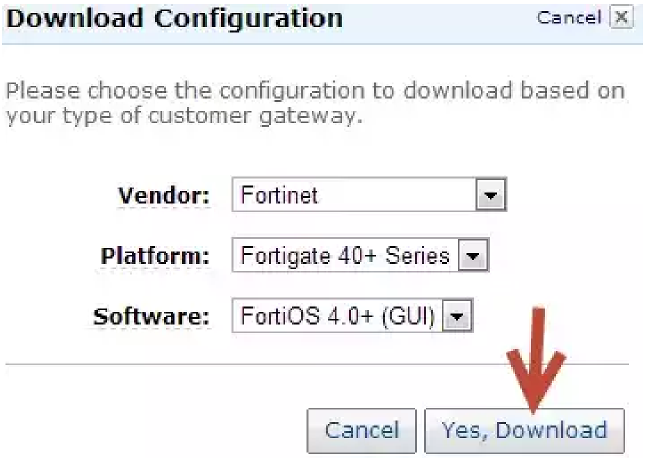
Details | Static Routes | Tags

VPN Tunnel	IP Address	Status	Status Last Changed
Tunnel 1	87.238.85.40	DOWN	2013-04-27 16:52 GMT
Tunnel 2	87.238.85.44	DOWN	2013-04-27 16:51 GMT

pfSense Amazon VPC – VPN connection

Note we have a button on top “Download configuration” and we also have two Tunnels, however Amazon does not offer a configuration file for pfSense. But the Phase1 and Phase2 settings will be default (until they change of course) for all **VPN**s created in **VPC**, apart of course the password and IPs. Also, we will be using the second tunnel as I had so much trouble (connection dropped very often) using the first one.

Download any configuration (we will be using Fortinet as an example) and get the password from there:



Download Configuration

Please choose the configuration to download based on your type of customer gateway.

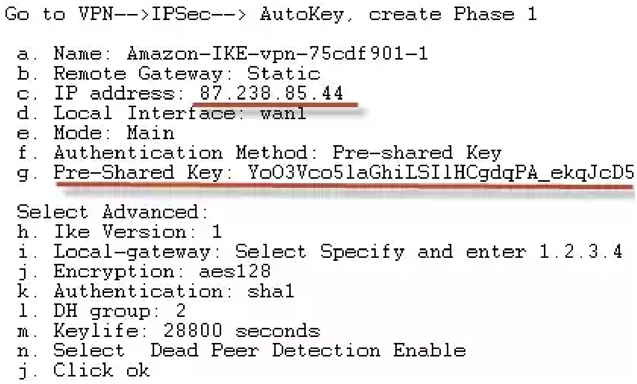
Vendor: Fortinet

Platform: Fortigate 40+ Series

Software: FortiOS 4.0+ (GUI)

pfSense Amazon VPC – Download VPC configuration

Open the text file downloaded previously and look for the **Pre-Shared key** in the **second peer** as shown below:

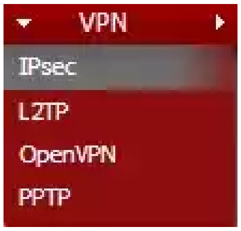


```
Go to VPN-->IPSec--> AutoKey, create Phase 1

 a. Name: Amazon-IKE-vpn-75cdf901-1
 b. Remote Gateway: Static
 c. IP address: 87.238.85.44
 d. Local Interface: wan1
 e. Mode: Main
 f. Authentication Method: Pre-shared Key
 g. Pre-Shared Key: YoO3Vco5laGhiLSIlHCgdqPA_ekqJcD5

 Select Advanced:
 h. Ike Version: 1
 i. Local-gateway: Select Specify and enter 1.2.3.4
 j. Encryption: aes128
 k. Authentication: sha1
 l. DH group: 2
 m. Keylife: 28800 seconds
 n. Select  Dead Peer Detection Enable
 j. Click ok
```

pfSense Amazon VPC – Pre-shared key

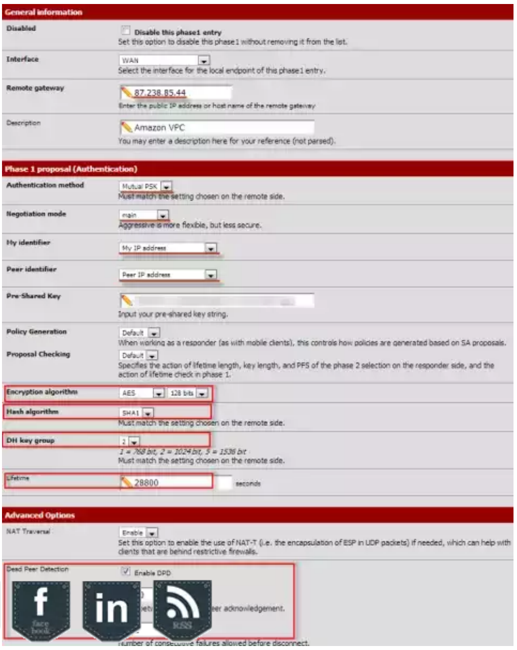
pfSense configuration

Open up your **pfSense** dashboard and go to **VPN – > IPsec**:



pfSense Amazon VPC
– IPsec option

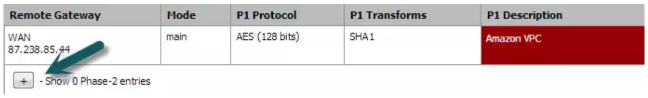
Then add a new Phase1 entry (clicking on button +) and fill out the **Phase1** as follows:



General information	
Disabled	□ **Disable this phase1 entry** Set this option to disable this phase1 without removing it from the list.
Interface	WAN Select the interface for the local endpoint of this phase1 entry.
Remote gateway	87.238.85.44 Enter the public IP address or host name of the remote gateway
Description	Amazon VPC You may enter a description here for your reference (not parsed).
Phase 1 proposal (Authentication)	
Authentication method	Mutual PSK Must match the setting chosen on the remote side.
Negotiation mode	main Aggressive is more flexible, but less secure.
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	 Input your pre-shared key string.
Policy Generation	Default When working as a responder (as with mobile clients), this controls how policies are generated based on SA proposals.
Proposal Checking	Default Specifies the action of lifetime length, key length, and PFS of the phase 2 selection on the responder side, and the action of lifetime check in phase 1.
Encryption algorithm	AES 128 bits
Hash algorithm	SHA1 Must match the setting chosen on the remote side.
DH key group	2 *1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit* Must match the setting chosen on the remote side.
Lifetime	28800 seconds
Advanced Options	
NAT Traversal	Enable Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
Dead Peer Detection	☑ Enable DPD er acknowledgement. Number of consecutive failures allowed before disconnect.

pfSense Amazon VPC – Phase1

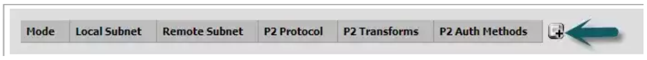
Once saved, expand the VPN configuration clicking in "+" and then create a new Phase2 entry as follows:



Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
WAN 87.238.85.44	main	AES (128 bits)	SHA1	Amazon VPC

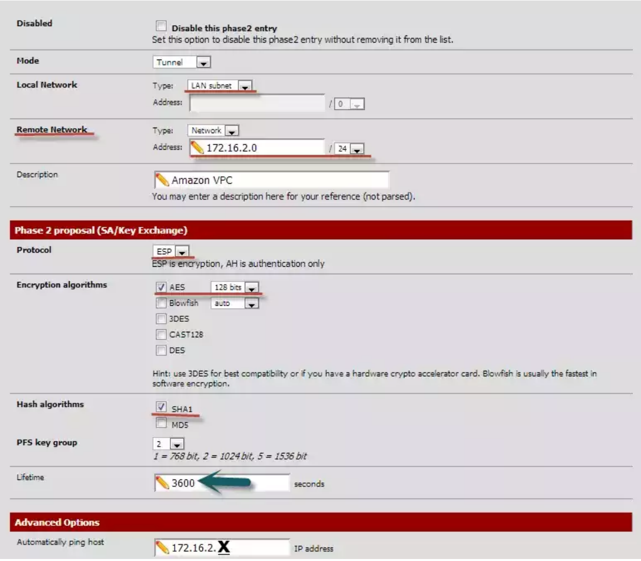
+ - Show 0 Phase-2 entries

pfSense Amazon VPC – Creating phase2



Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods

Fill out the form as follows:



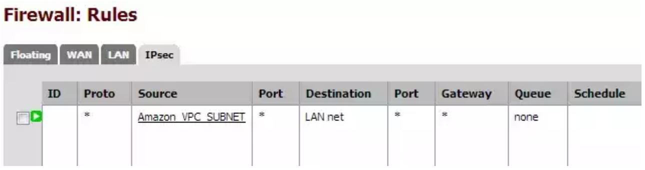
Disabled	□ **Disable this phase2 entry** Set this option to disable this phase2 entry without removing it from the list.
Mode	Tunnel
Local Network	Type: LAN subnet Address: / 0
Remote Network	Type: Network Address: 172.16.2.0 / 24
Description	Amazon VPC You may enter a description here for your reference (not parsed).
Phase 2 proposal (SA/Key Exchange)	
Protocol	ESP ESP is encryption, AH is authentication only
Encryption algorithms	☑ AES 128 bits □ Blowfish auto □ 3DES □ CAST128 □ DES Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator card. Blowfish is usually the fastest in software encryption.
Hash algorithms	☑ SHA1 □ MD5
PFS key group	2 *1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit*
Lifetime	3600 seconds
Advanced Options	
Automatically ping host	172.16.2.X IP address

pfSense Amazon VPC – Phase2

It's pretty much the same phase1 concerning Encryption and Hash algorithm, however note that we **Lifetime** has changed here**,** because all configuration must match in both sides (that's the way IPsec works).

Note in the last field "Automatically ping host" we have defined a 172.16.2.X which should be replaced to any host you have in Amazon, this keeps the tunnel UP and also brings the tunnel UP if there is any traffic.

Save and apply the changes in pfSense. By now, we have to configure a firewall rule under IPsec interface to allow traffic going through both ends. So, go to firewall -> Rules and then select IPsec interface there.



	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule
□		*	Amazon_VPC_SUBNET	*	LAN net	*	*	none	

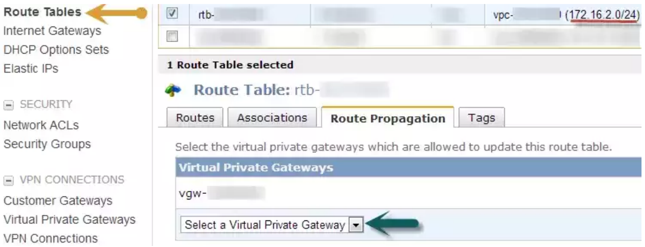
pfSense Amazon VPC – IPsec firewall rules

Basically, all you need to do is create a firewall rule allowing traffic from Amazon VPC Subnet (172.16.2.0/24) to your LAN subnet (10.180.7.0/24 in this case).

Amazon side

Briefly, we need to add a route to all our instances in that specific VPC subnet (172.16.2.0/24) and create a new rule in Security Group allowing traffic from our network.

Starting with routes, go to "Route tables" in the left-side menu, select **your subnet** (172.16.2.0/24 in this case), choose "Route propagation" option at the bottom, and then select your Virtual Private Gateway recently created. This will automatically create a route to your network in all instances that are in such subnet – It may take few minutes to propagate to all your instances.



☑	rtb-[redacted]	[redacted]	[redacted]	vpc-[redacted] (172.16.2.0/24)
□	[redacted]	[redacted]	[redacted]	[redacted]

1 Route Table selected

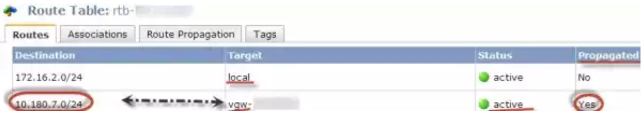
Route Table: rtb-[redacted]

Select the virtual private gateways which are allowed to update this route table.

Virtual Private Gateways
vgw-[redacted]
Select a Virtual Private Gateway ▾

pfSense Amazon VPC – Route table VPG

Choose then "Routes" option to see if your route was added correctly:



Route Table: rtb-[redacted]

Destination	Target	Status	Propagated
172.16.2.0/24	local	● active	No
10.180.7.0/24	vgw-[redacted]	● active	Yes

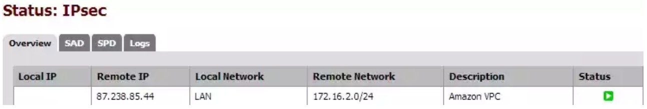
pfSense Amazon VPC – VPC routes

Note that we have two routes and two targets (Local|VGW), so we can confirm that our route was propagated to all instances in that VPC (Propagated = yes).

As a last thing, **don't forget** to update your Security Groups to allow traffic from your network 😉

Results

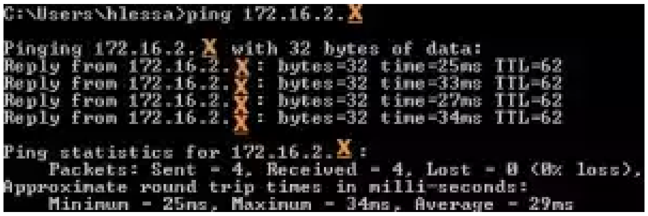
Check the VPN status on pfSense going to Status – > IPsec, if not connected you can do a ping from your machine to any machine in Amazon forcing any sort of traffic through the VPN:



Status: IPsec

Local IP	Remote IP	Local Network	Remote Network	Description	Status
	87.238.85.44	LAN	172.16.2.0/24	Amazon VPC	▶

pfSense Amazon VPC – Tunnel UP



```
C:\Users\hlessa>ping 172.16.2.X

Pinging 172.16.2.X with 32 bytes of data:
Reply from 172.16.2.X: bytes=32 time=25ms TTL=62
Reply from 172.16.2.X: bytes=32 time=33ms TTL=62
Reply from 172.16.2.X: bytes=32 time=27ms TTL=62
Reply from 172.16.2.X: bytes=32 time=34ms TTL=62

Ping statistics for 172.16.2.X:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 34ms, Average = 29ms
```

pfSense Amazon VPC – Ping results

In case your VPN is still down, look into IPsec logs (Status – > Logs – > IPsec) and look for error there – They are always very helpful. But even though you could not figure out by yourself, feel free to post a comment here and I would be grateful to help.

PS: If you are experiencing some packet fragmentation, consider tuning your MTU/MSS accordingly.

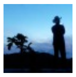
Stay connected to the next tip if you use SFTP.

April 27, 2013 **50** Replies

« Previous Next »

Leave a Reply

Enter your comment here...



Aidan on May 7, 2013 at 9:59 am

Isn't it easier to just use a client like ExpressVPN? (In case it's not a familiar app: https://expressvpn.biz). I'm not great with this stuff, but it looks like it will do the same thing, just with less work.

↪ Reply

admin on May 8, 2013 at 10:21 am

Hi Aidan,

Thanks for the feedback firstly.

Secondly, I have not heard about Express VPN at all, but I had a look at their website and understood how it works.

Express VPN would not do the same thing as we are dealing with Site-to-Site VPN which requires a permanent tunnel, and Express VPN is more Client-to-Site kind of VPN (great tool by the way).

Something similar could be made if we create an instance in Amazon and make such instance as a VPN Gateway (e.g OpenSWAN, Racoon, OpenVPN, etc), however it is not the best way to do as you would end up having a SPOF (Single point of Failure), and also would have to pay/maintain an instance just for this purposes.

As Amazon already supports and offers a VPN feature and we also have a UTM Firewall, VPN appliances, etc in our company, there is no need to create an extra instance for that.

Hope it clarifies a little bit 🙂

↪ Reply

Aidan on May 9, 2013 at 3:33 pm

Thanks, I think I get it, not sure what the setup effort would be, but I see how it could end up costing more.

↪ Reply

Pingback: Links 7/5/2013: Linux in Space | Techrights

Eduardo on May 20, 2013 at 8:09 pm

Hello Heitor,

Thank you for the tutorial. I'm having some trouble establishing the VPN, though.
Racoon logs the following:

```
racoon: DEBUG: getsainfo params: loc=’0.0.0.0/0' rmt=’0.0.0.0/0' peer=’amazon_ip’ client=’amazon_ip’
```

```
id=2
(…)
racoon: DEBUG: cmpid source: ‘my_internal_ip/mask’
racoon: DEBUG: cmpid target: ‘0.0.0.0/0’
racoon: DEBUG: check and compare ids : value mismatch (IPv4_subnet)
```

In other words, Amazon should be returning my internal IP address range, but instead it’s giving me ‘0.0.0.0’. I’m not even sure that’s allowed by the IPSec protocol.

I’ve found a lot of people complaining about this, both with Racoon and with OpenSwan.

That said, I’d like to ask: are you using Racoon with pfSense, or some other IPSec solution? Also, what’s your pfSense version?

Thank you very much,

Eduardo

↪ Reply

admin on May 20, 2013 at 11:10 pm

Hi Eduardo,

Thanks for you comment and I’m sorry to hear you are experiencing some problem with the VPN.

Would you mind posting a screenshot or more information about:

My identifier
Peer identifier

Local network
Remote network

In addition to this, could you also please post/attach (can be pastebin) Amazon configuration? If you are unsure how to do that, please refer to “Download configuration” button described above in the post.

As regards your questions, I do use Racoon (pfSense) and already used OpenSwan which also worked quite well.

That error in subject usually happens when Peer identifier/Remote network differs from the value entered in the other side. But post that information I asked previously and I will be more than happy to help.

Thank you

↪ Reply

Antonio on November 9, 2013 at 12:12 pm

“value mismatch” happens due to route propagation. You need either disable propagation at AWS side, or enable BGP at pfSense side.

↪ Reply

bob on May 21, 2013 at 1:27 am

thanks for the write up, i used it to successfully establish the connection (both AWS and pfSense show connection established)

however, i’m unable to ping the instance launched inside the VPC. i did a traceroute from my laptop on the LAN, it reaches the pfSense fw, then nothing, i dont see any blocks on the fw. is there a missing step showing how to add the route on the fw? what is Diagnotics -> Routing Table supposed to look like for this routing to this VPC?

↪ Reply

admin on May 22, 2013 at 9:44 pm

Hello Bob,

I am glad you liked and that somehow helped you.

I would advise to check the Security Groups of the instance you created, almost 100% sure that its blocking the traffic (which it does by default).

Have you succeeded propagating the route table to your instances?

Your pfSense routing table seems to be right, however as I said Security Group might be blocking the traffic, that’s why you can’t see anything – Unless the route propagation did not work or was missed, hence no instance will be to respond (route back).

Post your results thereafter, please.

↪ Reply

cmabastar-gumi on July 19, 2013 at 12:02 pm

whooooohoo!! thanks! PF SENSE rocks! Just some other tips.

DON’T USE PING TO TEST THIS!

↪ Reply

admin on July 27, 2013 at 11:17 pm

Hi,

Thanks for the comment 😉 It really makes me feel happy and keep up with all of this.

As regards to ping, I always use ping as first place if possible, but I do prefer to use a real TCP traffic (app, nc, iperf, whatever) for testing and measuring purposes.

🙂

↪ Reply

admin on July 27, 2013 at 11:17 pm

Hi,

Thanks for the comment 😉 It really makes me feel happy and keep up with all of this.

As regards to ping, I always use ping as first place if possible, but I do prefer to use a real TCP traffic (app, nc, iperf, whatever) for testing and measuring purposes.

🙂

↪ Reply

Nick McEwen on August 13, 2013 at 1:56 am

Hi Heitor,
I have been searching for a lower cost solution to connect a site to VPC that dont have expensive hardware ie cisco etc.. So I tried OpenVPN but had issues with routing and was unable to get it to work, this wasnt preferred anyhow but after reading your article I will give this a shot and fingers crossed routing will be all good. 🙂 thanks for sharing!

Nick

↪ Reply

Chris on August 13, 2013 at 10:58 pm

Thanks for this useful guide. I had more than a couple hiccups moving from a job where all my VPC VPN connections were handled by hardware firewalls to a shop where pfsense was the primary router at office branches. This post helped me fix the couple mistranslations I had between the downloaded Amazon config and what pfsense needed to get going.

My only question after this, though, is something you allude to briefly in the text and then don’t come back to: What's the best procedure to set up the second connection on pfsense? If I just create a second IPSec entry, with the same destination network, will pfsense load balance between the two, use one as a failover, or get confused and take a lunch break? I am not familiar with pfsense's architecture to guess its behavior.

↪ Reply

Chris on August 13, 2013 at 11:45 pm

Per my own testing: Pfsense is aggressive about timing out and shutting down the IPSec connections. It will bring up either of them as needed, but doesn't appear to bring up a second unless the first has trouble. The order seems random.

↪ Reply

---

admin on August 14, 2013 at 6:27 pm

That's the right behavior.

Amazon does not allow the second tunnel to be up, no matter how you configure you will never get both UP and working fine.

So, in one of my customers I have other tunnel configured however it only brings up when the other one fails completely. It also took me a while to figure out this after also testing with different hardwares (Cisco, Juniper, etc).

↪ Reply

Nick McEwen on August 15, 2013 at 10:38 pm

Woohoo! it works! To my surprise the tunnel is up. and i can ping the servers from my local network to the amazon servers on the other side and remote desktop to them also. but i do have one issue I cannot figure out; when i try to ping my local network from the amazon servers it fails. I performed a tracert and found the trace first hop is the amazon VGW 169.254.247.9 then the second hop is 169.254.247.5 which is the other end of the tunnel but then the hops that follow are timing out? I thought it must be the firewall from the local network but looking at the FW logs i cant see any traffic hitting it?is there any particular ports i should be opening?

Thanks
Nick

↪ Reply

Nick McEwen on August 15, 2013 at 10:39 pm

just correcting my email

Reply

admin on August 16, 2013 at 11:23 am

Hello Nick !

I'm glad you got it working, and issues that may arise are really good, trust me ! They will make you think out of the box once again to rule out, and that it will make you a better troubleshooter 😉

As regards to this issue, the best thing to do is having a sniffer between both machines you are trying to reach, and then the firewall until you get closer.

However, it's a little bit odd that you can reach but Amazon instances can't.. so a couple of questions that may help you out:

1. Have you checked routing table in Amazon VPC? Not from the instance, but the routing table that it propagates to all instances
2. What's the local/remote network in your VPN? Does that allow your whole subnet or is it a super net?

Reply

Nick McEwen on August 19, 2013 at 2:23 am

Hi,

1. Yes i have checked the routing table in the vpc and this is directing traffic out the VGW as expected
2. local 192.168.1.0 and remote 10.0.0.0 with the inside VPN being a 169 address that is assigned by amazon.

I have made some developments with the VPN and i can now see ICMP traffic hitting the pfsense WAN interface. if i look in the logs under Status > System Logs > Firewall I can see the Source IP 10.0.0.237 ICMP to destination 192.168.1.2 I am unfamiliar with the pfsense GUI but I am assuming the firewall is passing the traffic through because under Firewall > Rules I have allows all traffic to pass as per your above article.
However even though I can see the traffic hitting the pfsense firewall the ping is "timed out" on 10.0.0.237.
would the Firewall be blocking the traffic? How can i tell?

Thank you 🙂

Nick

Reply

admin on August 19, 2013 at 8:57 pm

Hi Nick,

I'm glad you made some improvements and is getting almost there.

Unfortunately I don't have access to any pfSense close to me right now, and I will have one next week only maybe.

But if you look at the Firewall Logs and can see traffic there, you should be able to note if there is a green or red button indicating if the traffic was blocked or accepted.

If you are still unable to see that for some reason, you can look for the TCP Flags in the logs like R, F, etc (Reset and Fin) to understand that further.

However, if you somehow can't see both of them, you still have the ability to run a sniffer in pfSense via command line or via GUI (Packet capture), then you will be able to see all flags and traffic behaviour.

Sometimes your firewall is passing the traffic correctly, but your machine is not able to respond that (maybe a local firewall blocking, wrong gateway or OS misconfiguration). Can you also test using a TCP port rather than ICMP only?

Reply

Nick McEwen on August 21, 2013 at 2:08 am

Hi again,

I think the issue i am having is routing on the PFsense. If i look on the FW logs I can see the traffic coming in from amazon in the firewall logs but i dont think pfsense is routing to my 192.168.1.0 network. If i use the tools on PFsense like nslookup or ping and try to ping a local address it fails 🙁
I failed to mention earlier that my WAN interface is actually behind my hardware firewall and I am forwarding traffic on specific ports through to the WAN int of the pfsense.

Nick McEwen on August 21, 2013 at 2:14 am

Sorry the pfsense diag ping and dns lookup are now working. however still the same issue and i am unable to ping from the amazon servers (times out on the AWS server, but i can see the ICMP traffic hitting the pfsense firewall).

admin on August 22, 2013 at 6:03 pm

Hi Nick,

That's an important point that you forgot to point out.

As you have internal addresses and not a proper WAN in your pfSense, you have to enable an option (I think it is under Advanced options) called:

Bypass firewall rules for traffic on same interface

Check this out immediately, and also if it is possible upload a packet capture file to CloudShark.org from:

1 – Host from Amazon AWS
2 – pfSense
3 – Your internal host

So, I can help you further on this – please make sure you have ICMP packets and another traffic like HTTP (you can use netcat or anything for sockets).

↪ Reply

Mike on October 17, 2013 at 11:12 pm

Thank you for the great tutorial. I have my tunnel working and I can talk to my instance in my VPC (ping back and forth). However, I would like to route all of my traffic over the IPSec tunnel through the VPC and out to the internet. I read on the tubes that policy-based routing is accomplished via the phase2 config for IPSec. However, things break if I specify the remote net (VPC) as 0.0.0.0/0. or have 0.0.0.0/0 as a second phase2 definition. Any tips on how to setup policy-based routing via VPC?

I was able to accomplish this using OpenVPN via an EC2 instance by creating pfSense gateway definitions based on the OpenVPN interface that was created. However, it seems more complicated for policy-based routing for IPSec and especially when you involve Amazon's VPC.

Thanks in advance.

Mike

↪ Reply

admin on October 19, 2013 at 4:25 pm

Hello Mike,

I'm glad you got it working using this tutorial.

As regards to your question, that's the expected behaviour because Amazon VPC devices make use of Route-based rather than policy-based VPN (i.e Cisco ASA), that's why some people run into loads of problems while configuring due to this requirements.

In order to achieve that, you will need to create a route and then send all your traffic to the tunnel, but if you want to share your goals with me we can find a better solution to achieve that 🙂

↪ Reply

Mike on October 20, 2013 at 7:05 am

Heitor,

I had two goals; one, was to determine if VPC offered better network latency than EC2 classic, and two, to familiarize myself with Amazon's VPC.
I finally accomplished my goal (route all home traffice bound for Internet over my VPC IPSec VPN and out the internet. However, it's a bit of a hack. I reconfigured my IPSec VPN on my side to only send traffic to one of my VPC EC2 instances (192.168.40.169). Then I setup a OpenVPN from my home home network to 40.169 and 40.169 NATs my traffic and sends it out over the public IP assigned to my EC2 instance inside my VPC. Essentially I have an OpenVPN running inside a IPSec VPN.
I now this is crazy and I expected the network performace to be crap, but it's actually very good. Before when I used OpenVPN to my EC2 classic instance, I could never get better than 200ms ping times to anywhere and could never exceed 5Mbps download speeds (my cable connection is 30Mbps down/5Mbps up). Also, EC2 classic had five (5) additional hops on it's internal 10.x network before reaching the internet. Now with the VPC with double VPN'd tunnel, I am able to saturate my cable speeds, get great ping times (40ms) to places like Google (8.8.8.8) and only have two hops before getting to the internet.
For the record both my EC2 Classic and EC2 VPC instances are in the Oregon West 2a zones.
I would still like to figure out how to remove OpenVPN from the equation and only have IPSec involved.

Mike

↪ Reply

admin on October 20, 2013 at 6:47 pm

Hello Mike,

I'm glad you are discovering more and more how to use AWS.. I've actually sent you an invite for a

Workshop that I presented yesterday, but I will do a public one and send you an invite days before to not be in a rush, Of course if you are interested in (it's free by the way).

As regards to your setup.. I'd say that you don't need an OpenVPN software to do that, because if I understood perfectly, you are doing the following traffic flow:

Home home network -> VPC VGW (tunnels) –> NAT instance (OpenVPN) –> Internet

As you thought correctly, all you need is an instance to play NAT role, however I've been thinking if you could use your VPC IGW (Internet Gateway) to route your traffic to, however you will need to play with your routing tables to make sure you have a route back. It's an interesting idea though.

But in most case scenarios, you will have to use a NAT instance (disabling source/destination check, using ip_forward+iptables). Give a try and come back with the results.. I will play around with this week maybe 🙂

↪ Reply

saravana kumar on December 12, 2013 at 4:17 am

It helped! Thanks for writing this up!

↪ Reply

admin on December 14, 2013 at 1:33 pm

Thank you Savarana,

It always makes me glad when someone take time to leave a comment as this is a sort of fuel to keep writing new articles, etc.

Thanks a lot.

↪ Reply

Michael Lindsay on January 10, 2014 at 6:23 pm

Hi Heitor,

Great article, got us up and running. However, our tunnel connection drops constantly. We've been working with the Amazon techs and, while they don't have experience with pfsense, they did look at our configuration and they said everything looks fine. The fundamental issue seems to be that they are closing the connection because, from their network's point of view, there is no interesting traffic. Their recommendation to have our networking keep a running ping to one of our EC2 instance has no effect.

Furthermore, we have a secondary gateway configured to fail over to and when it tries we get a lot of this: unknown Informational exchange received, and then this: phase2 negotiation failed due to time up waiting for phase1.

I have quadruple checked the only difference between the two gateways for all phases is the ip address and the pre shared keys.

↪ Reply

admin on January 12, 2014 at 7:51 am

Hi Michael,

Thanks for the feedback.

I've seen this before and it was all caused by DPD due to some glitches that happens, so DPD set to 3 it's not enough, so increasing that it's more likely to help you there.

As pfSense can work well with BGP and you require HA, I wouldn't advise on having this VPN setup as Static routing but Dynamic Routing to provide you more HA features.

Feel free to reach me out on e-mail as this requires some sensitive info.

↪ Reply

Johan Grundström on February 12, 2014 at 12:39 pm

Hi!
Thanks for a great instruction! I got the VPN working in no time. I also tweaked it a bit to my usage with other IPs than the default VPC.

All is working great except DNS in the IPSEC subnet.

I can't figure out what I missed.

I use route53. All my external IPs resolve fine. My internals IPs give host unknown and don't resolve. If I ping the IP's directly it works fine. Just DNS messing with me.

What could I have missed?

↪ Reply

Johan Grundström on February 13, 2014 at 5:51 pm

After further investigation I found the reason for the problem. The DNS internal IP number in the resolver log shows:

```
dnsmasq[82944]: possible DNS-rebind attack detected
```

So basically it has nothing to do with the VPN tunnel. But with pfsense and DNS-rebind attack protection. For now until I figure out a good way how to accept my internal IPs I have disabled DNS-rebind protection. Anybody know a better way to fix this? 🙂

// Johan

Reply

admin on February 15, 2014 at 11:45 am

Hi Johan,

I'm glad you've figured that out and sorted out temporarily, and I'm also glad that you found the article helpful… I'm trying to find some time between my new projects and this Website, so I can publish 3 more articles that I have reserved, specially pfSense as an EC2 instance.

This is normal due to these rebindings, however rather than disabling that you can also add the hostnames you want to be ignored (sort of Whitelist):

https://forum.pfsense.org/index.php?topic=42733.0

But as you grow you may find this task terribly hard, so you may end up creating your own script solution for that OR by simply disabling that at this stage, unfortunately =/

Reply

Brent Boecking on May 28, 2014 at 9:09 pm

I noticed you posted on a blog entry for PFSense as an AMI within AWS. You mentioned that you were able to get PFSense running on a m1.small instance. Can you publish your AMI? Or, any helpful hints on getting it to work. I currently have PFSense firewalls at all my locations and I am not excited to use AWS's VPN service. Thanks.

Reply

admin on May 30, 2014 at 5:29 pm

Hi Brent,

I'm terribly sorry for the late response, been sidetracked in several things here, and finally got a new laptop.

Yes, I indeed got it working in a smaller instance but still being masqueraded as 'Windows' platform. Let me know if you are still after this, so I can tell you the procedure as I couldn't publish the AMI publicly.

↪ Reply

Brent on June 2, 2014 at 4:11 am

It is really the only thing that is keeping me from moving a bunch of my business apps to aws. With general inquiries like this, I rarely get a response anyway – no worries about timeliness. Any help you could give would be greatly appreciated.

↪ Reply

admin on June 2, 2014 at 4:39 pm

Hi Brent,

You can 'reduce' the instance size by launching a new instance from the AMI provided in that list, and then you create a new AMI from the instance you've just launched (pfSense).

Once you go again to launch a new instance you will notice that there's no limitation since metadata is different, and then you can now create as m1.small.

I've sent you an e-mail saying exactly the same.

↪ Reply

Frank on June 27, 2014 at 9:18 pm

Hi Heitor,

Thanks a lot for the tutorial! I followed your instructions. I can see one of the two tunnels at VPC is up, which is a good sign. Unfortunately, I cannot ping the VPC machines from my LAN. I added security groups to allow all traffic, but without luck. Enclosed please find the log of my ipsec (192.168.2.0 is my local subnet while 10.0.0.0 and 10.0.1.0 are the VPC subnets):

```
Jun 27 19:33:29 racoon: INFO: Reading configuration from "/var/etc/ipsec/racoon.conf"
Jun 27 19:33:29 racoon: [Self]: INFO: MY_PUBLIC_IP[4500] used for NAT-T
Jun 27 19:33:29 racoon: [Self]: INFO: MY_PUBLIC_IP[4500] used as isakmp port (fd=9)
Jun 27 19:33:29 racoon: [Self]: INFO: MY_PUBLIC_IP[500] used for NAT-T
Jun 27 19:33:29 racoon: [Self]: INFO: MY_PUBLIC_IP[500] used as isakmp port (fd=10)
Jun 27 19:33:32 racoon: INFO: unsupported PF_KEY message REGISTER
Jun 27 19:33:32 racoon: INFO: unsupported PF_KEY message REGISTER
Jun 27 19:34:24 racoon: [VPC Tunnel 2]: INFO: IPsec-SA request for VPC_PRIMATE_GW_IP queued due to no phase1 found.
Jun 27 19:34:24 racoon: [VPC Tunnel 2]: INFO: initiate new phase 1 negotiation:
```

```
MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:34:24 racoon: INFO: begin Identity Protection mode.
Jun 27 19:34:24 racoon: INFO: received Vendor ID: DPD
Jun 27 19:34:24 racoon: [VPC Tunnel 2]: INFO: ISAKMP-SA established MY_PUBLIC_IP[500]-
VPC_PRIMATE_GW_IP[500] spi:8da4d35672f54abe:38a6e904a9d065d4
Jun 27 19:34:25 racoon: [VPC Tunnel 2]: INFO: initiate new phase 2 negotiation:
MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:34:26 racoon: [VPC Tunnel 2]: INFO: IPsec-SA established: ESP MY_PUBLIC_IP[500]-
>VPC_PRIMATE_GW_IP[500] spi=243993175(0xe8b0a57)
Jun 27 19:34:26 racoon: [VPC Tunnel 2]: INFO: IPsec-SA established: ESP MY_PUBLIC_IP[500]-
>VPC_PRIMATE_GW_IP[500] spi=3243902346(0xc15a058a)
Jun 27 19:51:34 racoon: INFO: unsupported PF_KEY message REGISTER
Jun 27 19:51:34 racoon: ERROR: pfkey DELETE received: ESP MY_PUBLIC_IP[500]-
>VPC_PRIMATE_GW_IP[500] spi=3243902346(0xc15a058a)
Jun 27 19:51:34 racoon: ERROR: no iph2 found: ESP VPC_PRIMATE_GW_IP[500]->MY_PUBLIC_IP[500]
spi=243993175(0xe8b0a57)
Jun 27 19:51:34 racoon: INFO: unsupported PF_KEY message REGISTER
Jun 27 19:51:34 racoon: ERROR: such policy already exists. anyway replace it: 192.168.2.0/24[0]
10.0.0.0/24[0] proto=any dir=out
Jun 27 19:51:34 racoon: ERROR: such policy already exists. anyway replace it: 10.0.0.0/24[0]
192.168.2.0/24[0] proto=any dir=in
Jun 27 19:54:29 racoon: [VPC Tunnel 2]: INFO: respond new phase 2 negotiation:
MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:54:29 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:29 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:29 racoon: [VPC Tunnel 2]: [VPC_PRIMATE_GW_IP] ERROR: failed to pre-process ph2
packet [Check Phase 2 settings, networks] (side: 1, status: 1).
Jun 27 19:54:34 racoon: [VPC Tunnel 2]: INFO: respond new phase 2 negotiation:
MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:54:34 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:34 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:34 racoon: [VPC Tunnel 2]: [VPC_PRIMATE_GW_IP] ERROR: failed to pre-process ph2
packet [Check Phase 2 settings, networks] (side: 1, status: 1).
Jun 27 19:54:44 racoon: [VPC Tunnel 2]: INFO: respond new phase 2 negotiation:
MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:54:44 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:44 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:44 racoon: [VPC Tunnel 2]: [VPC_PRIMATE_GW_IP] ERROR: failed to pre-process ph2
packet [Check Phase 2 settings, networks] (side: 1, status: 1).
Jun 27 19:54:54 racoon: [VPC Tunnel 2]: INFO: respond new phase 2 negotiation:
MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:54:54 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:54 racoon: ERROR: failed to get sainfo.
Jun 27 19:54:54 racoon: [VPC Tunnel 2]: [VPC_PRIMATE_GW_IP] ERROR: failed to pre-process ph2 packet [Check Phase 2 settings, networks] (side: 1, status: 1).
Jun 27 19:55:04 racoon: [VPC Tunnel 2]: INFO: respond new phase 2 negotiation: MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:55:04 racoon: ERROR: failed to get sainfo.
Jun 27 19:55:04 racoon: ERROR: failed to get sainfo.
Jun 27 19:55:04 racoon: [VPC Tunnel 2]: [VPC_PRIMATE_GW_IP] ERROR: failed to pre-process ph2 packet [Check Phase 2 settings, networks] (side: 1, status: 1).
Jun 27 19:55:14 racoon: [VPC Tunnel 2]: INFO: respond new phase 2 negotiation: MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 19:55:14 racoon: ERROR: failed to get sainfo.
Jun 27 19:55:14 racoon: ERROR: failed to get sainfo.
Jun 27 19:55:14 racoon: [VPC Tunnel 2]: [VPC_PRIMATE_GW_IP] ERROR: failed to pre-process ph2 packet [Check Phase 2 settings, networks] (side: 1, status: 1).
Jun 27 19:58:21 racoon: INFO: unsupported PF_KEY message REGISTER
Jun 27 19:58:21 racoon: INFO: unsupported PF_KEY message REGISTER
Jun 27 20:01:17 racoon: [VPC Tunnel 2]: INFO: initiate new phase 2 negotiation: MY_PUBLIC_IP[500]VPC_PRIMATE_GW_IP[500]
Jun 27 20:01:17 racoon: [VPC Tunnel 2]: INFO: IPsec-SA established: ESP MY_PUBLIC_IP[500]->VPC_PRIMATE_GW_IP[500] spi=226370070(0xd7e2216)
Jun 27 20:01:17 racoon: [VPC Tunnel 2]: INFO: IPsec-SA established: ESP MY_PUBLIC_IP[500]->VPC_PRIMATE_GW_IP[500] spi=1975333550(0x75bd32ae)
```

Could you please help me find what I am missing?

Really appreciate your help!

Frank

↪ Reply

Heitor Lessa on June 28, 2014 at 11:01 pm

Hi Frank,

Firstly, thanks for the feedback 🙂

Secondly, it's a bit hard to tell you where the problem is without seeing Routing Table from both sides (your VPC and your on-premise pfSense).

However, I can give you some tips on where to start troubleshooting this issue:

– As per its logs, your VPN itself looks fine as it could establish Phase1&Phase2 just fine
— But as you have 2 VPC Subnets, you shouldn't use 10.0.0.0/24, otherwise you won't be able to access both but only one
— For this reason, change this 10.0.0.0/24 to /16 which then covers the entire VPC CIDR

– Apart from that, have you created a Static Route under your VPN Connections – your VPN – > Static Routes, defining your local subnet 192.168.2.0/24?
— If so, make sure you then enabled Route Propagation under your Route Table in your VPC instead of adding a Static Route
— Once you enabled Route Propagation it will automatically propagate to all your instances across your VPC Subnets, which mean that all traffic should return to your Office through the VPN.

Please let me know the outcome after checking these points

Reply

Frank on July 14, 2014 at 2:33 pm

Hi Heitor,

What you said works like a charm! Thank you so much!!!

Frank

Reply

Oliver on August 25, 2014 at 8:42 am

Hi, Heitor,

Wonderful tutorial.

However, I'm having a problem on my vpn tunnel connectivity going to VPC with this error.

racoon: [onvolo_vpc]: [VPC_tunnel_IP] ERROR: phase2 negotiation failed due to time up waiting for phase1 [Remote Side not responding]. ESP VPC_tunnel_IP[0]->PFSENSE_WAN_IP[0]

Appreaciate your help. Thanks!

Oliver

Reply

Jim Thompson on August 29, 2014 at 11:53 pm

There is now a VPC wizard in pfSense® version 2.1.5, for hardware purchased via the pfSense store (http://store.pfsense.org) or Netgate® (http://store.netgate.com).

More details can be found here: https://forum.pfsense.org/index.php?topic=81113.0

Reply

Wayne on September 30, 2014 at 12:53 am

Thanks a lot. Got the site here working perfectly. we have a Cisco Firewall performing a tunnel to one VPC account, and now use PFSense for a second VPC Account as we found a bunch of problems connecting two Amazon VPCs to the same location from the same region (so really the pfsense is only to use a different public facing IP).
You saved my bacon sir!

↪ Reply

Pingback: How To Fix Tunnel Creation Error In Vpn in Windows

Joseph Jozwik on January 22, 2015 at 4:25 am

Hello,
Thank you for work documenting the tutorial.
I have the IPsec tunnel connected to my VPC. I have a slightly different setup as my pfsense box is also behind another nat. I can connect with no problem from within the AWS VPC to the Local network behind pfsense. But when I attempt to connect from the local network to the AWS VPC is just hangs forever.

It seems like the it doesn't have a good route, it is attempting to route the private VPC subnet over the default route for the pfsense box and not the tunnel.

Have a setting "In case you need NAT/BINAT on this network specify the address to be translated " not sure how that is used, or do I need to create security group rules.

For security groups would that just be the local private network subnet or some other identifier?

↪ Reply

admin on April 3, 2015 at 7:36 pm

Hi Joseph,

Apologies for the delay in responding as I've changed my role recently and have been extremely busy on it lately which sidetracked me from my personal projects.

Having a NAT is something complicated when trying to work with Hardware VPN in Amazon due to lack of NAT-T, where you can get it working using some workarounds but the overall solution can get either too complex or hard to maintain based on my experience.

The best in this situation is to always use a tcpdump in both places and check how the packets are arriving and very likely you will find out that the Source IP address that your VPC knows (route table wise) is not the one all your VPC instances know that traffic should be routed through the

VPN (VGW).

In this case you can solve the issue by having a tcpdump running, getting the right IP/IP range and setting that in VPN -> VPN Connection you have -> Static Route, then you have to make sure Route propagation is enabled under your Route table (which is attached to your Subnet). This will will force all your traffic to that IP/IP Range to go through the tunnel where your pfSense/on-premise gateway will have to handle it, which in fact will not go through VPC Default gateway (First IP of your VPC CIDR) as you're describing it.

Let me know if you still need some help on this

↪ Reply

Joe on March 23, 2015 at 11:20 am

Hi there, thanks for the post but I seem to be having trouble too.
The tunnel is up and running, but I cannot ping the clients in the VPC.

I have checked and re checked my firewall rules and the VPC settings but I am stuck.

I am also thinking of starting from scratch and using OpenBGPD, but I'd rather not since I seem to be close to getting it working.

Any help would be appreciated.

↪ Reply

---

admin on April 3, 2015 at 7:25 pm

Hi Joe,

I guess you've probably opened a ticket with AWS Support and they may have helped you already as it happened with others who commented here.

In terms of Routing problems, I'd need some extra info to help you there so feel free to email me directly (heitor . lessa at hotmail . com) and please provide some IP ranges (source/destination), screenshots (VPN config, VPC Routing table, SG, NACL, etc) so that I can help you better.

What I can say from now is that the most common issue in VPNs like that are the Routing Table in the VPC that may not have 'Propagation' enabled and hence your VPC instance doesn't know how to reply back through the tunnel (VGW). If you add that manually instead of going to VPN -> Static Route and have Propagation under Route table enabled, that will not work no matter how much you check your FW/SG/VPN settings.

Try using Tcpdump/Wireshark and filter for ICMP and try a simple ping to confirm if at least the packets are arriving and if they are possibly NATed…

Give me a shout if you are still in need of help here

Reply

Pages

About
Contact

View Full Site