Atlantic.Net Blog

How to Install and Configure strongSwan VPN on Ubuntu 18.04

July 8, 2020 by Hitesh Jethva (https://www.atlantic.net/author/hitesh-jethva/) (64posts)

under VPS Hosting (https://www.atlantic.net/category/vps-hosting/)

0 Comments (https://www.atlantic.net/vps-hosting/how-to-install-and-configure-strongswan-vpn-on-ubuntu-18-04/#disqus_thread)

A VPN allows you to access the Internet safely and securely on an untrusted public Wi-Fi network. You can connect to remote VPN servers using the encrypted connection and surf the web anonymously.

strongSwan is free, open-source, and the most widely-used IPsec-based virtual private network implementation, allowing you to create an encrypted secure tunnel between two or more remote networks.

strongSwan uses the IKEv2 protocol, which allows for direct IPSec tunneling between the server and the client. strongSwan stands for Strong Secure WAN and supports both versions of automatic keying exchange in IPsec VPN, IKE V1 and V2.

In this tutorial, we will show you how to install and configure strongSwan VPN on Ubuntu 18.04.

Prerequisites

- A fresh Ubuntu 18.04 VPS (https://www.atlantic.net/vps-hosting/) on the Atlantic.Net Cloud Platform.
- A root password configured on your server.

Step 1 – Create an Atlantic.Net Cloud Server

First, log in to your Atlantic.Net Cloud Server (https://cloud.atlantic.net/?page=userlogin). Create a new server (https://www.atlantic.net/cloud-hosting/how-to-create-new-atlantic-net-cloud-server/), choosing Ubuntu 18.04 as the operating system with at least 1GB RAM. Connect to your Cloud Server via SSH and log in using the credentials highlighted at the top of the page.

Once you are logged in to your Ubuntu 18.04 server, run the following command to update your base system with the latest available packages.

```
apt-get update -y
```

Step 2 – Enable Kernel Packet Forwarding

First, you will need to configure the kernel to enable packet forwarding for IPv4. You can configure it by editing the file /etc/sysctl.conf:

```
nano /etc/sysctl.conf
```

Add the following lines at the end of the file:

```
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

Save and close the file. Then, run the following command to reload the settings:

```
sysctl -p
```

Step 3 – Install strongSwan

First, you will need to install the strongSwan IPSec daemon in your system. You can install it by simply running the following command:

```
apt-get install strongswan libcharon-extra-plugins strongswan-pki -y
```

Once the installation is completed, you can proceed to the next step.

Step 4 – Setting Up a Certificate Authority

Now you will need to generate the VPN server certificate and key for the VPN client to verify the authenticity of the VPN server.

First, generate a private key for self-signing the CA certificate using a PKI utility:

```
ipsec pki --gen --size 4096 --type rsa --outform pem > ca.key.pem
```

Next, create your root certificate authority and use the above key to sign the root certificate:

```
ipsec pki --self --in ca.key.pem --type rsa --dn "CN=VPN Server CA" --ca --lifetime 365
```

Next, you will need to create a certificate and key for the VPN server so that the client can verify the server's authenticity using the CA certificate we just generated.

First, create a private key for the VPN server with the following command:

```
ipsec pki --gen --size 4096 --type rsa --outform pem > server.key.pem
```

Next, generate the server certificate by running the following command:

```
ipsec pki --pub --in server.key.pem --type rsa | ipsec pki --issue --lifetime 2750 --ca
```

Next, you will need to copy the above certificate in the respective IPSec certificates directories as shown below:

```
mv ca.cert.pem /etc/ipsec.d/cacerts/
mv server.cert.pem /etc/ipsec.d/certs/
mv ca.key.pem /etc/ipsec.d/private/
mv server.key.pem /etc/ipsec.d/private/
```

At this point, you have all of the certificates ready, and you can now proceed to the next step.

Step 5 – Configure strongSwan

strongSwan has a default configuration file located at /etc/ipsec.conf. It is recommended to rename the default configuration file and create a new file.

To rename the default configuration file, run the following command:

```
mv /etc/ipsec.conf /etc/ipsec.conf.bak
```

Next, create a new configuration file as shown below:

```
nano /etc/ipsec.conf
```

Add the following lines:

```
config setup
        charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2, mgr 2"
        strictcrlpolicy=no
        uniqueids=yes
        cachecrls=no

conn ipsec-ikev2-vpn
      auto=add
      compress=no
      type=tunnel  # defines the type of connection, tunnel.
      keyexchange=ikev2
      fragmentation=yes
      forceencaps=yes
      dpdaction=clear
      dpddelay=300s
      rekey=no
      left=%any
      leftid=@vpn.example.com    # if using IP, define it without the @ sign
      leftcert=server.cert.pem  # reads the VPN server cert in /etc/ipsec.d/certs
      leftsendcert=always
      leftsubnet=0.0.0.0/0
      right=%any
      rightid=%any
      rightauth=eap-mschapv2
      rightsourceip=192.168.0.0/24
      rightdns=8.8.8.8 DNS to be assigned to clients
      rightsendcert=never
      eap_identity=%identity  # defines the identity the client uses to reply to an EAP
```

Save and close the file when you are finished.

Where:

config setup : Specifies general configuration information for IPSec which applies to all connections.

charondebug : Defines how much Charon debugging output should be logged.

leftid : Specifies the domain name or IP address of the server.

leftcert : Specifies the name of the server certificate.

leftsubnet : Specifies the private subnet behind the left participant.

rightsourceip : IP address pool to be assigned to the clients.

rightdns : DNS to be assigned to clients.

Step 6 – Configure Authentication

At this point, your VPN server is configured to accept client connections. Next, you will need to configure client-server authentication credentials to define the RSA private keys for authentication and set up the EAP user credentials.

```
nano /etc/ipsec.secrets
```

Add the following lines:

```
: RSA "server.key.pem"
.vpnsecure : EAP "your-secure-password"
```

Save and close the file. Then, restart the strongSwan service and enable it to start at reboot:

```
systemctl restart strongswan
systemctl enable strongswan
```

You can also verify the status of the strongSwan service using the following command:

```
systemctl status strongswan
```

You should see the following output:

```
• strongswan.service - strongSwan IPsec IKEv1/IKEv2 daemon using ipsec.conf
   Loaded: loaded (/lib/systemd/system/strongswan.service; enabled; vendor preset: enab
   Active: active (running) since Fri 2020-05-08 08:02:08 UTC; 8s ago
 Main PID: 29947 (starter)
    Tasks: 18 (limit: 2359)
   CGroup: /system.slice/strongswan.service
           ├─29947 /usr/lib/ipsec/starter --daemon charon --nofork
           └─29973 /usr/lib/ipsec/charon --debug-ike 2 --debug-knl 2 --debug-cfg 2 --de

May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   eap_identity=%identity
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   dpddelay=300
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   dpdtimeout=150
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   dpdaction=1
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   sha256_96=no
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   mediation=no
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   keyexchange=ikev2
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG] adding virtual IP address pool 192.16
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG]   loaded certificate "CN=vpn.example.
May 08 08:02:08 ubuntu1804 charon[29973]: 05[CFG] added configuration 'ipsec-ikev2-vpn'
```

You can also verify the strongSwan certificates using the following command:

```
ipsec listcerts
```

You should get the following output:

```
List of X.509 End Entity Certificates

  subject:  "CN=vpn.example.com"
  issuer:   "CN=VPN Server CA"
  validity:  not before May 08 07:59:18 2020, ok
             not after  Nov 18 07:59:18 2027, ok (expires in 2749 days)
  serial:    7b:f8:ab:dc:ca:64:dd:93
  altNames:  vpn.example.com (http://vpn.example.com)
  flags:     serverAuth ikeIntermediate
  authkeyId: 12:60:f6:05:15:80:91:61:d6:e9:8f:72:a3:a5:a5:ff:a7:38:1a:32
  subjkeyId: bf:1d:b1:1b:51:a0:f7:63:33:e2:5f:4c:cb:73:4f:64:0f:b9:84:09
  pubkey:    RSA 4096 bits
  keyid:     e4:72:d0:97:20:ec:a5:79:f2:e0:bf:aa:0e:41:a8:ec:67:06:de:ee
  subjkey:   bf:1d:b1:1b:51:a0:f7:63:33:e2:5f:4c:cb:73:4f:64:0f:b9:84:09
```

At this point, your strongSwan VPN server is installed and configured. You can now proceed to install and configure the VPN client to connect the VPN server.

Step 7 – Install and Configure strongSwan Client

Log in to the client system and run the following command to install the strongSwan client packages:

```
apt-get install strongswan libcharon-extra-plugins -y
```

Once installed, disable the strongSwan service to start at boot:

```
systemctl disable strongswan
```

Next, copy the ca.cert.pem file from the VPN server to the VPN client using the following command:

```
scp root@your-vpnserver-ip:/etc/ipsec.d/cacerts/ca.cert.pem /etc/ipsec.d/cacerts/
```

Next, configure VPN client authentication by editing the file /etc/ipsec.secrets:

```
nano /etc/ipsec.secrets
```

Add the following line:

```
vpnsecure : EAP "your-secure-password"
```

Save and close the file. Then, edit the strongSwan default configuration file:

```
nano /etc/ipsec.conf
```

Add the following lines:

```
conn ipsec-ikev2-vpn-client
    auto=start
    right=vpn.example.com
    rightid=vpn.example.com
    rightsubnet=0.0.0.0/0
    rightauth=pubkey
    leftsourceip=%config
    leftid=vpnsecure
    leftauth=eap-mschapv2
    eap_identity=%identity
```

Save and close the file. Then, restart the strongSwan service with the following

command:

```
systemctl restart strongswan
```

On the strongSwan server, check the VPN connection status using the following command:

```
ipsec status
```

You should see that the IP 192.168.0.5 assign to the VPN client:

```
Security Associations (1 up, 0 connecting):
ipsec-ikev2-vpn-client[1]: ESTABLISHED 1 minutes ago, [vpnsecure]...192.168.0.1[vpn.exa
ipsec-ikev2-vpn-client{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: 74ab87d0db9ea3
ipsec-ikev2-vpn-client{1}:   192.168.0.5/32 === 0.0.0.0/0
```

Conclusion

Congratulations! You have successfully installed and configured strongSwan VPN Server and Client on Ubuntu 18.04. You are now securely traversing the internet protecting your identity, location, and traffic from snoopers and censors – get started on your VPS hosted (https://www.atlantic.net/vps-hosting/) Ubuntu server from Atlantic.Net today!.

< Older post (https://www.atlantic.net/hipaa-compliant-hosting/hipaa-compliance-guide-what-is-hipaa/)

Newer post > (https://www.atlantic.net/dedicated-server-hosting/how-to-protect-and-secure-website-infrastructure/)

(/press-releases/atlantic-net-attains-ssae-18-certification-compliance-aicpa-standard-principles/)

(/press-releases/atlantic-net-offers-hipaa-audited-hosting-solution-to-give-medical-companies-and-patients-protection/)

(/press-releases/atlantic-net-offers-hipaa-audited-hosting-

solution-to-give-medical-companies-and-patients-protection/)

Recent Posts

COVID-19: Will the OCR Exercise Enforcement Discretion and Waive Penalties for HIPAA Violations? (https://www.atlantic.net/hipaa-compliant-hosting/covid-19-will-the-ocr-exercise-enforcement-discretion-and-waive-penalties-for-hipaa-violations/)

What Is an Intrusion Prevention System and Why Do I Need It? (https://www.atlantic.net/dedicated-server-hosting/what-is-an-intrusion-prevention-

system-and-why-do-i-need-it/)

How to Enable User Quotas in cPanel/WHM (https://www.atlantic.net/hipaa-compliant-cloud-hosting-services/how-to-enable-user-quotas-cpanel-whm/)

How to Protect and Secure Website Infrastructure (https://www.atlantic.net/dedicated-server-hosting/how-to-protect-and-secure-website-infrastructure/)

How to Install and Configure strongSwan VPN on Ubuntu 18.04 (https://www.atlantic.net/vps-hosting/how-to-install-and-configure-strongswan-vpn-on-ubuntu-18-04/)

ALSO ON ATLANTIC.NET

Set Up a Mail Server with Postfix, Dovecot

4 months ago • 1 comment

In this tutorial, we will show you how to set up a full-featured Mail server with

How Does Employee Monitoring Software ...

2 years ago • 1 comment

The shift in the healthcare industry towards convenient, accessible ...

The Benefits of Cloud Based Applications: ...

7 months ago • 1 comment

More companies are migrating their apps to cloud ...

Healthcare Cybersecu

a year ago • 1 c

Why does the industry still l others when i

0 Comments Atlantic.Net Disqus' Privacy Policy 1 Login

Recommend Tweet Share Sort by Best

Start the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your siteAdd DisqusAdd Do Not Sell My Data

COMPLIANCE HOSTING (/COMPLIANCE-HOSTING/)

HIPAA Compliant Hosting (https://www.atlantic.net/hipaa-compliant-hosting/)
HIPAA Cloud (https://www.atlantic.net/hipaa-compliant-cloud-hosting-services/)
HIPAA Dedicated Hosting (https://www.atlantic.net/hipaa-compliant-dedicated-server-hosting/)

CLOUD PLATFORM (/CLOUD-PLATFORM/)

Virtual Cloud Servers (https://www.atlantic.net/vps-hosting/)
VPS Pricing (https://www.atlantic.net/vps-hosting/pricing-2/)
Dedicated Hosts (https://www.atlantic.net/dedicated-server-hosting/)
Block Storage (https://www.atlantic.net/cloud-

COMPANY

About Us (https://www.atlantic.net/about-us/)
Data Centers (https://www.atlantic.net/world-class-data-center/)
Press Room (https://www.atlantic.net/press-room/)
Why Atlantic.Net (https://www.atlantic.net/hosting-services-provider/)

HIPAA Data Storage (https://www.atlantic.net/hipaa-compliant-cloud-storage/)
HIPAA Database (https://www.atlantic.net/hipaa-compliant-database-hosting/)
Disaster Recovery (https://www.atlantic.net/disaster-recovery/)
PCI Compliant Hosting (https://www.atlantic.net/pci-hosting/)
platform/block-storage/)
Virtual Private Cloud (https://www.atlantic.net/virtual-private-cloud/)
Cloud Backups (https://www.atlantic.net/cloud-platform/backups/)
Managed Private Cloud (https://www.atlantic.net/managed-private-cloud/)
Partners (https://www.atlantic.net/partners/)
Careers (/careers/)
Contact Us (https://www.atlantic.net/about-us/corporate-contact/)

SUPPORT (/SUPPORT/)

Network Status (https://status.atlantic.net/)
Speed Test (https://www.atlantic.net/speed-test/)
Service Policies (https://www.atlantic.net/service-policies/)
Privacy Policy (https://www.atlantic.net/service-policies/privacy-policy/)
Cookie Settings

NEW YORK, NY (/HIPAA-DATA-CENTERS/NEW-YORK-HOSTING/)

100 Delawanna Ave, Suite 1

Clifton, NJ 07014

United States

SAN FRANCISCO, CA (/HIPAA-DATA-CENTERS/SAN-FRANCISCO-CALIFORNIA-HOSTING/)

2820 Northwestern Pkwy,

Santa Clara, CA 95051

United States

DALLAS, TX (/HIPAA-DATA-CENTERS/DALLAS-TEXAS-HOSTING/)

2323 Bryan Street,

Dallas, Texas 75201

United States

ASHBURN, VA (/HIPAA-DATA-CENTERS/ASHBURN-VIRGINIA-HOSTING/)

1807 Michael Faraday Ct,

Reston, VA 20190

United States

ORLANDO, FL (/ORLANDO-COLOCATION-HOSTING-DATA-CENTER/)

440 W Kennedy Blvd, Suite 3

Orlando, FL 32810

United States

TORONTO, CANADA (/HIPAA-DATA-CENTERS/TORONTO-CANADA-HOSTING/)

20 Pullman Ct, Scarborough,

Ontario M1X 1E4

Canada

LONDON, UK (/HIPAA-DATA-CENTERS/LONDON-UK-HOSTING/)

14 Liverpool Road, Slough,

Berkshire SL1 4QZ

United Kingdom

US: 888-618-3282

Int: +1-321-206-3734

(htt	(htt	(htt	(htt
ps://	ps://	ps://	ps://
ww	twit	ww	ww
w.fa	ter.c	w.lin	w.yo
ceb	om	kedi	utub
ook.	/atla	n.co	e.co
com	ntic	m	m
/Atl	net)	/co	/use
anti		mpa	r/Atl

cNet	ny	anti
)	/atla	cHo
	ntic.	stin
	net-	g/)
	inc.)	

RESOURCES

- What is Cloud Hosting? (/what-is-cloud-hosting/)
- What is Private Cloud Hosting? (/what-is-private-cloud-hosting/)
- What is HIPAA Cloud Hosting? (/hipaa-compliant-cloud-hosting-services/#WhatisHIPAACloud)
- What is HIPAA Compliance? (/hipaa-compliant-hosting/hipaa-compliance-guide-what-is-hipaa/)
- What is Database Hosting? (/what-is-database-hosting/)
- What is Block Storage? (/what-is-block-storage/)
- What is SaaS? (/what-is-saas/)
- What is VMWare? (/what-is-vmware/)
- What is Web Server Hosting? (/what-is-web-server-hosting/)
- What is Server Virtualization? (/what-is-server-virtualization/)
- What is SaaS Hosting? (/what-is-saas-hosting/)
- What is VPS Hosting? (/vps-hosting/#WhatisVPSHosting)
- What is Managed Hosting? (/what-is-managed-hosting/)
- What is Colocation Hosting? (/what-is-colocation-hosting/)
- What is Healthcare Hosting? (/hipaa-compliant-hosting/what-is-healthcare-hosting-hipaa/)
- What is the HIPAA Security Rule? (/hipaa-compliant-hosting/what-is-the-hipaa-security-rule-safeguard-checklist)
- What is IaaS? (/what-is-iaas/)
- What is an IIS Server? (/what-is-an-iis-server/)
- What is a BAA? (/what-is-baa-hipaa-business-associate-agreement/)
- What is an Apache Server? (/what-is-an-apache-server/)
- What is PaaS? (/what-is-paas/)
- What is a SAN? (/what-is-a-san/)
- What is MySQL? (/what-is-mysql/)
- What is MSSQL? (/what-is-mssql/)