netgate

Reduce Your Cost of Cloud Security on AWS

By TJ Scholand

REDUCE YOUR COST OF CLOUD SECURITY ON AWS

WHEN CONSIDERING A MOVE TO THE CLOUD, CUSTOMERS TEND TO LOOK AT ONE OR MORE HYPERSCALERS WHILE ALSO CONTINUING TO LEVERAGE THEIR DATACENTER. Moves to the cloud tend to be slow and meticulous. We have yet to see anyone simply “lift & shift”, and be happy about it 30 days later. Planning a cloud migration takes into account many factors, first and foremost: security. By migrating workloads to the cloud, your company has greatly increased its attack surface. When moving to multiple clouds for “best of breed”, the attack surface increases once again. A bad configuration, an open IP address, zero day exploits all tend to make the news these days. Yet one needs to balance security with functionality and cost. So how do you secure your on-premises and multi-cloud environment at the lowest possible TCO?

Why do you need a firewall in the cloud?

Let’s start by considering the global nature of organizations, whether they are businesses, government agencies, or academic institutions. Many of these organizations have operations distributed around the world, which means connecting different branch locations to the cloud. Employees might be further distributed, working from branch offices, remotely, or from different places every day.

It can be more cost-effective for organizations to store their data in the cloud as compared to on-premises storage. Depending on its industry, there may also be specific requirements about where an organization stores its data. Regulations like the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), to name a few, have specific data privacy and residency requirements. As the number of connection points increases, so does the opportunity for exploits by unsavory actors.

A cloud firewall monitors incoming and outgoing network traffic and blocks unauthorized or malicious network traffic, much like a traditional network firewall does. In addition, a firewall can provide virtual private network (VPN) connections, intrusion prevention, application firewalling, TLS/SSL encrypted traffic inspection, website filtering, rate limiting, and antivirus inspection. The firewall is your defense at every point of entry to your network, ensuring all data entering and leaving your network is expected and providing the utmost security for your data.

It can be more cost-effective for organizations to store their data in the cloud as compared to on-premises storage.

As organizations move away from on premises hosting to the cloud with numerous points of entry, securing those instances has never been more important. A cloud firewall can protect your Virtual Private Cloud (VPC) with intrusion detection/intrusion prevention (IDS/IPS), function as a DNS server, NAT, and provide additional secure communications between the following scenarios:

- Cloud instances (cloud-to-cloud)
- Your organization's network and cloud instance (site-to-cloud)
- Employee assets (computers, phones, tablets) and a cloud instance (endpoint-to-cloud)

In this white paper, we will take a deeper look at both pfSense Plus software on AWS and the AWS Firewall Manager. The goal is to drive a deeper understanding of how pfSense Plus software on AWS can help you lower your operating costs, have more control over your cloud network security, and have more options for securing access to and future-proofing your VPC.

pfSense Plus Software on AWS Provides

1. Lower Operating Costs and Total Cost of Ownership
2. More Control over Cloud Network Security
3. More Secure Access VPN Options
4. Future-proof Cloud Firewall

AWS Firewall Manager

The AWS Firewall Manager is comprised of 6 separate policies:

1. Network Firewall
2. Web Application Firewall
3. Shield and Shield Advanced
4. VPC Security Groups
5. Route 53
6. Third Party Firewalls.

Network Firewall and VPC Security Groups are the two AWS policies that perform the most traditional firewall functions. Shield and Shield Advanced provide protection against Distributed Denial of Service (DDoS) attacks, while Route 53 provides DNS services. AWS has assembled these policies under the Firewall Manager umbrella in the interest of providing easy, centralized access to security services.

There can be some significant expense associated with this convenience. pfSense Plus software compares with Network Firewall and VPC security groups. pfSense Plus software is a third party firewall.

The goal is to drive a deeper understanding of how pfSense Plus software on AWS can help lower your operating costs

À la carte Costs Your Business Money

One common pricing strategy on the cloud is that you only "pay for only what you need." Cloud platforms have taken this to the extreme by breaking out every function in the firewall as a separate service you purchase and assemble into your cloud solution. Unfortunately, À la carte services can get expensive quickly when looking at just a handful of common functions asked of a firewall.

Simply explained, AWS utilizes a multi-layered pricing model that encompasses various types of charges. These include compute, storage, and data transfer fees.

Compute charges cover a wide range of resources, such as EC2 instances, as well as associated services like VPN, DNS, Network Firewall, NAT Gateway, and IDS/IPS.

Storage charges apply to items such as S3 buckets, EBS volumes, logs, and backups.

Data transfer fees are incurred for outbound data (data egress) that is sent from AWS to different locations outside of the cloud.

It is important to note that AWS does not charge for inbound data transfer.

AWS Charges

AWS Services are much like a utility bill. There is a fee for the access to the service and then a fee for how much of the actual utility you use or consume. Think of it like a water or electricity bill; you are charged for having the service delivered to your home or business and then charged per unit used, be it kilowatt hours or gallons. When it comes to cloud services, a service has a fee and then a charge for each unit downloaded or egressed out of AWS' cloud. The unit of data egressed is a gigabyte (GB) for AWS.

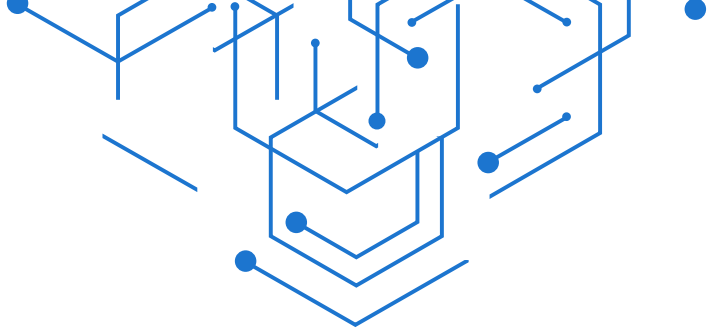
How you can Save Money with pfSense

To use pfSense Plus software on the AWS cloud platform, an AWS Elastic Compute Cloud (EC2) instance is required. In our example, we will use the AWS US East Region - Virginia or Ohio (see Assumptions[1] below). An EC2 instance size of m5.large, using **On-Demand hourly** pricing with no other services is $0.096 per hour, or approximately $69.12 per month.

[1]ASSUMPTIONS:
- The average month has 4.33 weeks, 30 days, 720 hours, and 22 work days.
- The average work day has 8 hours, or 176 hours per work month.
- The Netgate recommended AWS EC2 instance type for pfSense Plus software is m5.large.
- US East AWS Region - N Virginia or Ohio (different AWS regions will have different EC2 instance/hour rates).

NOTE: AWS assumes 730 hours per month in their VPC Pricing Calculator

It is important to note that AWS does not charge for inbound data transfer.



This is the Netgate recommended instance size for pfSense Plus software on AWS. Netgate recommends this instance size for production workloads as it represents a versatile blend of compute/memory/networking capabilities at a reasonable price point. This is only a recommendation, as users may choose their ideal instance size based on a variety of factors.

For new users that want to gain familiarity with pfSense Plus software capabilities on AWS, Netgate offers a 30 day free trial. During this trial, there is no cost for pfSense Plus software, but the user is responsible for the cost of the AWS EC2 instance.

Users can start small and find the best instance size to fit their individual needs. It is worth noting that the Netgate Engineering team builds all new pfSense Plus software releases on AWS using a t3a.micro EC2 instance. The t3a.micro EC2 instance costs less than $0.01 ($0.009) per hour!

QTY 1 EC2 instance = $0.096
✖ 720 hours in a month
= **$69.12/month**

The AWS Network Firewall has multiple charges to consider. This paper provides a basic overview and is not intended to be a comprehensive explanation of AWS Network Firewall pricing. For a complete description, please see the AWS Network Firewall Pricing page. The two main charges associated with the AWS Network Firewall are:

- Network Firewall Endpoint Hourly: **$0.395/hour**
- Network Firewall Data Processing Charge: **$0.065/1 GB** of data processed by the firewall

While the AWS Network Firewall is provisioned, AWS does not charge additional fees for NAT Gateway (hourly and data) usage. Please note that EC2 Data Transfer charges may apply; more on that later.

pfSense Plus software on an m5.large AWS EC2 instance will cost the user **$0.24/hour**.

Right away, choosing pfSense Plus software from Netgate saves the user **$0.155/hour**, or **$111.60/month,** or **$1339.20/year** in hourly charges.

EC2 Instance type	Software/hr	EC2/hr	Total/hr
○ m3.xlarge	$0.32	$0.266	$0.586
○ m4.large	$0.24	$0.10	$0.34
○ m4.xlarge	$0.32	$0.20	$0.52
● m5.large ★ *Vendor Recommended*	$0.24	$0.096	$0.336
○ m5.xlarge	$0.32	$0.192	$0.512
○ m5a.large	$0.24	$0.086	$0.326
○ m5a.xlarge	$0.32	$0.172	$0.492

pfSense Plus Software option saved $11,700/month, or $140,400/year on a single instance

The larger opportunity becomes clear when the reader understands that there are no pfSense Plus software charges for **for data processing** or data transfer (AWS data transfer charges may apply). Does that sound easy? That's because it is!

Consider how much data your organization would pass through a firewall on the cloud each .month. One use case egresses an average of 250GB/hour. This customer would pay $0.065/GB x 250GB/hr x 720hr/month = $11,700/month in data processing charges for data processed by the AWS Network Firewall. In this case, the pfSense Plus software option just saved the user $140,400 per year - on a single instance. Consider how many firewalls your organization requires and multiple the $140,400/year savings accordingly. The savings add up.

Please note that additional savings with pfSense Plus software are available by signing up for annual pricing.

VPN Example

Next, let's look at setting up a Client Virtual Private Network (VPN) on AWS using a single subnet association and consider the fees and charges. Assume you have 100 client devices to connect to the VPN. These devices could be computers, phones, or tablets, all establishing a connection to access your cloud resources, such as a database or file share. Data transfer fees will need to be considered in this example as well. We will first look at VPN fees and then cover data transfer fees.

The AWS Client VPN has a $0.10/hour endpoint association fee. This fee is similar to an EC2 instance fee — it provides for the AWS Client VPN on AWS. You can review AWS VPN pricing for your specific region. Note: using 2 subnets will double the Client VPN endpoint cost.

AWS Client VPN Endpoint
(using single subnet)
Association Fee ($0.10/hr)
✖ 720 hours/month = **$72.00**

DATA PROCESSING COST SAVINGS

	Data Egress	Unit Cost	Quantity	Cost/Month
Network Firewall	250GB/hr	$0.065/GB	720 hours	$11,700
pfSense Plus	250GB/hr	INCLUDED	720 hours	$0
				SAVINGS $11,700

There is also a charge for use or consumption — a $0.05 per client per hour connection fee for AWS VPN. We will assume that client devices average an 8-hour per day connection for 22 days of each month.

100 CLIENTS
✖ Connection Fee ($0.05/hr)
✖ 176 hours/month = **$880.00**

AWS VPN ENDPOINT (single subnet)
Association Fee $72/month
✚ 100 VPN client Connection Fee $880/month = **$952**

Your total cost for the AWS VPN (before outbound data transfer fees) is **$952.00/month**.

pfSense Plus software on AWS ($0.24/hr) + m5.large EC2 instance ($0.096/hr) ✖ 720 hours/month = **$241.92/month**

If we simply compare the cost of a 100 client VPN using pfSense Plus software vs. AWS Client VPN, the savings are significant. T**he pfSense Plus software on AWS solution is almost ¼ of the cost of using the AWS Network Firewall and the VPN services.**

If we wanted to consider a 1000 client VPN scenario, it is reasonable to assume that the pfSense Plus software option would require a larger EC2 instance size. Assume that we chose an EC2 instance size of c5.xlarge:

	Consumption	Cost/Interval	Quantity	Total (Monthly)
AWS Client VPN Endpoint	720 hours/mo	$0.10/hr	1	$72.00
AWS VPN Connection Fee	176 hours/mo	$0.05/hr	100	$880.00
TOTAL				**$952**

The pfSense Plus software on AWS solution is almost ¼ of the cost of using the AWS Network Firewall and the VPN services.

Number of Clients	pfsense+	AWS VPN	Monthly Savings
100 client VPN	$241.92	$952.00	$710.08
1000 client VPN	$352.80	$8,872.00	$8,519.20

Based on monthly billing. Does not include data egress fees. Fees as of March, 2023.

For the 100 client VPN, that is a savings of over **$700** in service fees alone each month. For the 1000 client VPN, the savings are over **$8500/month**, and over **$100,000 (USD) per year**! Additional users on AWS VPN will cost $8.80 per user per month. Additional VPN users are always included when running pfSense Plus software. As you can see, the costs are adding up, and we are only talking about a Virtual Private Network to access your companies' cloud resources.

Outbound Data Transfer Fees

We looked at the charges and costs associated with computing for a multi-client VPN solution in the cloud. In most cases, AWS does not charge for inbound data transfer or data transfer between other AWS services within the same region. Let us now look at AWS outbound data transfer, or egress fees using our Client VPN example.

You will consume a data resource like water from the tap or electricity from the outlet when turning the lights on. While AWS does not directly charge for data egress associated with the VPN client connection, AWS does charge for data transfer out of your VPC to the VPN service and your VPN client. At the time of this writing, AWS provides for the first 100 GB of data egress out to the internet. After that, the data transfer fee starts at $0.09 per GB for the first 10 Terabytes (TB) of data transfer. In this example, we will egress, or "use" 1 TB or 1,000 GB of data (after the first free 100 GB) transfer per month for ease of consideration:

1,000 GB/month ✖ $0.09/GB = $90

You will have this data transfer fee regardless of which VPN solution you use, AWS VPN or pfSense Plus software. Let us look at your total cost for 100 VPN clients and 1TB of data transfer for a month with both solutions.

PFSENSE PLUS SOFTWARE: UNLIMITED CLIENTS

c5.xlarge EC2
$0.17/hour ✖ 720 hours =
$122.40/month

pfSense Plus software on AWS ($0.32/hr) + **c5.xlarge EC2 instance** ($0.17/hr) ✖ 720 hours/month =
$352.80/month

AWS CLIENT VPN: 1000 CLIENTS

- **AWS Client VPN Endpoint** (single subnet) Association Fee ($0.10/hr) ✖ 720 hours/month = **$72.00/month**
- **1000 clients ✖** Connection Fee ($0.05/hr) ✖ 176 hours/month = **$8800.00/month**
- **AWS VPN Endpoint** Association Fee $72/month + 1000 VPN client Connection Fee ($8800/month) = **$8872/month**

AWS VPN

Single subnet Endpoint
Association Fee ($0.10/hr)
✖ 720 hours/month
= $72 (*Additional subnets are an extra cost*)
100 clients
✖ Connection Fee ($0.05/hr)
✖ 176 hours/month = $880
1,000 GB of data transfer
✖ $0.09/GB = $90
Total AWS VPN Fees: $1,042.00

PFSENSE PLUS SOFTWARE ON AWS

pfSense Plus
software on AWS ($0.24/hr)
+ EC2 instance ($0.096/hr) ✖
720 hours/month = $241.92
1,000 GB of data transfer
✖ $0.09/GB = $90
Total pfSense Plus software VPN Fees: $331.92

The service fees for the AWS VPN plus data egress are over three times as much as the flat rate for pfSense Plus software on AWS. In addition, you can add additional services with pfSense Plus software, such as network address translation (NAT) and intrusion detection and prevention for no additional service fees and only additional AWS data transfer fees per gigabyte of outbound data transfer.

Cost	pfSense Plus	AWS VPN	Savings
Monthly Cost	$331.92	$1,042.00	$710.08
Annual Cost	$3,983.04	$12,504.00	$8,520.96

Based on monthly billing. Assumes 1 TB of data egress fees. Fees as of March, 2023.

Network Address Translation (NAT)

If your organization's AWS virtual private cloud (VPC) requires a private subnet access to the internet (for downloading **software packages or package upgrades,** etc), you may opt to use the AWS NAT Gateway. If you do, you will have an hourly NAT gateway fee of $0.045/hr and a NAT gateway data processing charge of $0.045/1 GB of data through the NAT gateway. If we do not consider any data processing charges, the **AWS NAT Gateway would add a minimum of an additional $32.40/month to your AWS bill.**

pfSense Plus software on AWS includes data processing, a theoretically unlimited number of VPN connections, and NAT. For more information on pfSense Plus software and the AWS NAT Gateway, read our AWS NAT Gateway Alternative blog.

Easy-to-Use, with Granular Control

Let us continue with the Client Virtual Private Network (VPN) example and look at the configuration options. AWS VPN is a managed firewall solution that focuses on a single protocol for client VPN connections: OpenVPN.

pfSense Plus software on AWS includes data processing, a theoretically unlimited number of VPN connections, and NAT.

pfSense Plus software supports OpenVPN, IPSec, L2TP, and Wireguard.

pfSense Plus software also supports OpenVPN, in addition to IPSec, L2TP, and Wireguard. pfSense Plus software goes beyond unlimited client VPN connections and supports site-to-site, and cloud-to-cloud VPN connections.

Type	pfsense+	AWS Network Services
Site-to-Site VPN	✔ Included	AWS VPN ($36/month)
Client VPN	✔ Included	AWS VPN ($72.00 + $8.80/client/month)
Network Firewall	✔ Included	VPC Network Firewall ($284.40/month)
DNS	✔ Included	route53 ($0.50/route/month)
Load Balancing/ Reverse Proxy	✔ Included	CloudFront ($87.04/month)
IDS/IPS	✔ Included	GuardDuty ($6.40/month + $0.60/GB)
NAT Gateway	✔ Included	VPC NAT Gateway ($32.40/month)
Monitoring	✔ Included	CloudWatch ($0.05/GB)
Cost	$241.92/month	> $500+/month*
24/7 Support	$399/year ($799/year w/ 4 hr SLA)	$1200/year

** Based on monthly billing. 1 month = 720 hours. Does not include data egress, storage, or per-client fees. Fees as of March, 2023.*

The **AWS VPC Wizard**, available in pfSense Plus software, simplifies the configuration of a VPN to a remote VPC from an on-premises pfSense Plus firewall, allowing you to use pfSense Plus in both cloud and local implementations, if you prefer, standardizing your platforms.

If you need a **load balancer** for servers running in your Virtual Private Cloud (VPC), pfSense Plus software fits the bill. You can automatically distribute incoming application traffic across multiple servers for no additional service cost.

Load balancing ensures your services continue without disruption and ensure business continuity during peak traffic times. It is worth noting that the AWS load balancer can distribute incoming traffic across your EC2 instances across multiple availability zones as well. Both scenarios would require multiple instances.

Attack Prevention features built into pfSense Plus software protect your cloud instances from malicious actors' threats and exploits. There is no need to add on AWS GuardDuty at the additional expense of $6.40/month + $0.60/GB processed.

From intrusion detection and prevention systems (IDS/IPS) to traffic analysis to deep packet inspection (DPI), pfSense Plus software can monitor incoming and outgoing traffic. As a firewall and gateway, pfSense Plus software includes everything you need to defend your VPC.

pfSense Plus software includes a **package system** that can extend the software's functionality without adding bloat and potential security vulnerabilities to the base distribution. More than **60 different packages** are available that add additional filtering functionality, provide IDS/IPS, and add bandwidth monitoring, proxies, and additional services. Packages in the Netgate package repository do not incur additional fees and increase the value of using pfSense Plus software.

When it comes to knowing what is happening with your firewall, pfSense Plus software makes available all of the collected data to help monitor pfSense Plus on AWS. **System Monitoring** is not hidden from you nor does it require additional subscriptions. From an overview dashboard to monitoring graphs to unrestricted log access, pfSense Plus software on AWS provides unrestricted access to all of the data required to make informed decisions on the performance of your firewall and services.

Why Trust pfSense Plus Software from Netgate?

Netgate is not new to the firewall and router industry, **with over 20 years of business experience** and well over 500 combined years of technical knowledge on the team. pfSense Plus software from Netgate operates with the same rich feature set in the cloud, on Netgate **Security Gateway Appliances**, or on your own hardware (with **pfSense Plus subscription software**). With over 7 million installations world-wide, pfSense software continues to be a highly trusted solution.

pfSense Plus software from Netgate includes TAC Lite to get you from zero to ping quickly. With TAC Professional and TAC Enterprise support plans, you will receive expert technical support worldwide from five continents via email, portal, or phone with a four (4) or 24-hour initial response SLA from the Netgate Technical Assistance Center (TAC). The Netgate TAC team consistently scores over 90% in satisfaction ratings.

Netgate is also proud to support the Open-Source Community and Open-Source Projects. Netgate has a long heritage of giving back significant financial sponsorship, engineering and test resources, and upstreamed code to numerous open-source projects. Our project list includes Clixon, DPDK, FD.io/VPP, FreeBSD, Free Range Routing (FRR), Linux, pfSense Community Edition, and strongSwan.

Netgate employs or contracts many developers with roles in the FreeBSD, pfSense, Clixon, and VPP/FD.io projects. Their contributions and responsibilities include development, administration, maintenance, release engineering, and foundation board membership. These developers and many more at Netgate are regular contributors to these projects.

Conclusion

pfSense Plus software on AWS is a remarkably effective, powerful, and simple-to-use solution. Businesses, schools and governments around the world will benefit from pfSense Plus software and its associated cloud and edge firewall, router, and VPN functions. IT managers no longer need to requisition yet another new à la carte service, and the associated expense, thanks to pfSense Plus software's rich feature set and low total cost of ownership.

You can learn more about pfSense Plus software on AWS by browsing the manual. Of particular interest are these details on using a Netgate appliance instance to protect AWS VPC subnets.

pfSense Plus software on AWS is a remarkably effective, powerful, and simple-to-use solution.