Versa Cloud Firewall for AWS

Background

Businesses are rapidly adopting public clouds for their computational needs. One motivation for the move is agility. Public clouds offer automation and on-demand computing, allowing customers to build and tear down services programmatically and practically instantaneously. Customers have been quite successful at achieving this promised agility. However, workloads do not exist in isolation. When instantiating an instant application, securing the cloud application is a key consideration.

Traditional security solutions were designed for a slower pace. Longer sales cycles and more involved deployments with sales reps and partners gave customers weeks or even months to deploy a firewall to safeguard their workloads. With today's increasing speed of deployments, there's a growing demand for a more flexible commercial model and faster deployment strategies to satisfy immediate security needs.

Introducing Versa Cloud Firewall for AWS

Versa Cloud Firewall for AWS is an Amazon Web Services (AWS) based cloud firewall built to deliver robust security for dynamic workloads in public cloud environments. Versa Cloud Firewall for AWS provides a seamless, on-demand experience that ensures comprehensive protection for dynamically instantiated enterprise cloud applications and data repositories.

Versa Cloud Firewall is based on Versa's industry-leading enterprise NGFW. Versa NGFW is recognized by reputable testing labs such as CyberRatings.org and many Fortune 5000 Enterprises. In CyberRatings NGFW tests, Versa NGFW has consistently received "Recommended" ratings year after year. Versa NGFW also boasts 99.9% security effectiveness, the fastest throughput among competitors with its ability to handle encrypted traffic (HTTPS) efficiently, and a market leading price-to-performance ratio.

The security and cryptographic strength of Versa's solutions and processes have also been affirmed through key security certifications, including FIPS 140-2, Common Criteria EAL4+, PCI DSS Compliance, NIST USGv6r1, and SOC 2 Type 2.

Key Features of Versa Cloud Firewall for AWS

- Automation and Flexibility: Versa Cloud Firewall allows enterprises to deploy security solutions quickly using cloud automation, providing efficient and scalable firewalls for cloud workloads and data. Versa Cloud Firewall offers a flexible commercial model, allowing customers to pay for what they use, an ideal solution for cloud environments with dynamic workloads.
- Advanced Security Capabilities: Versa Cloud Firewall offers comprehensive security including the ability to identify and manage applications, restrict traffic from specified geographical locations, and inspect encrypted traffic to protect against hidden threats. Other security features include built-in Deep Packet Inspection (DPI), URL categorization, IP feeds and filtering, application classification and filtering, and user and group level policies.
- Easy Configuration and Management: The platform is designed for ease-of-use, featuring an intuitive user interface for firewall configuration, rule creation, and security management. Users can define custom rules based on IP addresses, applications, URLs, and zones.
- Unified Threat Protection: Versa provides comprehensive Unified Threat protection features including Intrusion Prevention Systems (IPS), Anti-Virus, hash-based file filtering, and TLS proxy to decrypt HTTPS flows to protect against advanced threats and ensure compliance with security policies.
- Cloud-Managed: Versa Cloud Firewall for AWS comes with a cloud-hosted orchestration and analytics infrastructure, offering users a worry-free experience with no additional infrastructure required. Versa's integrated big-data analytics provides real-time and historical insights into security events, trends, and alerts.

- Optional Remote Access: Versa offers an optional remote access VPN add-on for organizations to seamlessly bridge cloud technology with existing infrastructure.
- Native integration with AWS: Versa Cloud Firewall for AWS integrates natively with AWS Market-place and Amazon Virtual Private Cloud (VPC), ensuring seamless instantiation and protection of AWS workloads through the Versa Operating System (VOS). VOS powers various Versa services such as Versa Secure Cloud SD-WAN and Versa NGFW.

Overview of Versa Cloud Firewall for AWS

Versa Cloud Firewall for AWS is designed to easily connect to Amazon VPCs using a static IP address. Once connected, use the easy-to-use, intuitive User Interface (UI) to configure network firewall functions and protect your cloud workloads.

Easily instantiate required security functions with our built-in rule creation engine and default best-practice configurations. Firewall zones, such as trusted and untrusted zones, are characterized by easy-to-understand labels (e.g. cloud facing LAN port to Internet facing WAN port) and selection of arrows for direction of traffic.

The Versa Cloud Firewall application identification capability identifies all applications across all ports, including custom applications. Features such as Layer 7 DPI can identify URL, protocol and port numbers, destination IP addresses and more. Versa Cloud Firewall also comes with comprehensive policy-based controls including Geo IP filters to restrict incoming traffic from specified countries, and File Filter rules to check all attachment and protocols against a cloud lookup of malicious files.

Versa Cloud Firewall provides a rich set of URL and IP categorization and filtering capabilities in 80+ URL categories to enable safe browsing while blocking malicious sites. URLs are categorized by reputation, risk, and trustworthiness. In addition to predefined classifications, Versa provides support for user-defined/custom classifications that can be created and managed as needed. Hundreds of millions of domains and 13+ billion URLs are scored and classified for maximum threat coverage.

- 86 predefined URL categories and user defined URL category
- URL database is updated periodically via security package automatic updates (Spack) without the need for VOS or software upgrades
- Real-time cloud lookups of URL categories for those uncategorized in the VOS cache
- Custom URL categories based on regex and/or fixed string match
- Customizable captive portal screens for policy enforcement and redirection
- Support for Block, Inform, Ask, Justify, Override, and Authenticate pages
- Support for logging in Versa Analytics and deeper inspections

TLS Proxy: Protects against threats hidden in encrypted traffic by inspecting TLS/SSL traffic and applying additional security policies for threat detection and data protection.

- Directs encrypted traffic based on application signatures, scans encrypted content for malware and exploit prevention, detects and prevents data leakage to enforce company compliance.
- Support for transparent or split-proxy modes.
- Supports TLS versions 1.1, 1.2 and 1.3. Versa has been ahead of many security vendors in support for TLS v1.3.

IPSEC: Allows creation of IKEv2 based IPSEC tunnels to/from the cloud firewall instance to any remote device. Once created, you can direct traffic to the tunnel based on easy policy-based routing

Routing: Supports static routes, EBGP routing options are supported to connect to AWS workloads or to the Internet.

Next Generation Intrusion Prevention (NG-IPS):

- Signature-based and anomaly-based detection and prevention of vulnerabilities.
- Extensive coverage for vulnerabilities found over the last 10 years.
- Vulnerability signatures and anomaly detection engine updated dynamically via security package updates to provide real-time protection without needing to upgrade VOS.

Malware Protection: Versa Cloud Firewall provides a rich set of embedded antiviruses (AV) and malware protection capabilities using multilayered techniques such as heuristics, signature matching, emulation, and more. Versa's AV uses an optimum set of hardware resources to achieve optimized cost, performance and market leading efficacy. Versa's AV signatures are updated frequently (via Versa Cloud) and security package, allowing customers to always use the latest antivirus signatures.

File Filtering: Various types of viruses, malware and other malicious code travel using files. Versa Cloud Firewall's built-in File Filtering capability provides signature-based file type identification of various file types.

- Scans protocols HTTP, FTP, SMTP, POP3, IMAP, MAPI
- Computes a file hash signature and compares that against its database of file signatures to conduct an assessment. Versa's File Filtering function uses on file hashes and fingerprints, and not just files names. This method decreases the load on more detailed analysis engines, such as NG-IPS, AV and ATP engines by acting before such content inspection scanning functions kick-in

Versa Analytics: Versa Cloud Firewall comes with built-in big data based analytical capabilities provided by Versa Analytics. Versa Analytics also provides a use-case focused deep insights and actionable analysis for Routing, SD-WAN, and Security use-cases. It is a rich, near real-time big data analytics solution that provides visibility and control, baselining, correlation, and prediction capabilities to IT administrators. It provides near real-time and historical search, reports on usage patterns, trends, security events, and alerts.

Built-in Automation Capabilities: Made for lean IT organizations, Versa Cloud Firewall for AWS boasts an easy-to-understand, intuitive UI that does not require expert security skills to use. Users can make automated, mass configuration changes with ease – create rules once, and deploy to many devices on AWS with the rules.

Versa Cloud Firewall for AWS integrates our industry recognized security portfolio with AWS, minimizing the overhead for deploying and managing best-in-class security infrastructure.

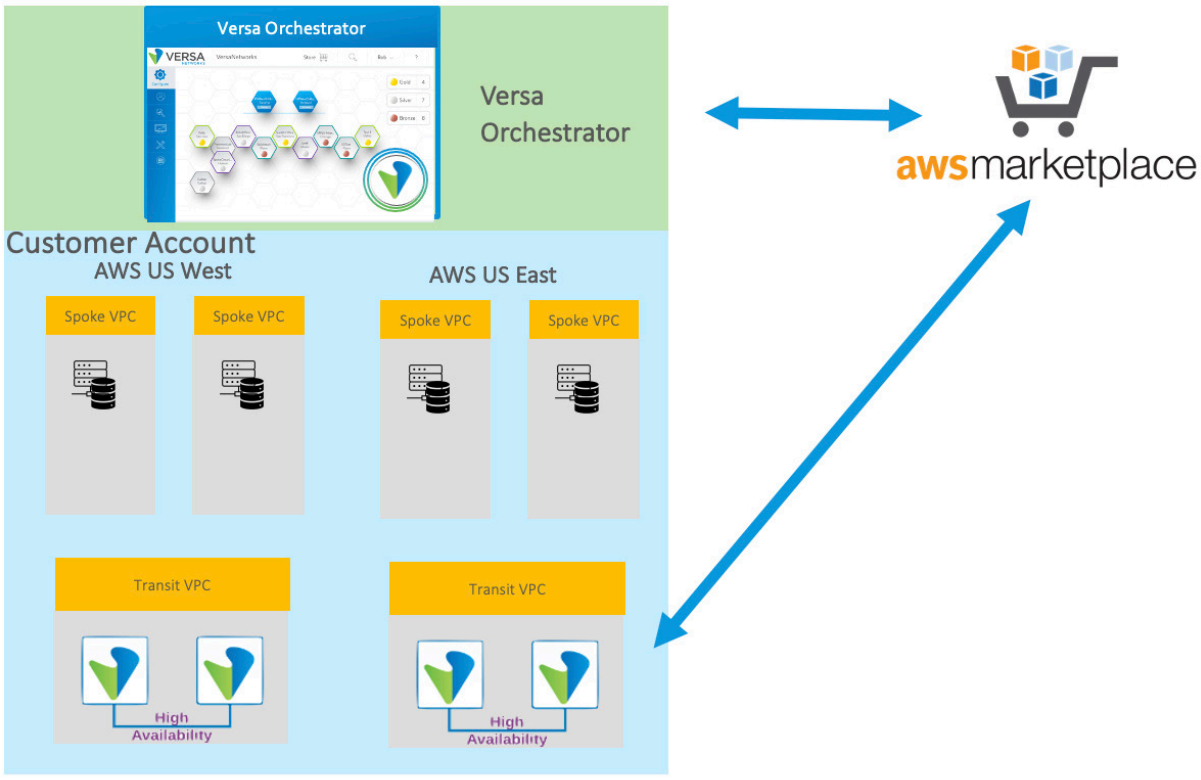

Figure: Versa Cloud Firewall for AWS deployed in Customer VPC

No Infrastructure to Manage

Versa Cloud Firewall for AWS is cloud hosted and cloud delivered. The cloud-based Versa orchestration infrastructure to support and secure your workload is entirely managed by Versa. All you need to do is subscribe and use.

Simple Procurement and Licensing Models

Versa Cloud Firewall for AWS is available through the AWS Marketplace, simplifying procurement, billing, and consumption. Its regional availability spans across multiple worldwide AWS zones, globally, providing broad coverage for enterprises with a global footprint. This solution is ideal for organizations seeking cloud-native security that adapts to dynamic cloud environments without the need for physical infrastructure. This subscription is offered on a Pay-as-You-Go basis, providing flexibility and scalability based on the actual usage of services. The subscription period is indefinite and renews automatically, unless terminated. The second option is Private Contract with feature license Tier, fixed long-term durations, and any add on options.

- Pay-as-You-Go Model: Under this model, the subscriber will be billed based on actual usage of services, measured in real-time. Charges will be calculated monthly and invoiced accordingly. There are no long-term commitments or upfront fees required, allowing the subscriber to scale usage up or down as needed. Pricing is based on the number of Versa Cloud Firewall Professional cores (4,8 or 16) and add on option for VPN Remote Access. Payment is billed by AWS services.
- Private Contract Option: For enterprises or customers seeking more tailored terms, a Private Contract may be negotiated. This allows for customized Versa Cloud Firewall license tier, pricing, and terms of service to fit the unique needs of the customer. The contract duration, payment structure, and any additional terms will be agreed upon. Quotes are done by Versa, and the customer sends a PO and pays Versa.

In the Pay-as-You-Go model, the purchasing experience is entirely self-service, allowing customers to quickly subscribe and deploy Versa Cloud Firewall directly through the AWS Marketplace without the need to engage with a sales representative. Here's how the process works:

- Discovery and Selection: Users can browse through AWS Marketplace, where they can find Versa Cloud Firewall for AWS (or other services). AWS Marketplace provides detailed product descriptions, pricing models, and reviews to help customers make informed decisions.
- Instant Subscription: Once the customer decides to subscribe, the process is straightforward. They simply click "Subscribe" and select their desired usage tier. There's no need for lengthy negotiations or discussions—everything is transparently listed, including pricing on an hourly, monthly, or yearly basis.
- No Long-Term Commitment: Since this is a Pay-as-You-Go model, customers only pay for what they use. There's no upfront cost or commitment to a long-term contract, making it ideal for businesses with fluctuating demand or those looking for flexibility.
- Billing and Invoicing: AWS automatically handles billing, with the cost being charged to the customer's AWS account based on actual usage. This provides frictionless experience, with no manual intervention or need for a sales representative to oversee transactions. In short, the Pay-as-You-Go purchasing experience is streamlined, automated, and ideal for users looking to deploy quickly without interaction with sales teams or negotiations.

For the Private Contract option, the purchasing experience involves interaction with a versa sales representative to tailor the solution to the specific needs of the enterprise. The process generally follows these steps:

- Sales Consultation: Unlike the Pay-as-You-Go model, a Private Contract involves reaching out to Versa sales representative. This step is crucial for organizations with unique requirements in terms of usage volume, compliance needs, or service levels.
- Customized Offer: During discussions with the sales rep, terms such as service level agreements (SLAs), volume discounts, custom pricing structures, and the length of the contract are negotiated. This process can result in significant cost savings and better alignment with the company's needs, but it requires more time compared to the self-service option.
- Formal Contracting: Once the terms are agreed upon, a formal contract is drawn up, which outlines the pricing, SLAs, and any custom requirements. This contract must be signed before services can be provisioned, which adds time to the purchasing process.
- Dedicated Support and Management: With a Private Contract, enterprises often gain access to higher levels of customer support, including dedicated account managers, which can be crucial for large-scale or mission-critical deployments.

Billing and Custom Invoicing: Unlike Pay-as-You-Go billing, which is automated and based on usage, a private contract includes invoicing, the customer's PO, and payment to Versa.

Easy Instantiation and Onboarding

Versa Cloud Firewall for AWS provides an end-to-end solution with easy, guided step-by-step onboarding and managing for cloud-based firewall services. Our pre-built templates and step-by-step workflow eliminates the need for manual setup, while the dashboard ensures that users have complete visibility and control over their security infrastructure from day one.

This approach reduces the time and effort required to deploy and manage cloud-based security, enabling organizations to protect their AWS workloads with minimal setup time and effort. This also ensures that organizations can easily scale, monitor, and update their security services as their cloud environments evolve. Versa Cloud Firewall embodies lean IT by reducing unnecessary complexity, automating repetitive tasks, and providing a unified platform for all network, security, and SD-WAN needs. This simplicity leads to faster troubleshooting, quicker deployments, and fewer errors, maximizing IT efficiency.

Simple Procurement and Consumption

You can easily login to your AWS account and review pricing and subscribe and activate the Cloud Firewall device. Billing is handled by AWS services. Device management is done by Versa's own infrastructure, so is the support help desk. Unsubscribe from the Versa Portal or AWS portal, to stop or restart the billing.

Versa Cloud Firewall for AWS is available as a pay-as-you-go service in the AWS Marketplace. You pay an hourly rate for the cores you subscribe to (4/8/16 Core CPU) and the license tier (Professional).

Regional Availability: Versa Cloud Firewall is available in several zones of AWS globally: US, Canada, Europe, Asia, and South America.

Licensing and Pricing

Versa Cloud Firewall for AWS is available through Amazon Web Services Marketplace. See AWS Marketplace pricing options for latest pricing options.

Unit
Versa Cloud NGFW Professional 4C
Versa Cloud NGFW Professional 8C
Versa Cloud NGFW Professional 16C
VPN Concentrator add-on for Versa Cloud NGFW Professional 4C
VPN Concentrator add-on for Versa Cloud NGFW Professional 8C
VPN Concentrator add-on for Versa Cloud NGFW Professional 16C

Features Summary

Versa Cloud Firewall for AWS	Professional
Stateful (L4) firewall	✓
CGNAT with ALGs	✓
IKEv2 IPSEC	✓
Rich set of routing protocols	✓
Next-Generation (L7) firewall	✓
URL reputations, classification and filtering	✓
IP reputations and filtering	✓
SSL/TLS proxy- decryption – including TLS1.3	✓
Antivirus, anti-malware protection	✓
NG-IPS	✓
Remote access VPN add on	✓

Support

Support is provided via the Versa Networks support portal. Open a ticket at Versa Support and contact support personnel. Additionally, you can get more information in the portal by clicking the info icon for each configuration. For more details on any feature, you can also refer to Versa documentation. Access to documents is also available in the dashboard.

VERSA

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com