40CLOUD

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

Cloud Network Firewall for AWS

40cloud's Cloud Network Firewall is a comprehensive security solution for AWS that is delivered in a SaaS model. The 40cloud solution makes your AWS public cloud private by building a new virtual private network over your AWS deployment. This network uses encrypted VPN links to interconnect all your AWS regions as well as your enterprise sites.

40cloud's Cloud Network Firewall is fully integrated with the AWS platform, providing automation of security and networking tasks (e.g. Security Groups, VPC routing), automatically detecting new resources and updating security rules accordingly.

Easily installed as an AMI, 40cloud's solution enhances AWS native security capabilities by adding important components such as user-VPN, Network Access policies, Two-Factor authentication, multi-region connectivity and firewall policy orchestration as well as IDS and SIEM integration.

The 40cloud solution is field-proven and fully Enterprise Grade, deployed by leading SaaS Providers, Healthcare Solution Providers and Financial Institutes, as well as Managed Security Service Providers.

Product Spotlight

- **Gateway –** a software appliance providing firewall, virtual router, VPN gateway and Network Access control point in a single entity. The Gateway is installed as an AMI, typically one per AWS VPC and it provides the entry point firewall for this VPC. Gateways can be deployed in High Availability mode.
- **Web Admin Console –** used to configure firewall policies, user access rules, build the static VPN connectivity, and monitor network connectivity status, system events and alerts. Can manage any number of Gateways over any number of AWS regions. The web admin console is provided centrally as-a-service.
- **API Engine –** 40cloud provides a full set of REST APIs that allow automation of all system capabilities.

Key Benefits

- **Agile** and cost-effective security solution that scales as your organization adds users, instances, regions, devices and geographic locations.
- **Operational efficiency:** all security tasks are automated, reducing manual intervention to minimum.
- **Full visibility** of the cloud deployment: notification and logging mechanisms, real time alerts as well as forensic capabilities.
- **Free Support:** assistance with implementation of data security and networking tasks, including free training, setup and ongoing support throughout the integration of 40cloud within the AWS deployment.
- **Compliance:** hardens the AWS deployment to comply with your security requirements.

Identity-based Network Access

40cloud enables you to centrally control back-end access to your entire AWS deployment, so that no one gains access unless they are authenticated. In addition, authorization is enforced on all remote **VPN** users by means of central, identity-based access rights policies (i.e. who can access what). These policies are configurable and can be integrated with existing (on-premise or cloud-based) identity-based authentication and authorization systems, such as **Active Directory** (AD) or **RADIUS.**

Multi-Region VPCs

40cloud's solution securely connects VPCs on multiple AWS regions into a single, fully connected 'global VPC'. In addition, you can define global firewall policies that will be automatically configured by 40cloud for the relevant AWS Security Groups on all regions. Using 40cloud, the connectivity between the regions is VPN based and highly available.

Security Automation

40cloud greatly reduces the IT intervention for security and networking tasks by offering automation of **AWS Security Groups, VPC routing** and other security and network configurations. **REST APIs** also enable orchestration and streamlining of identity-based access policies, firewall policies, VPNs, network elements and much more.

Enterprise Grade Solution

With its single and dual Gateway High Availability (**HA**) setups, 40cloud provides fast and automatic recovery should network, tunnel and Gateway outages occur. Using site-to-site IPSec connections, the 40cloud Gateways can securely connect any device on a remote site to the AWS cloud, in any topology or IP addressing setup.

The 40cloud web admin console provides full **network view** in real time, over any number of Gateways and regions, including Gateway and VPN status, connected users, active instances, TCP/IP flows, as well as last system events, current alerts and audit trails. 40cloud Gateways can connect to **IDS** and **SIEM** nodes to allow full visibility of security events occurring in the cloud.

Technical Specs

Firewall

- Stateful inspection, filtering and forwarding
- NAT (SNAT, DNAT, PAT)
- Network Access Control
- VPNs: site to site, user to site
- Tunneling: IPSec, GRE
- User VPNs: L2TP/ IPSec (iOS, Windows, Linux), Open VPN, XAUTH (Cisco) IPSec
- IPSec authentication methods: PSK, RSA, PKI
- Encryption algorithms: 3DES, AES (128 and 256)
- DNS caching and forwarding

Identity-based Authentication and Authorization

- Support for RADIUS, LDAP, LDAPS, Active Directory
- Two Factor Authentication
- Identity-based access rights enforcement (authorization profiles)

Enterprise Grade Operations

- High Availability
- Real time configuration, administration and status
- Automatic configuration of Security Groups and VPC routing
- REST APIs
- HIPAA compliance
- Two-factor authentication for administrators

Visibility

- Audit trail and system event logs
- Graphical network view for administrators
- Alerts and email notifications to administrators
- SIEM Integration
- IDS integration

Product Options

	Business Gateway	Enterprise Gateway	Enterprise+ Gateway	Notes
AWS Marketplace availability(AMI)	Hourly, BYOL (Monthly)	Hourly, BYOL (Monthly)	BYOL (Monthly)	
Free trial period	14 days	14 days	30 days	
Number of admins	2	Unlimited	Unlimited	
Auditing period	6 months	12 months	24 months	
Interconnecting VPCs on multiple regions	✓	✓	✓	VPN links between Gateways
Site-to-site VPN	Yes (5 site-to-site connections included in the hourly AMI)	Yes (5 site-to-site connections included in the hourly AMI)	Supported for additional cost per connection	Connects to IPSec devices external to AWS (including AWS VPN gateway)
User-to-site VPN	✓	✓	✓	
VPN users authentication and authorization	Local profiles	Local, AD, LDAP, RADIUS	Local, AD, LDAP, RADIUS	
Network Access Control	✓	✓	✓	Enforcing access rights policies for groups of VPN users
Firewall	✓	✓	✓	Includes stateful inspection, NAT
Gateway High Availability	-	✓	✓	
Security Group automation	✓	✓	✓	
SIEM/IDS Integration	-	-	✓	
Compliance	-	*See notes	HIPAA, *See notes	*AMI hardening follows CIS guidelines
40cloud APIs	-	✓	✓	
Visibility	✓	✓	✓	40cloud web admin console, system logs, events and noti ications
On-going support	Email	Email	Email + phone	Free of charge, including online training and setup

Specifications may change without notice

 8400 W. 110th, Suite 500, Overland Park, KS 66210 I +1 214-720-6118 I info@40cloud.com I www.40cloud.com