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.

<table>
<thead>
<tr>
<th>Product Spotlight</th>
<th>Key Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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.</td>
<td>• Agile and cost-effective security solution that scales as your organization adds users, instances, regions, devices and geographic locations.</td>
</tr>
<tr>
<td>• 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.</td>
<td>• Operational efficiency: all security tasks are automated, reducing manual intervention to minimum.</td>
</tr>
<tr>
<td>• API Engine – 40cloud provides a full set of REST APIs that allow automation of all system capabilities.</td>
<td>• Full visibility of the cloud deployment: notification and logging mechanisms, real time alerts as well as forensic capabilities.</td>
</tr>
</tbody>
</table>

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.

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), OpenVPN, 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

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

*Specifications may change without notice*