

Securing Amazon Web Services (AWS) EC2 Instances with Dome9

A Whitepaper by Dome9 Security, Ltd.



Amazon Web Services (AWS) provides business flexibility for your company as you move to the cloud, but new capabilities and deployment models create new security challenges. Using Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (VPC), companies access resizable computing capacity in the cloud. With EC2, new server instances can be provisioned and brought online in minutes, and taken offline just as quickly. This flexibility enables your business to rapidly scale your infrastructure up and down as needed and allows you to pay only for the actual capacity used. By providing a robust infrastructure, Amazon EC2 addresses many common failure scenarios and frees your developers to focus on meeting the needs of your customers. Of course, as part of that infrastructure, Amazon has provided basic tools for securing your cloud-based servers, starting with a set for managing the server firewalls, called AWS Security Groups.

AWS Security Groups provide a mechanism for managing communication restrictions between groups of servers within your cloud-based deployment. Amazon describes this scenario for using Security Groups to lock-down communication between services:

The firewall can be configured in groups permitting different classes of instances to have different rules, for example the case of a traditional three-tiered web application. The group for the web servers would have port 80 (HTTP) and port 443 (HTTPS) open to the world. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. Highly secure applications can be deployed using this expressive mechanism.

This basic AWS toolset for managing communication between servers provides a terrific solution for segregating security policy for specific and groups of servers. Despite this, many customers look to third-party security management solutions, like Dome9, to enhance the power of Security Groups and address additional security management requirements.

Security Groups, by themselves, provide static firewall management for AWS environments. Less security minded administrators often leave ports like RDP (Remote Desktop Protocol) and SSH (Secure Shell) open 24x7 so they can connect to and manage their instances. This means anyone (including hackers) can try to connect to a server, reach the administrative login prompt, and simply try to guess or brute force the username and password.

More security conscious admins will keep these and other ports closed, and manually open them when they need access. This, however, can be time-consuming, especially in larger environments. In scenarios like this, ports opened for a one-time need may inadvertently be left open continually. Administrators often forget to manually reconfigure the server's firewall after finishing their work. Additionally, in many cases, services are opened more broadly than necessary as a convenience. As an example, a security group may include multiple servers (e.g., your database server group). If a security group has port 3389 open for RDP, every server in that group has that same port open, publicly, to the Internet. To further complicate matters, security groups manage only inbound firewall connections and lack controls on out bound traffic, which may be a security requirement for your organization.

AWS Security Groups are available for AWS EC2 and VPC only, and don't deliver or manage security for other clouds. Organizations that have multiple private and/or public clouds serviced by multiple vendors will not benefit from Security Groups in non-AWS environments, or have centralized management or persistent and portable security policy across all of their servers and clouds. So, in the scenario where a server is migrated from one cloud to another, security must be re-applied and separately managed.

Fortunately, Dome9 integrates with AWS EC2 and VPC, supporting the above scenarios to:

- **Enable on-demand access** with time and location-based security controls so administrative ports aren't left open 24x7.
- **Automate secure, cloud server access** so that ports opened temporarily later close automatically once work is complete.
- **Apply and manage persistent security policies** that stay with the cloud server as it's migrated across providers.
- **Centralize and consolidate management** for server security across all servers and clouds.

Dome9 enhances the capabilities of AWS Security Groups by providing a layer of security management to support advanced security requirements.

Dome9 Server Security Management-as-a-Service

Dome9 centralizes security management for all servers and clouds, including AWS EC2 and VPC environments. It provides an automated control layer that dramatically increases security while streamlining administration.

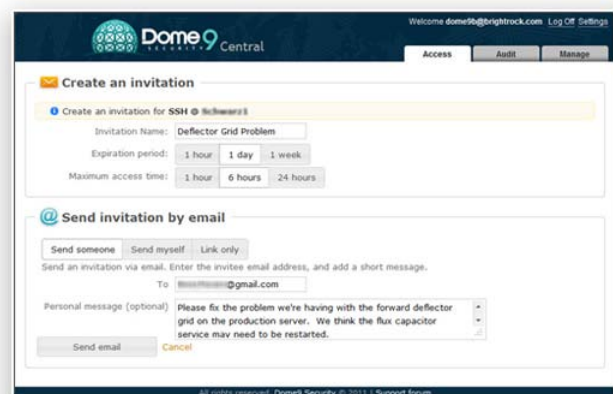
Take the example of an application developer needing SSH access to a server, perhaps to perform some one-time diagnostic task. Using Amazon EC2's Security Groups dashboard, the process might look something like this (assuming the port isn't already open by default):

1. The developer would contact your organization's EC2 administrator and ask them to open up a port between the cloud and their IP address (perhaps the IP range for the company office, or perhaps the IP for a remote location in the case of an off-site employee or contractor).
2. The administrator would open up the port for that Security Group for the IP address or range in the Security Groups dashboard.
3. The developer would do their work and, if you're lucky, after they complete the task send a second request to the administrator to disable the previously opened port.
4. If the administrator fails to manually change the Security Group setting, that port remains open (for all servers in that Security Group), creating a big security risk.

Dome9 simplifies and makes this process much more efficient with its innovative **Secure Access Lease™** technology, which enables a "default-closed" state for all administrative ports, with the ability to securely enable them on-demand for a specific person, time period, and purpose. Using Dome9 Central, Dome9's web-based management console, you don't simply open the port. Instead, you issue a secure access lease invitation – a one-time, limited access authorization assigned to the recipient's IP address and that expires after a specified period of time. When the Secure Access Lease expires, the port is closed automatically.

Unlike the manual and error-prone process we described for the admin using the AWS native tools, Dome9 Secure Access Leases provide a much more efficient and secure method of access. Invitations can be created and sent within minutes. Simply specify:

- The recipient's email
- An expiration time for the invitation
- A maximum access time (up to 24 hours)

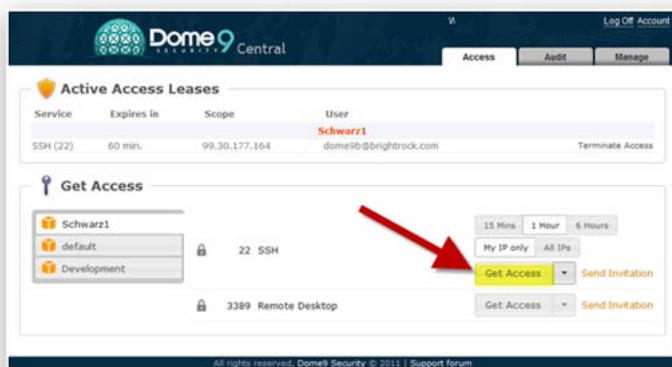


The recipient then receives an email with an embedded link to accept the invitation before they can connect to the server on the designated port. When the recipient clicks on the link, Dome9 automatically maps their IP address enacts authorized access from the recipient's computer for the period of time you've specified.



Secure Access Leases provide multiple advantages over manually managing ports using the native AWS tools, including:

- **Automatically limit the scope of access** - no need to leave a port wide open for a roaming user who may have to connect from home, a coffee shop, or a hotel. No need to worry about manually determining the public IP when connecting from a NATed network - the invitation process automatically determines the correct remote address for which to enable access, and limits the scope and period of access to only those authorized.
- **Automate a more secure workflow** - close the administrative port, automatically, after the admin-defined time period expires. Provide security **by default** without the need for managing an error-prone and manual process for returning your servers to a more secure configuration.



Dome9 users can also manage their own access. When logged into Dome9 Central, simply click the “Get Access” button and open access to a port for a limited time. Whether you need a few hours of RDP access to your server or just 15 minutes to log in via SSH, Dome9 provides a simple and easy to use interface for providing temporary access. Trusted users can manage their own access, and administrators can rest assured that the servers will automatically be returned to a default, secure state.

What can I do with Dome9?

After setting up your Dome9 account, you can begin using Dome9 Central to use innovative features such as:

- **Secure Access Leases**
Provide secure access to time- and location limited lease invitations, providing one-time access passes for a specific port on a cloud server. As detailed above, a Secure Access Lease provides flexible access while insuring that servers return to a default, secured configuration when the lease expires.
- **Multi-user Delegated Administration**
Grant administrative control for AWS Security Groups on a functional basis, providing each manager with control over only the resources necessary for their functional task.

For external consultants and developers, use secure access invitations as described above, but for internal IT teams or teams that require longer term access, multi-user delegated administration provides quick, segregated access to the Web servers for the Web development team; the database servers for the database team, etc.

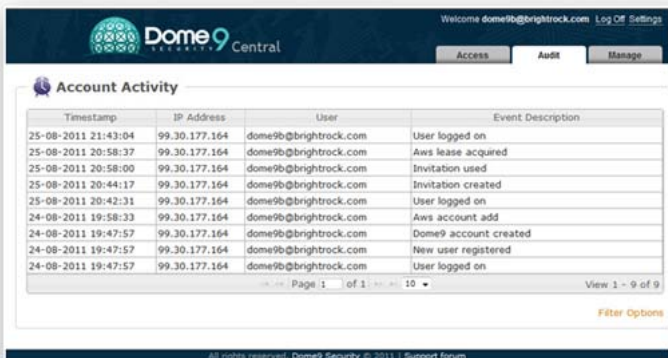
Authorize each user to self-grant access to their servers, and use your super-administrator capabilities to manage your entire cloud server environment.

If you have multiple IT security administrators across different business units, you can also segregate who can manage security policy for what machines. So, for example, the Web development team may be able to self-grant access to the Web servers, but they cannot manage the security policy for them. However, you, the super-admin, and the delegated IT security admin for that business unit can both self-grant access and manage the security policy configuration for those machines.



- **Account Activity Auditing and Logging**

All configuration changes and lease invitations are audited, with detailed logs providing super administrators with both the history of their own changes and the changes made by all delegated admins and third-party consultants and developers. Rather than manually pulling logs from each cloud server, Dome9 shows you, at-a-glance, who's accessing and modifying policy centrally, from one pane of glass. What's more, because the logs are stored within Dome9 Central (and not on the server), they're available continually even for servers that are removed from service and/or deleted from your cloud. For organizations with regulatory compliance requirements, Dome9 ensures that you have an audit trail for machines that might host PII, PCI, or other sensitive data.



- **Manage Security Across Multiple Cloud Providers**

What if your infrastructure spans multiple cloud providers? In that case, your admins will spend significant effort syncing up security between the infrastructures. Dome9 provides a better way.

Dome9 unifies the management of your cloud-based servers. With Dome9 Connect, an API integration module for Amazon EC2, you can instantly set security controls for your EC2 servers simply by registering your AWS account within Dome9 Central. Then, using the Dome9 Agent, servers outside of the Amazon EC2 cloud can be setup within your Dome9 Central account and have the exact same controls, simplifying the integration of servers hosted in other clouds. You can set one policy for all of your database servers, for example, regardless of their location. Centralized management enables mixed cloud deployments and simplifies the migration of servers from one cloud provider to another. For example, you might use AWS for development and testing, and another cloud provider for production environments, yet with Dome9 you can centrally manage your servers' security no matter which environment it's running in.

- **Flexible, API and Agent-based Security**

In addition to agentless deployment utilizing the Dome9 Connect API, Dome9 also supports an agent-based deployment option. The agent can be installed at any time, or preinstalled as part of a server image template. The benefits of using the agent include outbound firewall control and the ability to manage individual servers separately from the security group in which they reside. An administrator can, for example, provide access to an outside consultant for a specific server without giving that consultant any access to the rest of the servers in the security group. Without the agent, the administrator would either have to allow access to the entire group, potentially compromising security, or move the server into a new security group, adding complexity to the task. In addition, the Dome9 Agent also provides policy portability. If, for example, you move a virtual machine from one cloud to another, because the agent is deployed on the machine the policy goes with it, ensuring your server is continually secured and seamlessly managed.

Getting Started

To get started with Dome9, simply add your AWS Access ID Key to your Dome9 account (note: [we recommend creating a key with the minimal required rights](#)). Providing this key gives Dome9 access to your Security Groups via the Amazon AWS security APIs. No need to deploy agents or make any other changes to your server configuration - Dome9 seamlessly takes care of the details.



Summary

Dome9 provides the advanced security management tools needed to secure your AWS based infrastructure. As you migrate more of your servers into the cloud and outside your corporate firewall, Dome9 can ensure that those servers are secure by default, with access to ports available on-demand for a specific person, time period, and purpose.

Amazon excels at providing infrastructure, but the basic Security Groups-based firewall management does not provide the security-by-default that you require in your cloud-based infrastructure. Dome9 delivers the critical security management-as-a-service capabilities that you need, making your security as elastic as your cloud.

About Dome9 Security

Dome9 makes security as elastic as the cloud with first-of-its-kind multi-platform cloud server security management. Available for the enterprise and hosting providers, Dome9 provides dynamic security policy control for Clouds, Virtual Private Servers (VPS), dedicated servers, and Amazon's EC2 Security Groups, across all major operating systems and service providers.



Copyright © 2011 Dome9 Security, Inc. All rights reserved. Dome9 Security, its logo, and other marks are registered trademarks of Dome9 Security. All other trademarks are the property of their respective owners.