Amazon EC2 Platform Set-up Guide

Using Amazon EC2 as a platform for SWG Cloud Scanners

SWG Release 10.2 Manual Version 1.0.1

Confidentiality, Copyright and Disclaimer

This document may not, in whole or in part, be copied, published or reproduced without prior written consent from M86 Security. Every effort has been made to ensure the accuracy of the content contained in this document. Such content is provided "as is" without warranty of any kind. M86 Security disclaims all warranties and conditions with regard to this content, including all expressed or implied warranties and conditions of merchantability, and fitness for a particular purpose. The company shall not under any circumstance be liable for any errors or damages of any kind (including but not limited to compensatory, special, indirect or consequential damages) in connection with the document's contents. M86 Security, the M86 Security logo and M86-branded products are registered trademarks under license by M86 Security. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies. All rights reserved.

Amazon EC2 Platform Set-up Guide

Using Amazon EC2 as a platform for SWG Cloud Scanners

8845 Irvine Center Drive, Irvine, CA 92618, United States

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

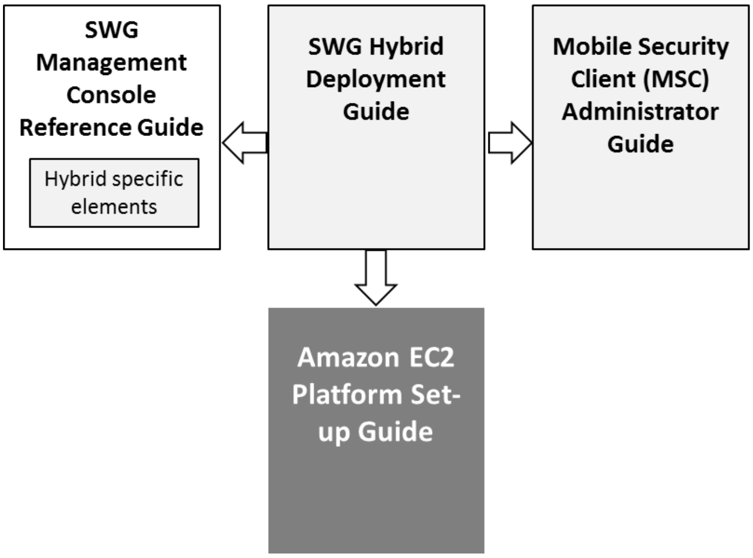
Other product names mentioned in this manual may be trade- marks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

1 Start Here

1.1 What is the Purpose of this Guide?

This guide is intended to help systems administrators with the set-up of the **Amazon Web Services EC2** platform for M86 Security SWG Cloud Scanners. These instructions should be used in conjunction with the M86 **SWG Hybrid Deployment Guide** and other resources as shown below:


SWG Management Console Reference Guide
Hybrid specific elements
SWG Hybrid Deployment Guide
Mobile Security Client (MSC) Administrator Guide
Amazon EC2 Platform Set-up Guide

1.2 What is the Amazon EC2 SWG Cloud Scanner Platform?

Amazon Web Services EC2 (www.amazon.com/ec2) is a cloud based service that can be used as a virtualized platform for running M86 Security Cloud Scanners.

M86 SWG Cloud Scanners can be run on a number of different platforms including hardware appliance, Virtual Appliance, M86 Secure Web Service Hybrid (SWS-Hybrid)[1] and Amazon Web Services EC2. The EC2 option is for customers who wish to use off-premise locations for SWG Cloud Scanners, but retain direct control over the virtual platform. M86 Security SWG Cloud Scanner AMI code is used to create Cloud Scanner instances that run in chosen geographic regions throughout the world. This allows the SWG customer to place SWG Cloud Scanners close to the mobile/roaming user and remote/branch offices.

1.3 Top Tips!

Key items that will make deployment easier:

- To see an outline of the deployment steps see section 2.
- To ensure a secure configuration see the “Security Group (Firewall Rules) Guidance” table in section 2.5.4
- For Secure Web Service Hybrid (SWS-Hybrid) platform set-up, stop here and refer to M86 Security.

[1] Set-up of the M86 Secure Web Service Hybrid (SWS-Hybrid) platform option is performed entirely by M86 Staff.

1.4 User Guide Conventions

The following icons are used throughout this user guide:

📝 ***NOTE**: The “note” icon is followed by italicized text providing additional information about the current topic.*

💡 ***TIP**: The “tip” icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

❗ ***WARNING**: The “warning” icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.*

⚠ ***IMPORTANT**: The "important" icon is followed by italicized text informing you about important information or procedures to follow.*

1.5 Glossary of Terms

AWS	Amazon Web Services, provides the Infrastructure as a Service used as a platform for the SWG Cloud Scanner.
AMI	Amazon Machine Image is an encrypted machine image stored in Amazon. It contains all the information necessary to boot instances of your software.
Cloud Load Balancer	A load balancer that is either deployed by a customer on the Amazon EC2 platform or by M86 Security on the M86 Security SWS-Hybrid platform.
Cloud Scanner	An SWG scanning server type designed to support mobile/roaming workers whilst being deployed in cloud based infrastructure such as Amazon EC2, M86 Security SWS-Hybrid or in an organization’s own private cloud infrastructure.
EC2	Amazon Elastic Computer Cloud (Amazon EC2). http://aws.amazon.com/ec2/ is a web service that provides resizable compute capacity in the cloud. It is used as a platform for the M86 Security SWG Cloud Scanner.
Elastic IP Address	Amazon EC2 Elastic IP addresses are static IP addresses designed for dynamic cloud computing. An Elastic IP address is associated with your EC2 account and then used against a specific Cloud Scanner Instance or Cloud Load Balancer instance.
Instance	After an AMI is launched, the resulting running system is called an instance. Instances remain running unless they fail or are terminated. When this happens, the data on the instance is no longer available.
MSC	M86 Security Mobile Security Client software installed on the user’s Personal Computer (Windows or Mac OS X) to redirect web traffic to available SWG Cloud Scanners.
PAC file	A Proxy Auto-Configuration (PAC) file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL. A PAC file contains a JavaScript function "FindProxyForURL(url, host)".
Security Group	An EC2 Security Group is a set of firewall rules used to secure an instance.
SWG Scanner	An M86 Security SWG Scanning Server installed in the corporate network.
SWG Policy Server	An M86 Security SWG Policy Server installed in the corporate network.
Remote Computer	A laptop, home office desktop or otherwise non-static computer.

2 EC2 Cloud Scanner Set-up

⚠ ***IMPORTANT**: The Amazon EC2 web interface can change without notice and so this document must be taken only as a guide to the steps required. The exact screens and process details may vary.*

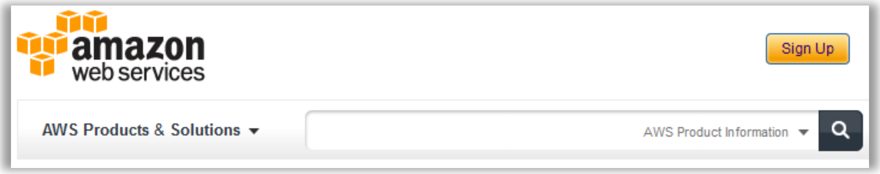
The following steps are required to deploy an SWG Cloud Scanner on the EC2 platform:

EC2 Cloud Scanner Deployment Step	Explanation
Create/obtain Amazon EC2 account and sign-in	Pre-requisite for the EC2 platform.
Region Selection	Where do you want to have Cloud Scanners located?
Configure Key Pairs	Needed for secure operating system level access on EC2 instances.
Security Groups Set-up	Firewall rules for SWG Policy Server access, mobile/roaming user and remote/branch office scenarios.
Elastic IPs Set-up	IP addresses used by the SWG Policy Server to manage the cloud scanners and for the Mobile Security Client to connect to.
Launch Cloud Scanner Instance	Get the cloud scanner ready to connect to the SWG Policy Server.
Load Balancing Set-up	When more than one EC2 instance is required in a given EC2 geographic region.

2.1 Create/obtain Amazon EC2 Account

An Amazon EC2 account is needed before the set-up process can begin. This can be a new account specifically for the purpose or an existing account. Instructions are provided in the Amazon Web Services web site:

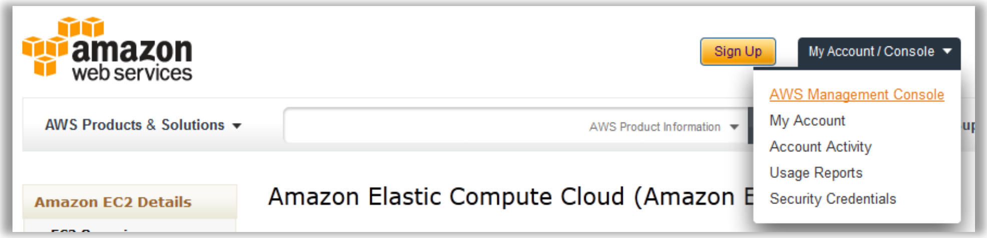
http://aws.amazon.com/ec2/ simply select Sign Up and follow instructions.



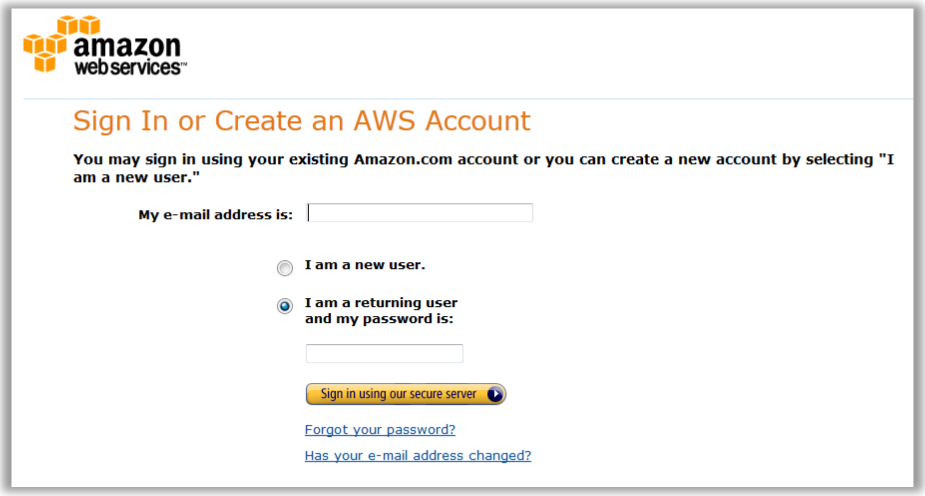
2.2 Sign-in

To sign-in to Amazon EC2 account:

1. Navigate to http://aws.amazon.com/ec2/
2. Select My Account / Console then click the AWS Management Console link.



3. Provide your AWS email address and password, ensuring that the **I am a returning user** radio button is enabled.


amazon webservices™
Sign in using our secure server
Forgot your password?
Has your e-mail address changed?

Sign In or Create an AWS Account

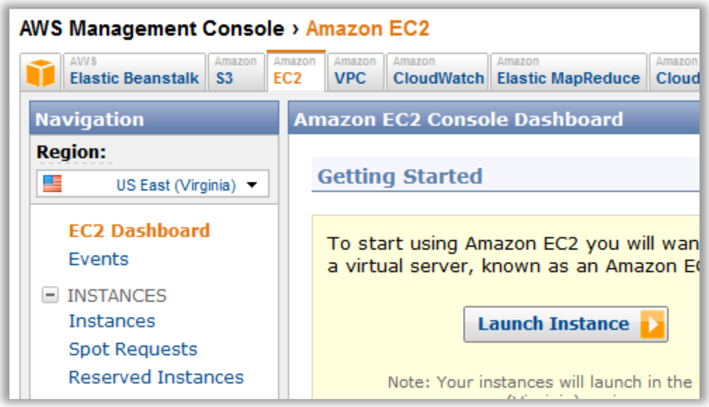
You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."

My e-mail address is:

○ I am a new user.

● I am a returning user and my password is:

4. Click the **Sign in** using the secure server button.
5. Click on the “EC2” tab.



Region: US East (Virginia)

To start using Amazon EC2 you will wan
a virtual server, known as an Amazon E

Note: Your instances will launch in the

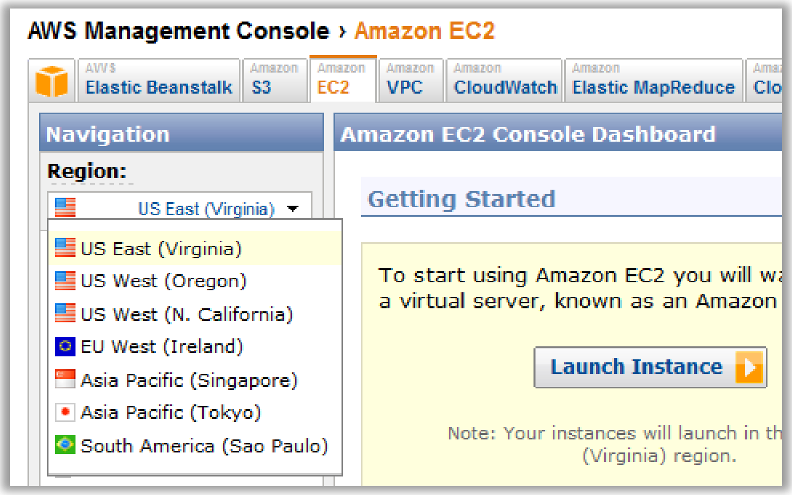
2.3 Region Selection

Amazon EC2 provides a number of geographic Regions (data centers) in which Cloud Scanners can be deployed or launched.   See **Appendix A – Supported Amazon EC2 Instance** for further information.

Read more about EC2 datacenters and regions at http://awsdocs.s3.amazonaws.com/EC2/latest/ec2-ug.pdf

To select a region

1. In the left Navigation pane, click the drop-down menu of the **Region** field.
2. Select the region nearest to the mobile/remote users who will use the Cloud Scanner.



To start using Amazon EC2 you will wa
a virtual server, known as an Amazon

Note: Your instances will launch in th
(Virginia) region.

2.4 Configure Key Pairs

A key pair is a combination of a public key and a private key that allows an IT administrator to launch and access a specific EC2 instance using SSH (Linux/Unix) or RDP (Windows) connection methods. These keys are different than those provided during the initial AWS registration.

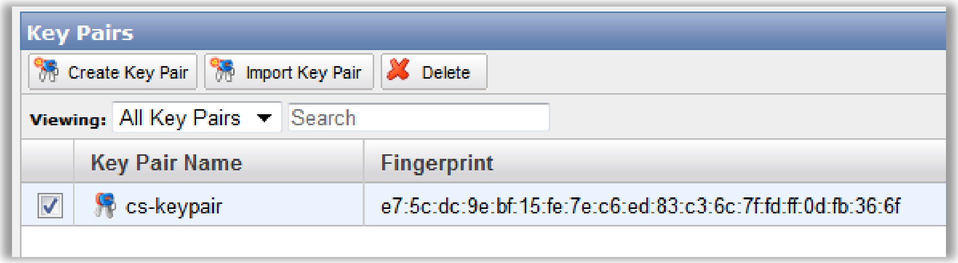
After initiating an instance, and as part of the process of adding the SWG Cloud Scanner scanner to that instance, a key pair is created. This can be handled using command line tools or through the AWS console.

The private key is downloaded and provided upon launching a specific instance. Amazon retains the corresponding public key and provides it to the running instance.

***NOTE**: Create a Key Pair through the Launch Wizard or before launching an Instance by accessing the left navigation pane and clicking **Key Pairs**.*

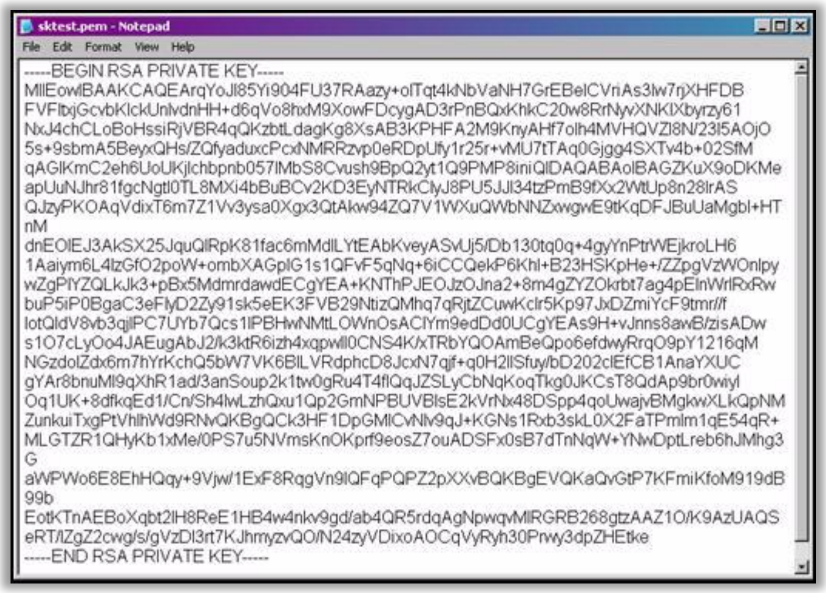
Create a Key Pair (AWS Console)

1. In the left navigation pane, under Networking & Security, click **Key Pairs**.
2. The **Key Pair Name** dropdown menu displays a list of key pairs associated with your account.
3. If no key pair currently exists, click the Create Key Pair button in the main Key Pairs section.
4. Enter a name for the new key pair in the corresponding free text box.
5. Then click the **Create & Download your Key Pair** option.
6. Download the private key file and store it in a safe place to be used to access any instances that are launched with this key pair.



	Key Pair Name	Fingerprint
☑	cs-keypair	e7:5c:dc:9e:bf:15:fe:7e:c6:ed:83:c3:6c:7f:fd:ff:0d:fb:36:6f

7. After downloading and saving, the Key Pair should be in a .pem file and appear as follows:



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEArqYoJI85Yi904FU37RAazy+oITqt4kNbVaNH7GrEBeICVriAs3lw7rjXHFDB
FVFIbjGcvbKIckUnlvdnHH+d6qVo8hxM9XowFDcygAD3rPnBQxKhkC20w8RrNyvXNKIXbyrzy61
NxJ4chCLoBoHssiRjVBR4qQKzbtLdagKg8XsAB3KPHFA2M9KnyAHf7olh4MVHQVZI8N/23I5AOjO
5s+9sbmA5BeyxQHs/ZQfyaduxcPcxNMRRzvp0eRDpUfy1r25r+vMU7tTAq0Gjgg4SXTv4b+02SfM
qAGIKmC2eh6UoUKjlchbpnb057IMbS8Cvush9BpQ2yt1Q9PMP8iniQIDAQABAoIBAGZKuX9oDKMe
apUuNJhr81fgcNgtl0TL8MXi4bBuBCv2KD3EyNTRkClyJ8PU5JJI34tzPmB9fXx2WtUp8n28IrAS
QJzyPKOAqVdixT6m7Z1Vv3ysa0Xgx3QtAkw94ZQ7V1WXuQWbNNZxwgwE9tKqDFJBuUaMgbI+HT
nM
dnEOIEJ3AkSX25JquQIRpK81fac6mMdILYtEAbKveyASvUj5/Db130tq0q+4gyYnPtrWEjkroLH6
1Aaiym6L4lzGfO2poW+ombXAGpIG1s1QFvF5qNq+6iCCQekP6KhI+B23HSKpHe+/ZZpgVzWOnlpy
wZgPIYZQLkJk3+pBx5MdmrdawdECgYEA+KNThPJEOJzOJna2+8m4gZYZOkrbt7ag4pEInWrIRxRw
buP5iP0BgaC3eFlyD2Zy91sk5eEK3FVB29NtizQMhq7qRjtZCuwKclr5Kp97JxDZmiYcF9tmr//f
lotQIdV8vb3qjIPC7UYb7Qcs1IPBHwNMtLOWnOsACIYm9edDd0UCgYEAs9H+vJnns8awB/zisADw
s1O7cLyOo4JAEugAbJ2/k3ktR6izh4xqpwlI0CNS4K/xTRbYQOAmBeQpo6efdwyRrqO9pY1216qM
NGzdoIZdx6m7hYrKchQ5bW7VK6BILVRdphcD8JcxN7qjf+q0H2lISfuy/bD202cIEfCB1AnaYXUC
gYAr8bnuMI9qXhR1ad/3anSoup2k1tw0gRu4T4flQqJZSLyCbNqKoqTkg0JKCsT8QdAp9br0wiyl
Oq1UK+8dfkqEd1/Cn/Sh4lwLzhQxu1Qp2GmNPBUVBIsE2kVrNx48DSpp4qoUwajvBMgkwXLkQpNM
ZunkuiTxgPtVhlhWd9RNvQKBgQCk3HF1DpGMICvNlv9qJ+KGNs1Rxb3skL0X2FaTPmlm1qE54qR+
MLGTZR1QHyKb1xMe/0PS7u5NVmsKnOKprf9eosZ7ouADSFx0sB7dTnNqW+YNwDptLreb6hJMhg3
G
aWPWo6E8EhHQqy+9Vjw/1ExF8RqgVn9IQFqPQPZ2pXXvBQKBgEVQKaQvGtP7KFmiKfoM919dB
99b
EotKTnAEBoXqbt2IH8ReE1HB4w4nkv9gd/ab4QR5rdqAgNpwqvMIRGRB268gtzAAZ1O/K9AzUAQS
eRT/IZgZ2cwg/s/gVzDI3rt7KJhmyzvQO/N24zyVDixoAOCqVyRyh30Prwy3dpZHEtke
-----END RSA PRIVATE KEY-----
```

2.5 Security Group Set-up

***WARNING**: It is critical to the security of the Cloud Scanner instance that the AWS Security Group is correctly configured as per the guidance below. If ports have to be opened to a wider IP range than that specified, for example when testing, ensure that it is for a <u>limited</u> time period only.*

2.5.1 Security Group Background

***NOTE**: Amazon Security Groups are essentially firewall rules used to secure communications with Cloud Scanner and Cloud Load Balancer instances.*

Within EC2, you can assign your instances to user-defined groups and define firewall rules for these groups. As instances are added or removed, the appropriate rules are enforced. Similarly, if you change a rule for a group, the changes are automatically applied to all members of the group, including both running instances and instances launched in the future.

An AMI instance can be assigned to multiple groups. After an instance is running, however, the Security Groups to which it belongs cannot be changed. **Security Groups must be configured before launching an instance**.

2.5.2 Communications to be allowed by EC2 Security Group

The following communications need to be catered for by the Security Group:

- Management traffic from the SWG Policy Server (specific IP address) to the Cloud instances management ports.
- Web traffic (HTTP and HTTPS) and configuration update queries from the MSCs (which can be anywhere) to the Cloud instances.
- Web traffic from remote/branch office proxy servers (specific IPs) to the Cloud instances.

***IMPORTANT**: The EC2 firewall should only allow traffic from the customer's Policy Server IP to access the Cloud Scanner management ports.*

2.5.3 Communications to be allowed by Corporate Network Firewalls

Note that the firewalls must be configured on both the EC2 and the corporate side in order for the solution to function correctly.

- From the location of the SWG Policy Server: Management ports must be opened to the EC2 Cloud instances.
- From each remote/branch office:
  - Using a local web proxy server: Ports used by a local proxy server must be opened to the chosen EC2 Cloud instance.
  - MSC equipped users working from the office: Ports used by the MSC must be opened to the EC2 Cloud instances.

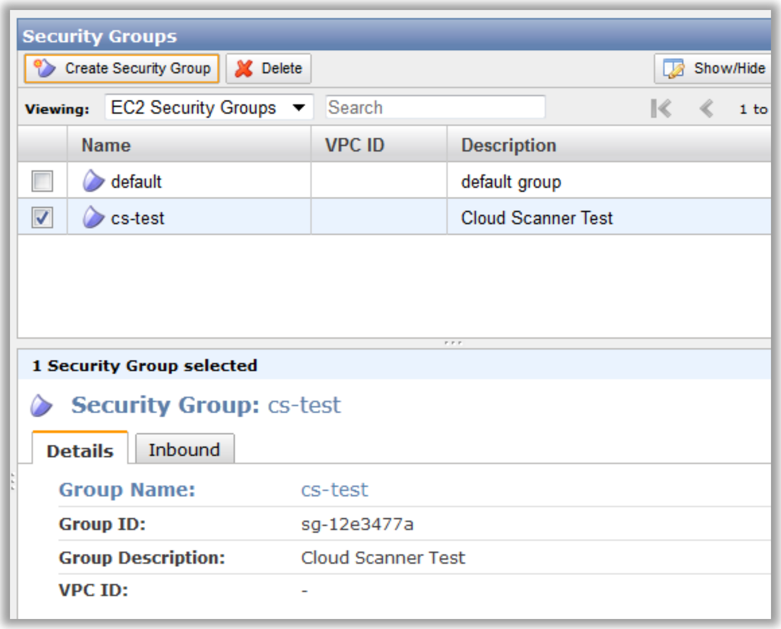
Details of the required port numbers are given in the **Security Group (Firewall Rules) Guidance** table below.

2.5.4 Configuring the Security Groups for Mobile/Roaming users

NOTE*: Security Group configuration is accessible either through the Launch Instance Wizard or before an Instance launch by clicking Security Groups in the left pane.*

To configure Security Groups (AWS Console, EC2 tab)

1. In the left Navigation pane, under the Networking & Security section, select **Security Groups**.
2. To create new Security Groups, click the Create Security Group at the top of the Security Groups work area.
3. Provide a Name and Description for the Security Group you wish to create. Click **Create**.



Viewing: EC2 Security Groups

Search

	Name	VPC ID	Description
□	default		default group
☑	cs-test		Cloud Scanner Test

1 Security Group selected

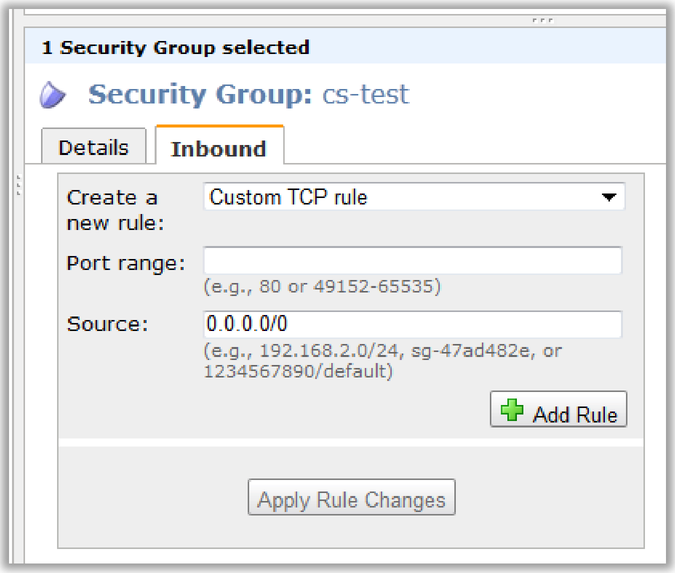
Security Group: cs-test

Details | Inbound

Group Name:	cs-test
Group ID:	sg-12e3477a
Group Description:	Cloud Scanner Test
VPC ID:	-

4. Click the newly created Security Group. The bottom window in the screen presents the group details and a separate tab for the firewall rules.

5. Click on the **Inbound** tab to begin creation of the firewall rules.



1 Security Group selected

Security Group: cs-test

Create a new rule: Custom TCP rule

Port range:
(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

6. Create one rule for each entry in the **Security Group (Firewall Rules) Guidance** table below as applicable.

Table: Security Group (Firewall Rules) Guidance

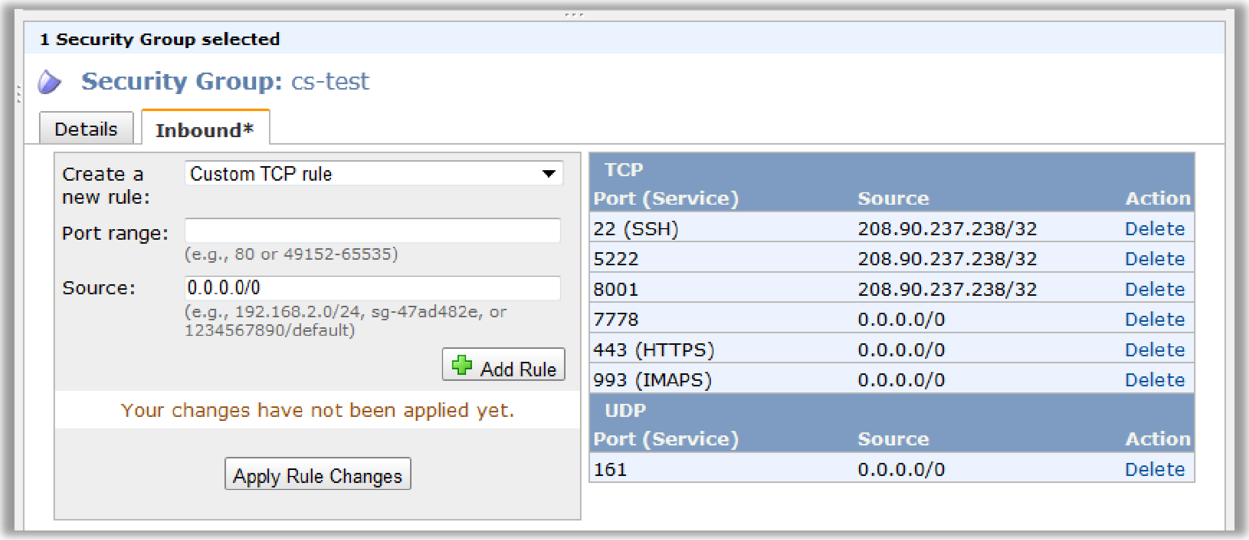
	Protocol	Port range	Source (IP address)	Guidance/Purpose
Management Ports	UDP	161 (Fixed)	SWG Policy Server IP ONLY	SNMP - used by SWG Policy Server management tools to pull data from Cloud Scanners.
	TCP	22 (Fixed)	SWG Policy Server IP ONLY	SSH - Used by Engineers to perform command line administration of the Cloud Scanner platform. Also used by the Policy Server to query for device status and perform remote actions.
	TCP	5222 (Fixed)	SWG Policy Server IP ONLY	SWG Configuration port (notifier/manager). Used by SWG Policy Server to push policy configuration to all Cloud Scanners.
	TCP	8001 (Fixed)	SWG Policy Server IP ONLY	SWG Log relaying using HTTPS. Used by SWG Policy Server to pull logs from all Cloud Scanners.
Mobile/Roaming Workers	TCP	7778 (Fixed)	Mobile/remote Workers IPs, i.e. all IPs (0.0.0.0/0)	This is the **Cloud Scanner Control port.** It is hard coded and does not change. Used by the MSC software to connect to the Cloud Scanner and receive configuration information. **NOTE**: Please do not confuse this with the Client Side Control Port which is configurable and historically made use of the same port number.
	TCP	443 (admin choice, default 443)	Mobile/remote Workers IPs, i.e. all IPs (0.0.0.0/0)	**Cloud Proxy Port for HTTP** (as per the SWG Policy Server Administration > Cloud > Configuration > Proxies (Cloud) tab). Remote workers connecting to the cloud scanner from their PC using the Secure Web Service Agent and HTTP.
	TCP	993 (admin choice, default 993)	Mobile/remote Workers IPs, i.e. all IPs (0.0.0.0/0)	**Cloud Proxy Port for HTTPS** (as per the SWG Policy Server Administration > Cloud > Configuration > Proxies (Cloud) tab). Used by the client software to connect to the Cloud Scanner from their PC using the Secure Web Service Agent and HTTPS. **Note**: Used only when HTTPS is configured on the Cloud Scanner.
Remote/Branch Office	TCP	8080 - HTTP	Remote/Branch Office External LAN IP ONLY	**WARNING**: Only IP addresses of branch offices using the EC2 located Cloud Scanner service must be allowed on this port. Failure to control access could result in an open proxy which could be exploited.
	TCP	8443 – HTTPS	Remote/Branch Office External LAN IP ONLY	**WARNING**: Only IP addresses of remote/branch offices must be allowed on this port. Failure to control access could result in an open proxy which could be exploited. **Note**: Used only when HTTPS is configured on the Cloud Scanner.

For more information on SWG port mappings, refer to:

http://www.m86security.com/software/secure_web_gateway/manuals/10.2/SWGPortMapping19042012.pdf

7. Click **Apply Rule Changes** to save the changes and put them into effect.

A sample security group configuration for a Cloud Scanner instance is shown below.



1 Security Group selected

Security Group: cs-test

Create a new rule:	Custom TCP rule
Port range:	(e.g., 80 or 49152-65535)
Source:	0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

Your changes have not been applied yet.

TCP

Port (Service)	Source	Action
22 (SSH)	208.90.237.238/32	Delete
5222	208.90.237.238/32	Delete
8001	208.90.237.238/32	Delete
7778	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete
993 (IMAPS)	0.0.0.0/0	Delete

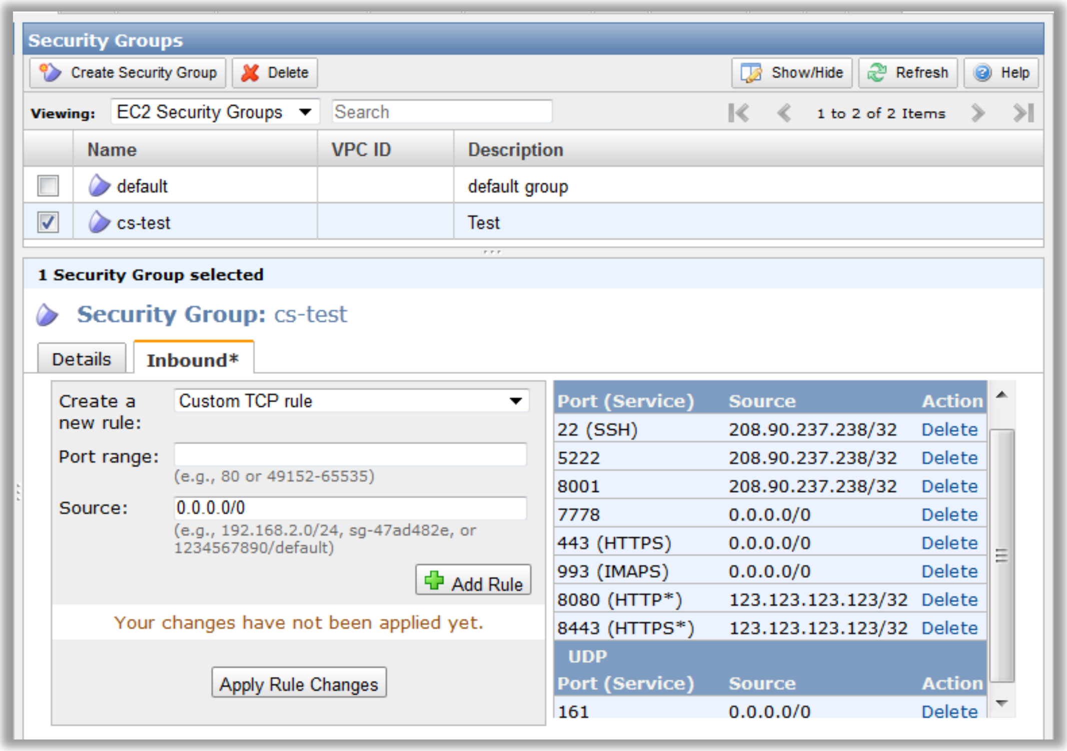
UDP

Port (Service)	Source	Action
161	0.0.0.0/0	Delete

⚠ ***IMPORTANT**: Note that the IP address of 0.0.0.0 allows for **any** and **all** remote IP addresses to use the port and protocol opened on the Security Group. The specific IP address is typically the IP address of the public internet facing router or gateway used by the SWG Policy Server to access the Cloud Scanner AWS Instance over the public internet.*

2.5.5 Remote/Branch Office Security Group Set-up

In the example below which shows the whole security groups screen, two additional firewall rules have been added to allow connection from a remote/branch office proxy using both HTTP and HTTPS.



Security Groups

Viewing: EC2 Security Groups | Search | 1 to 2 of 2 Items

	Name	VPC ID	Description
□	default		default group
☑	cs-test		Test

1 Security Group selected

Security Group: cs-test

Create a new rule:	Custom TCP rule
Port range:	(e.g., 80 or 49152-65535)
Source:	0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

Your changes have not been applied yet.

Port (Service)	Source	Action
22 (SSH)	208.90.237.238/32	Delete
5222	208.90.237.238/32	Delete
8001	208.90.237.238/32	Delete
7778	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete
993 (IMAPS)	0.0.0.0/0	Delete
8080 (HTTP*)	123.123.123.123/32	Delete
8443 (HTTPS*)	123.123.123.123/32	Delete

UDP

Port (Service)	Source	Action
161	0.0.0.0/0	Delete

For a remote/branch office configure PC browsers or your network gateway to proxy HTTP & HTTPS traffic to the Cloud Scanner.

⚠ ***IMPORTANT****: It is recommended to block port 80 from the corporate network to the internet. This way, employees will only be able to access the internet via the scanners in the Cloud and not directly.*

2.5.6 Load Balancing Solution Security Group Settings

If more than one Cloud Scanner instance is needed in a single EC2 Region, an Amazon Elastic Load Balancer will be required. For details of security group settings for Elastic Load Balancer scenarios see **Configuring the EC2 Security Group** below.

2.6 Amazon EC2 Elastic IP Set-up

Unlike traditional dedicated static IP addresses, elastic IPs can be assigned to many different instances over time. The elastic IP address owner can cover instance or scanner failures by quickly re-mapping the public IP addresses to any instance. An IP address can usually be re-mapped within a few minutes of launching an instance.

Furthermore, by using an elastic IP, there is no need for reconfiguration of the firewall (security group) because the elastic IP allows for the same scanner information that was in the failed instance to be present in the new instance.

Elastic IPs are static public IP addresses that are associated with an account and not with specific instances. Any elastic IP addresses that are associated with the account remain associated with the account until they are explicitly released.

NOTE*: It is not necessary to have an Elastic IP address for each instance, but it is highly recommended for the reasons outlined above. Every instance comes with a default private IP address and internet-routable IP address, which are fixed.*

To Allocate an Elastic IP address:

1. In the left navigation pane in the EC2 Management Console, click **Elastic IPs**.
2. In the Addresses navigation bar, click **Allocate New Address**.
3. At the prompt, click **Yes** to allocate new address.
4. A new elastic IP address now appears in the list of available elastic IP addresses. You can now assign the address to an Amazon EC2 instance.

2.7 Launching a Cloud Scanner Instance

The next step is to add or 'launch' a scanner instance. Within EC2, Cloud Scanners are displayed as Instances of M86 SWG Cloud Scanner AMIs, which are virtual representations of hardware within the cloud. An AMI is comparable to a 'product model' and an Instance is comparable to a 'Product ID' (a specific model ID of the same product).

The number of scanner instances used per customer is dependent upon the required bandwidth and performance the customer demands.

Cloud Scanner instances provide the actual protection for mobile/remote workers and remote/branch offices. In order to function correctly the earlier steps must be completed fully and correctly.

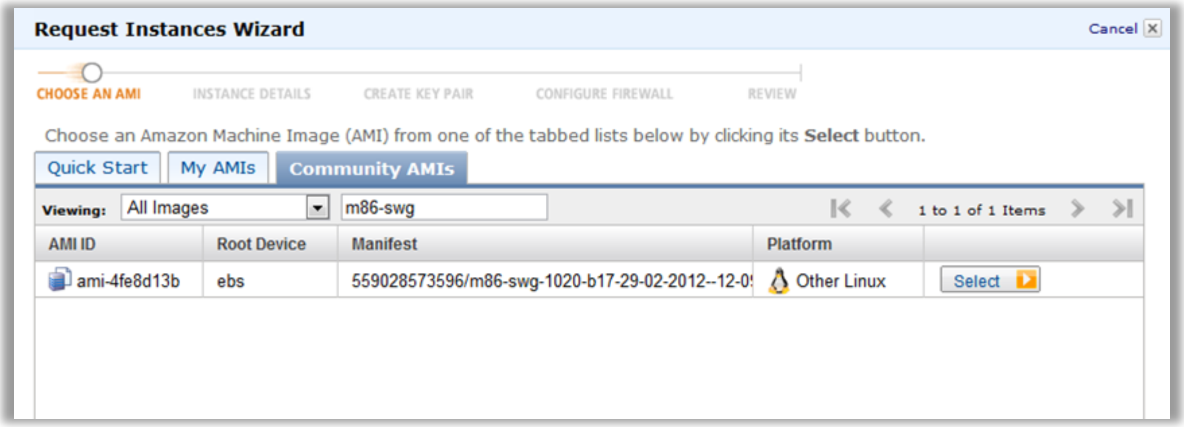
NOTE*: A Customer's Cloud Scanners instances are dedicated to and used only by themselves, even though they are part of the wider Amazon EC2 Cloud.*

***NOTE**: For details of the Cloud Scanner selection behavior consult the **M86 Mobile Security Client Administrator Guide**.*

To initiate an Instance in a regional datacenter (Region):

1. Click **Launch Instances** in the **Getting Started** panel to launch your own server. This opens the **Request Instances Wizard**.

2. Navigate to the **Community AMIs** tab. In the Viewing options drop down menu, select **All Images**.



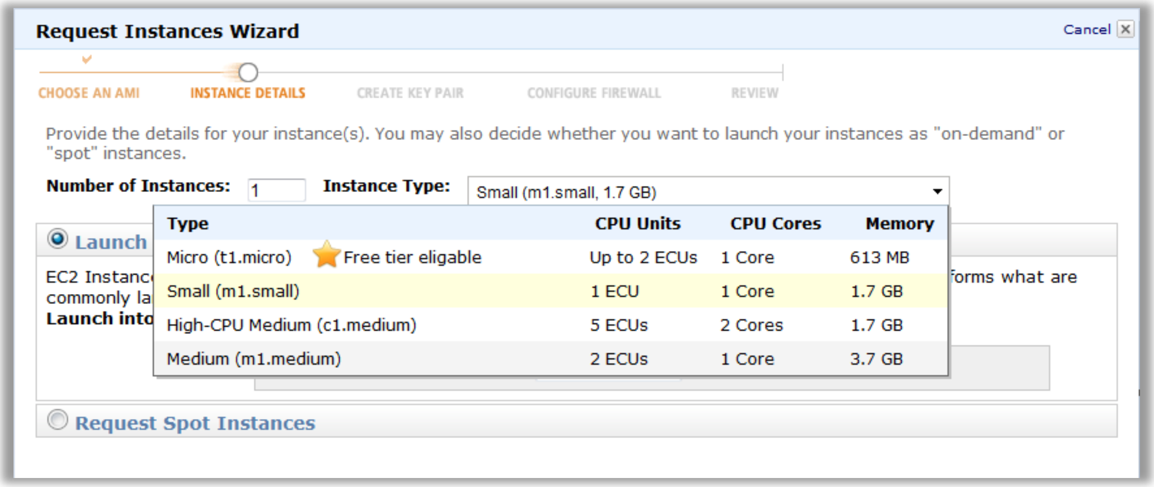
Request Instances Wizard

Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

Viewing: All Images m86-swg 1 to 1 of 1 Items

AMI ID	Root Device	Manifest	Platform	
ami-4fe8d13b	ebs	559028573596/m86-swg-1020-b17-29-02-2012--12-0!	Other Linux	Select

3. Selection of the preferred AMI and source version, for example, type "m86-swg" in the free text window. The last number in the sequence identifies the version number of the scanner.
4. To select, click the Select button to the right of the screen. Ensure that it matches the build of the Policy Server you are deploying. Contact M86 Technical Support for clarification if you do not find an exact match in the source columns version information.
5. In the following Instance Details screen, select the size instance based on the customer configuration. Additionally, select whether to use a one or three year reserved instance.



Request Instances Wizard

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: 1 **Instance Type:** Small (m1.small, 1.7 GB)

● Launch

EC2 Instanc… commonly la… **Launch into** … forms what are

Type	CPU Units	CPU Cores	Memory
Micro (t1.micro) Free tier eligable	Up to 2 ECUs	1 Core	613 MB
Small (m1.small)	1 ECU	1 Core	1.7 GB
High-CPU Medium (c1.medium)	5 ECUs	2 Cores	1.7 GB
Medium (m1.medium)	2 ECUs	1 Core	3.7 GB

○ Request Spot Instances

6. Select the number of instances to launch and the instance size, either Small (m1.small) or "High-CPU medium (c1.medium)". See Appendix A – Supported Amazon EC2 Instance Types for details.
7. Select the Availability Zone.
   a. When only one Cloud Scanner is being used choose "**No Preference**".

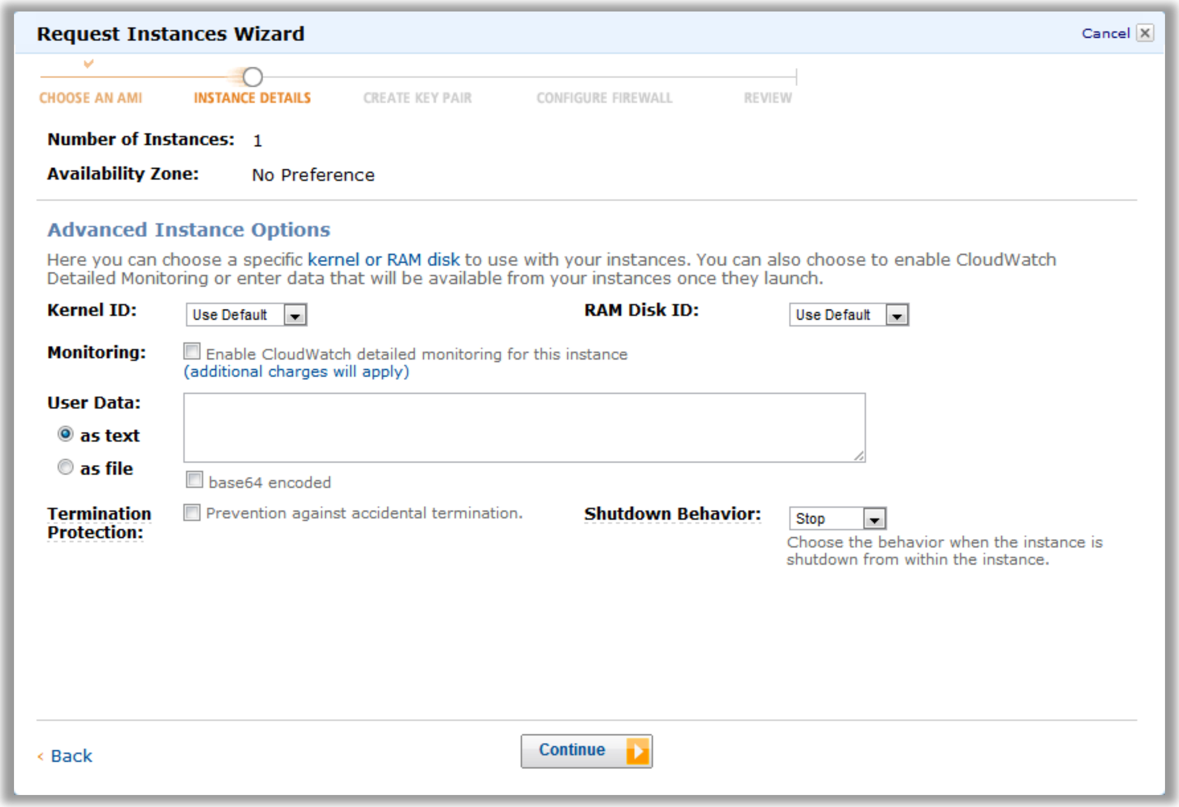
b. If more than one Cloud Scanner is being deployed in the same Region with an Elastic Load balancer see the note below:

***IMPORTANT**: Using more than one availability zone will lead to increased Amazon EC2 data transfers charges. There are two scenarios to consider:*

a) In order to minimize costs, e.g. where increasing Cloud Balancer capacity is the main consideration, ensure that all Cloud Scanners and Elastic Load Balancers are created in the same Availability Zone within a Region.

b) In order to increase resilience, choose different availability zones for each Cloud Scanner, and place the Elastic Load Balancer in the same availability zone as one of the Cloud Scanners.

8. In the next Instance Details screen, choose the given default settings. Click **Continue** to proceed.



Request Instances Wizard

Number of Instances: 1

Availability Zone: No Preference

Advanced Instance Options

Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

Kernel ID: Use Default

RAM Disk ID: Use Default

Monitoring: □ Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

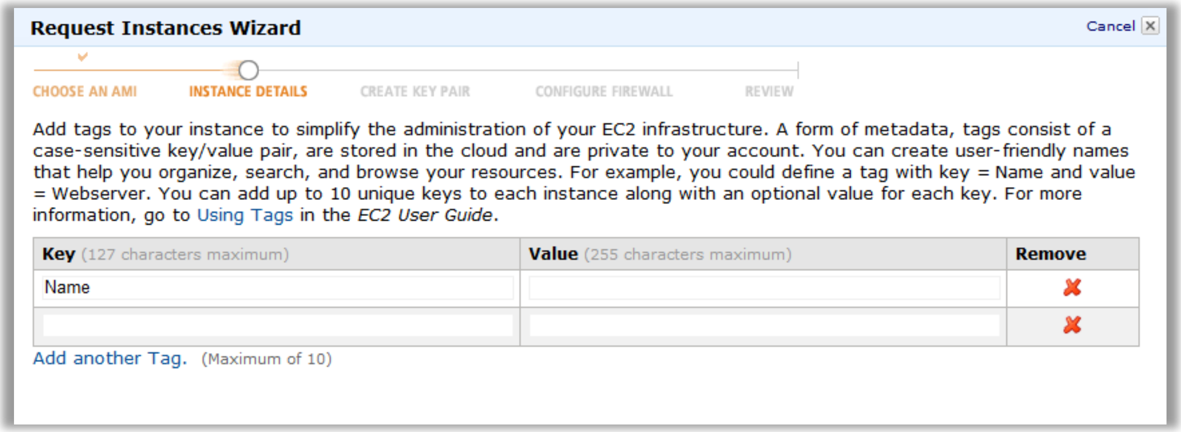
User Data:
● as text
○ as file

□ base64 encoded

Termination Protection: □ Prevention against accidental termination.

Shutdown Behavior: Stop
Choose the behavior when the instance is shutdown from within the instance.

9. In the next Instance Details screen optionally add tags to help manage your instance.



Request Instances Wizard

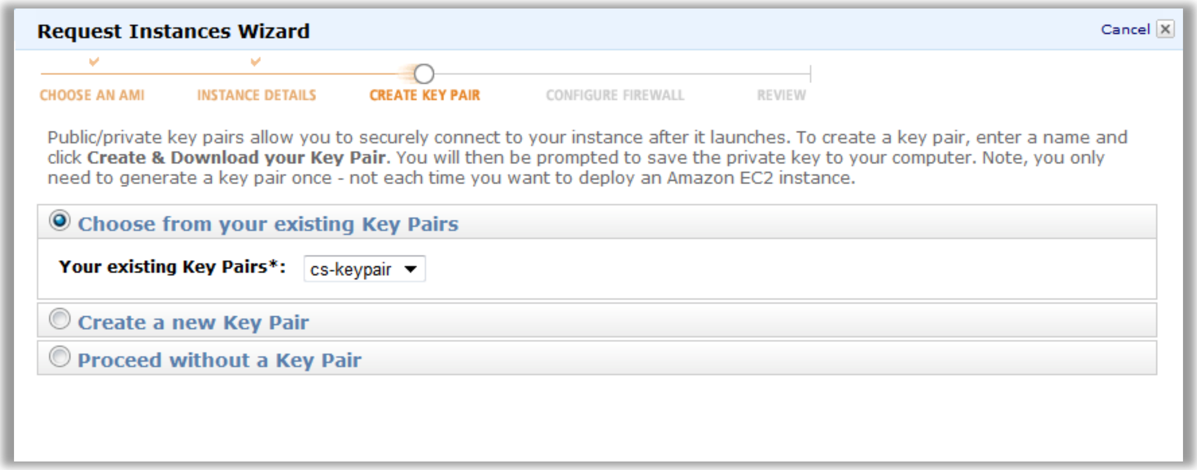
Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Using Tags in the *EC2 User Guide*.

Key (127 characters maximum)	**Value** (255 characters maximum)	**Remove**
Name		✗
		✗

Add another Tag. (Maximum of 10)

10. The **Create Key pair** screen allows you to apply the previously created key pair saved to your computer earlier in the process (see Configure Key Pairs above for further details). Enable the **Choose from your existing Key Pairs** field and select the required Key pair from the drop down menu. Click **Continue**.

NOTE: *Key Pairs need only be generated once. They do not need to be generated each time an instance is deployed.*



Request Instances Wizard

Public/private key pairs allow you to securely connect to your instance after it launches. To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

● Choose from your existing Key Pairs

Your existing Key Pairs*: cs-keypair ▼

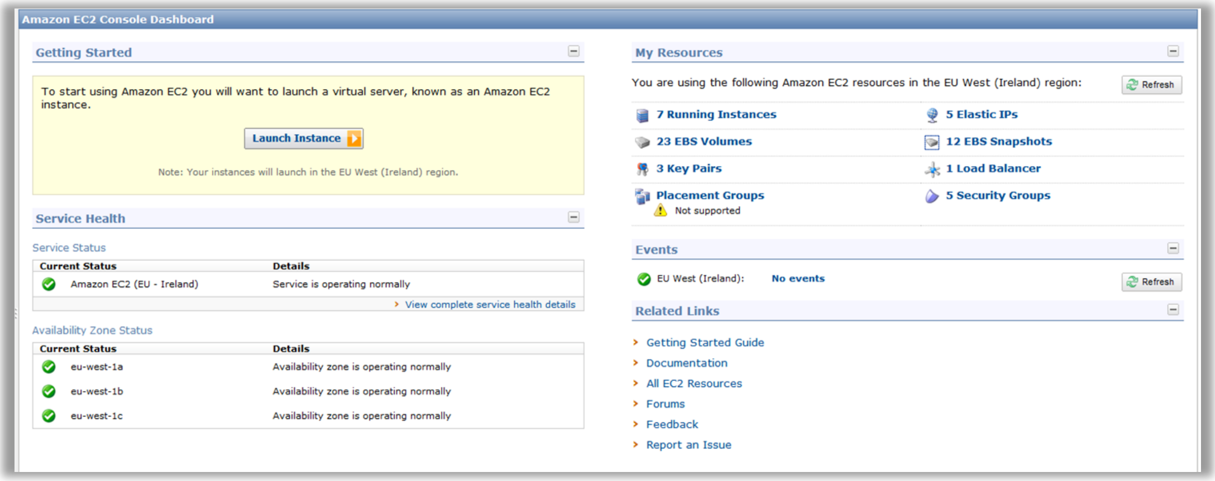
○ Create a new Key Pair

○ Proceed without a Key Pair

11. The Configure Firewall screen enables you to apply the Security Groups created earlier in the process. (See Security Groups for further details). Select the Choose one or more of your existing Security Groups checkbox and choose the required Security Group from the menu.
12. The Review screen provides all relevant details of the Instance before launching. All configurations remain editable up to this point. (Key Pairs and Firewalls are also still editable before final launch.)

NOTE: *To ensure the Security Group has been configured with the correct default ports and protocols, refer to the Security Groups section of this document for a listing of 'Allowed Connections'.*

13. Click the **Launch** button to complete the wizard and launch the instance.
14. The final screen gives an update of the instance status. Review the details once more and click **Close**.
15. Return to the main dashboard to view a summary of the client account. It should appear similar to the following:



Amazon EC2 Console Dashboard

Getting Started

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the EU West (Ireland) region.

Service Health

Service Status

Current Status	Details
✓ Amazon EC2 (EU - Ireland)	Service is operating normally

› View complete service health details

Availability Zone Status

Current Status	Details
✓ eu-west-1a	Availability zone is operating normally
✓ eu-west-1b	Availability zone is operating normally
✓ eu-west-1c	Availability zone is operating normally

My Resources

You are using the following Amazon EC2 resources in the EU West (Ireland) region:

7 Running Instances	5 Elastic IPs
23 EBS Volumes	12 EBS Snapshots
3 Key Pairs	1 Load Balancer
Placement Groups ⚠ Not supported	5 Security Groups

Events

✓ EU West (Ireland): No events

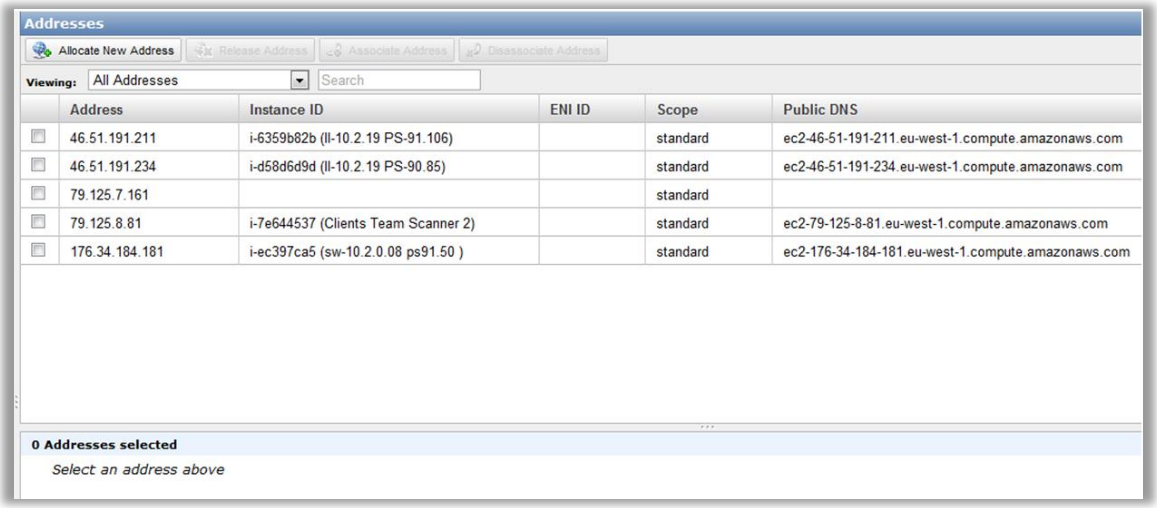
Related Links

- Getting Started Guide
- Documentation
- All EC2 Resources
- Forums
- Feedback
- Report an Issue

2.7.1 Allocate Elastic IP to the Cloud Scanner Instance

To associate an elastic IP address with an instance:

1. In the left navigation pane in the EC2 Management Console, click **Elastic IPs**.
2. Select an IP address to associate. In the addresses navigation bar, click the **Associate** button.
3. At the prompt, click **Associate** to connect the new address.
4. Select the instance and click **Associate**. The current public IP address is no longer associated, and the new elastic IP address is now associated with the instance.



	Address	Instance ID	ENI ID	Scope	Public DNS
□	46.51.191.211	i-6359b82b (ll-10.2.19 PS-91.106)		standard	ec2-46-51-191-211.eu-west-1.compute.amazonaws.com
□	46.51.191.234	i-d58d6d9d (ll-10.2.19 PS-90.85)		standard	ec2-46-51-191-234.eu-west-1.compute.amazonaws.com
□	79.125.7.161			standard	
□	79.125.8.81	i-7e644537 (Clients Team Scanner 2)		standard	ec2-79-125-8-81.eu-west-1.compute.amazonaws.com
□	176.34.184.181	i-ec397ca5 (sw-10.2.0.08 ps91.50)		standard	ec2-176-34-184-181.eu-west-1.compute.amazonaws.com

0 Addresses selected

Select an address above

The procedure above is an initial startup configuration of a Security Group for a Cloud Scanner AWS Instance running on AWS EC2. Note that the IP address of 0.0.0.0 allows for any and all remote IP addresses to use the port and protocol opened on the Security Group. The specific IP address (in this case 208.90.237.238/32) is typically the IP address of the public internet facing router or gateway used by the Policy Server to access the Cloud Scanner AWS Instance over the public internet.

2.7.2 Configure local network to use Cloud Scanners (remote/branch office)

Computers managed through the remote/branch office that do not have the Mobile Security Client software installed, can use an HTTP proxy protocol to access the Cloud Scanner. By default, the Cloud Scanner is configured to listen on port 8080. The Administrator should configure the EC2 Security Group to permit traffic with a source IP. This source IP should be the Branch Offices' public NAT IP or Subnet, which accesses the Cloud Scanner.

***NOTE**: For security reasons, it is recommended to configure the Cloud Scanner Security Group to block proxy communication from the Public Internet and restrict it only to the remote/branch office's IP address.*

Add LAN Public IP to the Security Group Policy:

1. Sign-in to the EC2 Management Console.
2. In the left navigation pane, click **Security Groups**.
3. Select the **Security Group** required for configuration.
4. The **Security Group Permissions** pane, which shows Group rules currently in use, appears at the bottom of the screen.
5. Fill in the **Protocol, From Port**, and the **To Port** fields.
6. To configure this rule to apply to an IP address range, enter the source IP in the **Connection Source (IP or Group)** field. Enter an IP address and subnet mask to limit access to that one computer or network, for example 192.168.0.0/16.

7. Click **Save**.

Set your Client's Browsers or your network Gateway to proxy HTTP & HTTPS traffic to the Chosen Cloud Scanner.

For details of the Security Group Configuration required, consult **Security Group (Firewall Rules) Definition Suggestions** table in section 2.5 Security Group above.

NOTE*: It is recommended to block port 80 from the corporate network to the internet. This way, employees will only be able access the internet via the Cloud Scanner and not directly.*

2.7.3 Load Balancers (multiple Cloud Scanner instances in a Region)

If more than one Cloud Scanner Instance is required in a given EC2 region, e.g. 2 in Europe in order to meet user capacity requirements, then an Elastic Load Balancer will be needed. Details are provided in section 3 Elastic Load Balancer below.

2.8 Next Steps

Once the EC2 setup is complete, the SWG Policy Server cloud configuration must now be implemented. For details see the **M86 Security SWG Hybrid Deployment Guide** document.

3 Elastic Load Balancer

__WARNING__: Use an Amazon Elastic Load Balancer only with Cloud Scanner instances in the same EC2 Availability Zone within a Region; otherwise data transfer costs will rise. Resilience is gained by failing over to another region as opposed to using multiple availability zones in the same region.

This section describes the steps required to set up an Amazon ELB instance for a set of SWG Cloud Scanners.

3.1 Requirements

SWG Version: In order to perform reliable health checking of the scanner, the scanner should have Hybrid Agent 2.0 (SWG 10.2) or higher installed. For previous versions of the Hybrid Agent, a more limited form of health checking is available.

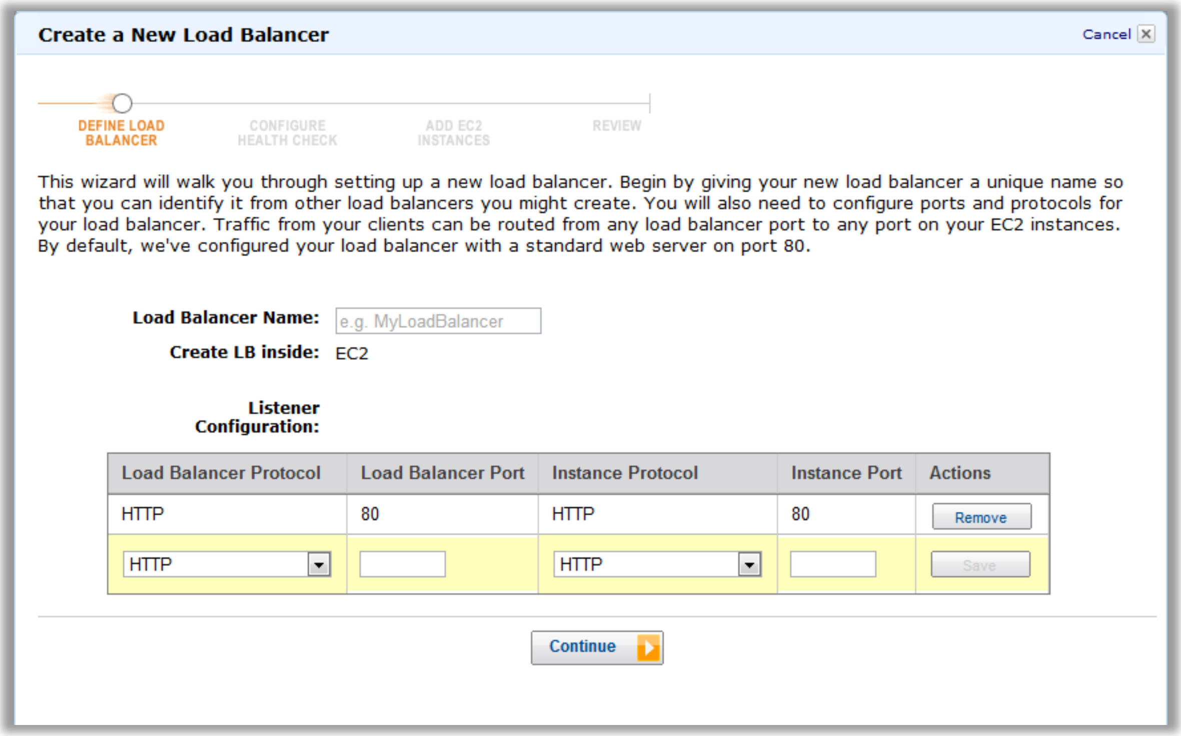
Load Balancer Type: Only the Amazon Elastic Load balancer is supported for use with M86 SWG Cloud Scanner instances.

3.2 Configuring the ELB:

To configure and Elastic Load Balancer:

1. From the AWS Management Console choose **Load Balancers** from the Navigation menu and then click on **Create Load Balancer**.

   c. Initial Definitions.



Create a New Load Balancer

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer Name: e.g. MyLoadBalancer

Create LB inside: EC2

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Actions
HTTP	80	HTTP	80	Remove
HTTP		HTTP		Save

   d. Give your load balancer a name.

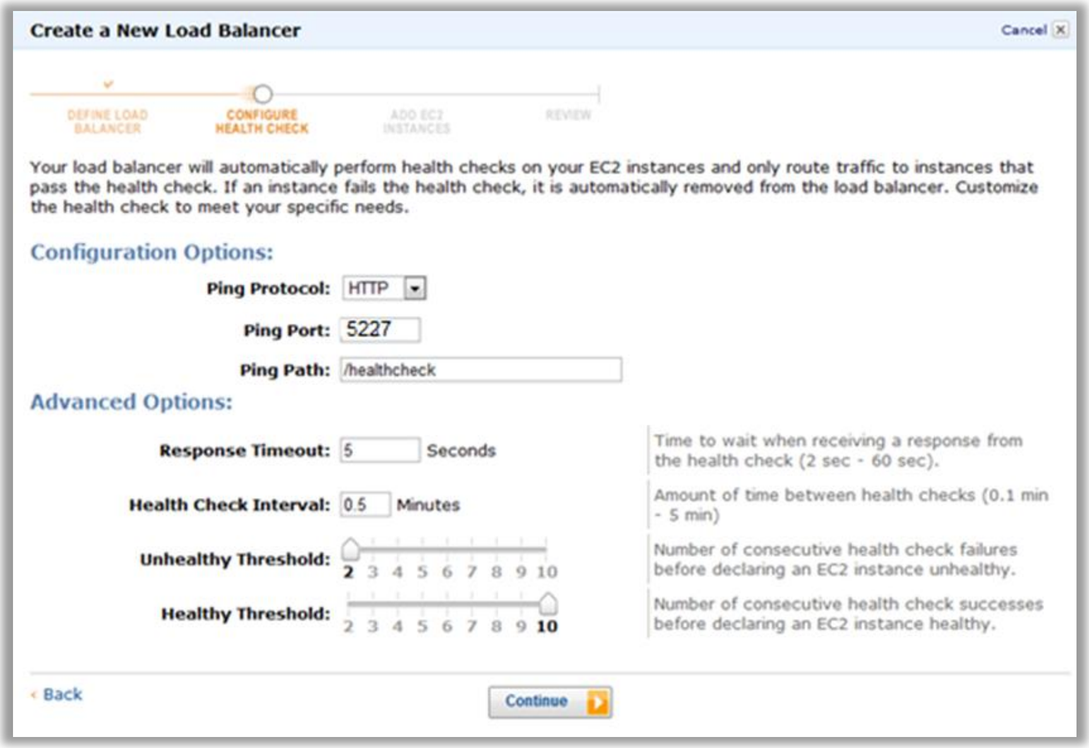
   e. Remove the default forwarding of port 80.

   f. For each of the cloud proxy ports (http and https) defined in the Cloud Configuration screen of the PS, add a line with information from the following table:

Load Balancer Protocol	**TCP**[2]
Load Balancer Port	As defined on the SWG Policy Server.
Instance Protocol	**TCP**[1]
Instance Port	As defined on the SWG Policy Server.

Before pressing continue ensure that all of the parameters are correct. There is no way to change these parameters after the ELB is defined; the only option is to recreate the ELB. Press **Continue**.

2. Health Check Configuration


Create a New Load Balancer

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Configuration Options:

Ping Protocol: HTTP

Ping Port: 5227

Ping Path: /healthcheck

Advanced Options:

Response Timeout: 5 Seconds — Time to wait when receiving a response from the health check (2 sec - 60 sec).

Health Check Interval: 0.5 Minutes — Amount of time between health checks (0.1 min - 5 min)

Unhealthy Threshold: 2 — Number of consecutive health check failures before declaring an EC2 instance unhealthy.

Healthy Threshold: 10 — Number of consecutive health check successes before declaring an EC2 instance healthy.

For users of release 2.0 (SWG 10.2) and higher: On the **Configure Health Check** screen you should set the following parameters

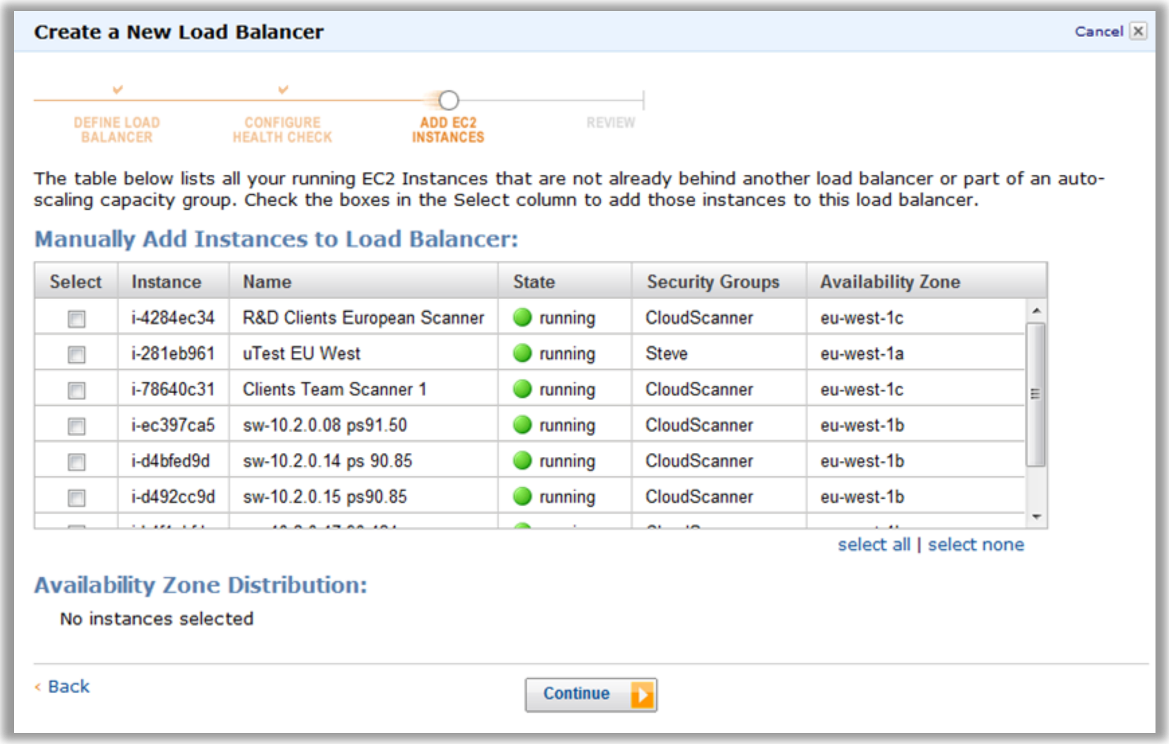
Ping Protocol	**http**
Ping Port	5227
Ping Path	**/healthcheck**

There is no need to change the parameters in the Advanced Options. A **Response Timeout** of 5 seconds is reasonable. Reducing the **Health Check Interval** may reduce the time before unhealthy scanners are removed from the Load Balancer. If you lower this value, consider increasing the **Unhealthy Threshold**. Reducing the **Healthy Threshold** may cause scanners to be re-added to the Load Balancer earlier.

Press **Continue**.

[2] Note: The use of TCP rather than HTTP or HTTPS. TCP is correct.

3. Adding Cloud Scanner to Load Balancer



The table below lists all your running EC2 Instances that are not already behind another load balancer or part of an auto-scaling capacity group. Check the boxes in the Select column to add those instances to this load balancer.

Manually Add Instances to Load Balancer:

Select	Instance	Name	State	Security Groups	Availability Zone
□	i-4284ec34	R&D Clients European Scanner	● running	CloudScanner	eu-west-1c
□	i-281eb961	uTest EU West	● running	Steve	eu-west-1a
□	i-78640c31	Clients Team Scanner 1	● running	CloudScanner	eu-west-1c
□	i-ec397ca5	sw-10.2.0.08 ps91.50	● running	CloudScanner	eu-west-1b
□	i-d4bfed9d	sw-10.2.0.14 ps 90.85	● running	CloudScanner	eu-west-1b
□	i-d492cc9d	sw-10.2.0.15 ps90.85	● running	CloudScanner	eu-west-1b

Availability Zone Distribution:

No instances selected

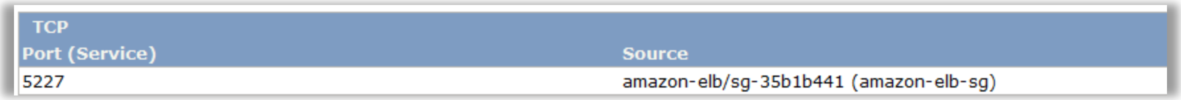
Select the cloud scanners that should be connected to this Load Balancer and finish creating the ELB instance.

3.3 Configuring the EC2 Security Group

The EC2 security group containing the Cloud Scanners must be configured to accept requests from the ELB on port 5227 (see below for firewall rule example).

To configure the EC2 Security Group for a Load Balancer:

1. From the AWS Management Console choose **Instances** from the Navigation menu.
2. Note the value of the **Security Groups** field.
3. Choose Security Groups from the Navigation menu.
4. Select the Security Group that you noted in step 2 from the list of Security Groups.
5. Click on the **Inbound** tab of the Security Group Configuration.
6. In the Port Range field enter **5227**.
7. In the source field we will enter the Security Group of the ELB. By default this is amazon-elb\ amazon-elb-sg. At present there does not appear to be any way of changing the Security Group of the ELB.



TCP Port (Service)	Source
5227	amazon-elb/sg-35b1b441 (amazon-elb-sg)

Set the SWG Policy Server Cloud Configuration to use the ELB as though it were a Cloud Scanner.

***NOTE**: Although the other Cloud Scanner instances will need to be defined as Scanning Devices in the SWG Policy Server, ELBs do <u>not</u> need to be defined as Scanning Devices.*

Appendix A – Supported Amazon EC2 Instance Types

As part of an M86 SWG 10.2 deployment the SWG Cloud Scanner AMI provides users with the ability to extend web security and filtering to roaming/mobile/remote users in each of the Amazon EC2 regions.

Compatibility:

This AMI will function only with M86 SWG v10.2 implementations; it is not backward compatible with earlier SWG versions.

Instance Types & Settings:

Instance Type: “**Small**” and “**High-CPU Medium**” only.

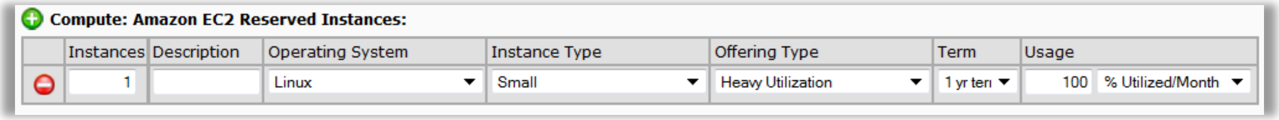
Reserved instance recommended – this should produce the lowest running costs but involves commitment of one year minimum and up-front costs. http://aws.amazon.com/ec2/reserved-instances/?ref_=pe_12300_21983840

Operating system: **Linux**

Offering Type: **Heavy Utilization**

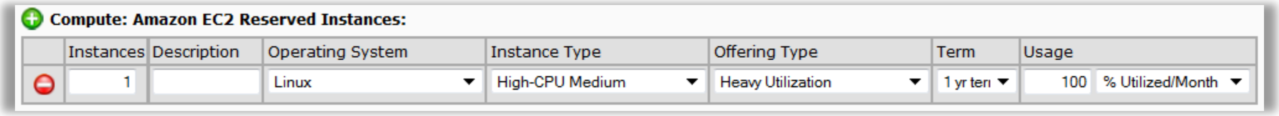
Usage: **100%**

Example screen shots from Amazon EC2 price calculator (http://calculator.s3.amazonaws.com/calc5.html):



Compute: Amazon EC2 Reserved Instances:

	Instances	Description	Operating System	Instance Type	Offering Type	Term	Usage	
⊖	1		Linux	Small	Heavy Utilization	1 yr ten	100	% Utilized/Month



Compute: Amazon EC2 Reserved Instances:

	Instances	Description	Operating System	Instance Type	Offering Type	Term	Usage	
⊖	1		Linux	High-CPU Medium	Heavy Utilization	1 yr ten	100	% Utilized/Month

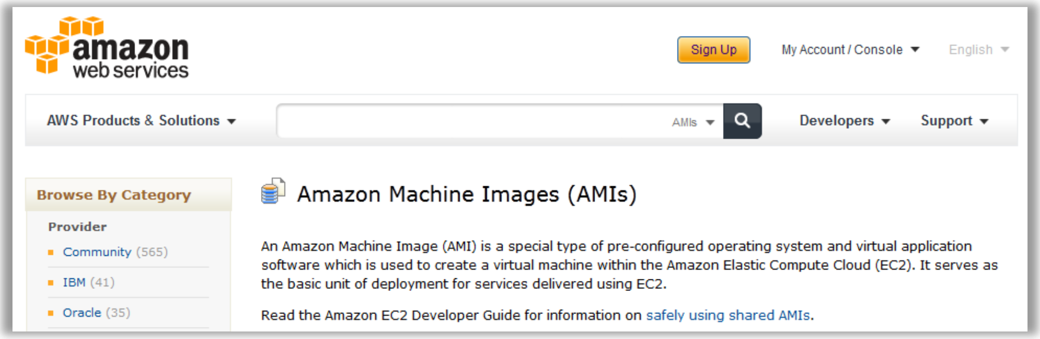
Supported EC2 Regions:

The following Amazon EC2 regions are supported: APAC (Tokyo), APA (Singapore), Europe (Eire), South America (Sao Paulo), US East (Virginia), US West (California), US West (Oregon).

Locating the AMI:

To locate available M86 Security SWG Cloud Scanner AMIs use:

https://aws.amazon.com/amis?_encoding=UTF8&jiveRedirect=1 and Search for “m86-swg”.



Amazon Machine Images (AMIs)

An Amazon Machine Image (AMI) is a special type of pre-configured operating system and virtual application software which is used to create a virtual machine within the Amazon Elastic Compute Cloud (EC2). It serves as the basic unit of deployment for services delivered using EC2.

Read the Amazon EC2 Developer Guide for information on safely using shared AMIs.

Appendix B – Useful Links

M86 Security Documentation: http://www.m86security.com/support/Secure-Web-Gateway/Documentation.asp

General Amazon EC2 www.amazon.com/ec2

EC2 documentation: http://aws.amazon.com/documentation/

Elastic Compute User Guide: http://awsdocs.s3.amazonaws.com/EC2/latest/ec2-ug.pdf

EC2 Reserved instances: http://aws.amazon.com/ec2/reserved-instances/?ref_=pe_12300_21983840

EC2 what's new?: https://aws.amazon.com/about-aws/whats-new/

EC2 Elastic Load Balancing: http://aws.amazon.com/elasticloadbalancing/?ref_=pe_8050_21124970

EC2 Global Infrastructure: http://aws.amazon.com/about-aws/globalinfrastructure/?ref_=pe_12300_21749180

Regions and Availability Zones: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

---

About M86 Security

M86 Security is the global authority in malware prevention and content security. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit www.m86security.com.