Secure Web Service Hybrid - Frequently Asked Questions

July 2010

FAQ about M86 Secure Web Service Hybrid
# Table of Contents

## Overview
1. What is M86’s SWS-H Solution? 4
2. What is M86’s SWS-H Hybrid Solution? 4
3. Where does SWS-H work? 4
4. What are the benefits of SWS-H? 4
5. What are the cost savings to enterprises using SWS-H? 5
6. Is SWS-H really unique? Are other vendors offering similar solutions? 5
7. How can customer evaluate SWS-H? 5

## Remote Worker: Technical Details
1. What is split tunneling? 6
2. Does the VPN have to be in split tunnel mode or full tunnel mode? 6
3. What happens to users visiting a 3rd party client site? 6
4. What happens when the user wants to register to a public hotspot? 6
5. What happens when the remote user is connected to the organization’s LAN? 6
6. Does SWS-H also scan Intranet traffic? 6
7. How is the SWS-H client provisioned to the end client? 7
8. Can the user disable SWS-H Client? 7
9. What is a SWS-H Client? 7
10. Can a user disable the SWS-H? 7
11. On which operating systems is the SWS-H Client supported? 7
12. Is it possible for current users to use multiple logins on multiple desktops? 7
13. Can PAC files be centrally managed for global users? 8

## Branch Office: Technical Details
1. Must SWS-H Clients also be used in branch office deployment? 9
2. When should the SWS-H Client be used at branch offices? 9
3. How does SWS-H authenticate end-users in a branch office deployment? 9
4. What time zone does SWS-H use? 9

## SWS-H Hybrid: Technical Details
1. When is the on-premise Secure Web Gateway the recommended solution? 10
2. What makes M86’s SWS-H Hybrid for the borderless enterprise such a unique solution? 10
Deployment
1. What is Amazon EC2? 11
2. What is the latency impact when using SWS-H? 11
3. What is the SWS-H Scanner performance and sizing? 11
4. How many scanners are needed? 12
5. Which version of the NG Policy Server supports the SWS-H? 12
6. What is currently not supported in SWSH? 12

Competition
1. Where can I find information about the competitive landscape and SWS-Hs added-value? 13

Business Model and Pricing
1. What is the SWS-H Pricing and what is the SWS-H business model? 14

Quality of Service and Service Level Agreements
1. What is the uptime of the SLA? 15
2. Who manages and monitors the scanners in the cloud? 15
3. What happens when the SWS-H Scanner is unreachable by the Client? 15
4. What happens when the SWS-H Scanner is unreachable by the Policy Server? 15
5. How do I keep my SWS-H with the latest updates? 15
6. How do I upgrade to upcoming SWS-H versions? 16
7. What should a customer having a problem with a scanner-in-the-cloud do? 16
8. Is there a customer support system in place? 16
9. How many SWS-H datacenters are available? 16
10. Is there a new EULA for SWS-H? 16

Compliance and Security
1. How does SWS-H help protect data privacy and integrity? 17
2. Is SWS-H a secure environment? 17
3. Is EC2 certified by SAS 70 Type II? 17
4. Is SWS-H PCI-Compliant? 18
5. Can customers visit and audit EC2 datacenters? 18
6. How is SWS-H built to reduce the impact of a DDOS attack? 18
Overview

1. **What is M86’s SWS-H Solution?**

   M86’s SWS-H is a Web Security Gateway hosted in the cloud. M86’s SWS-H provides unified web security to an entirely borderless enterprise, including corporate headquarters, remote workers and branch offices, while keeping costs at a minimum.

   M86’s SWS-H is available in two deployment models; a cloud-based solution, and a hybrid model that combines both an on-premise and cloud-based solution.

2. **What is M86’s SWS-H Hybrid Solution?**

   M86’s SWS-H Hybrid model is the world’s first web security solution for the borderless enterprise consisting of a hybrid model combining on-premise appliances and in-the-cloud scanners. M86’s SWS-H hybrid deployment model provides enterprises with a smooth transition from on-premise web security to Web Security-as-a-Service (SaaS). The unique combination of on-premise and in-the-cloud web security enables enterprises to enjoy the best of both worlds.

   The SWS-H Hybrid model provides organizations with the most effective balance of on-premise appliances, and scanners in-the-cloud tailored to specific topologies and requirements.

3. **Where does SWS-H work?**

   SWS-H works at any location where roaming employees connect to the Internet. These may include; remote branch offices, at home, hotel rooms, client premises, coffee shops or public Wi-Fi hotspots.

4. **What are the benefits of SWS-H?**

   - Extends secure Internet connectivity to office workers in branch offices, and all employees regardless of location (roaming).
   - Reduces the risk of infected laptops reconnecting to the office LAN.
   - Reduces the TCO of branch Internet security by moving real-time scanning into the cloud.
   - Simplifies management by eliminating endpoint client hassle or continuous updating.
• Reduces network bandwidth congestion and latency as there is no need to backhaul traffic via a VPN.
• Simplifies use for internal users. No need for VPN software to connect to the Internet.

5. **What are the cost savings to enterprises using SWS-H?**

- No need to backhaul all data via a VPN or lease line, hence large bandwidth savings.
- No large cleanup expenses when remote users become infected, since there is no enforced backhaul via a VPN.
- Minimized re-routing latency which avoids traffic flow through other countries via slow VPN or leased-line connections.

6. **Is SWS-H really unique? Are other vendors offering similar solutions?**

SWS-H Hybrid is the world’s first true hybrid solution. It combines on-premise appliances and cloud-based scanners for the borderless enterprise. All other vendors in the marketplace offer either a pure cloud-based solution (SaaS), or extend their on-premise solution with an additional cloud-based solution.

7. **How can customer evaluate SWS-H?**

To evaluate M86’s SWS-H, please contact your M86 representative or contact sales@M86.com
Remote Worker: Technical Details

1. **What is split tunneling?**

   Split tunneling is a VPN term. In computer networking, it means that data that is bound for the corporate network is tunneled back to the corporate gateway via the VPN. All other traffic is routed to the Internet directly.

2. **Does the VPN have to be in split tunnel mode or full tunnel mode?**

   Remote workers with a SWS-H Client should use VPN in split tunnel mode. Alternatively, the VPN can be disabled altogether.

   All Internet Web traffic (both HTTP and HTTPS) should be allowed to go directly to the Internet. The SWS-H Client will redirect this traffic to the SWS-H Scanners.

3. **What happens to users visiting a 3rd party client site?**

   The SWS-H Client has been designed to work through third party proxies and transparent proxies that do not inspect SSL traffic. It will therefore work at 3rd party client sites smoothly.

4. **What happens when the user wants to register to a public hotspot?**

   The SWS-H Client has been designed to work through public hotspots that require registration. Upon registration, all traffic will be redirect to the SWS-H scanning infrastructure and the correct policies will be applied.

5. **What happens when the remote user is connected to the organization’s LAN?**

   SWS-H Client can be configured to bypass SWS-H. It can seamlessly use the local organization’s Secure Web Gateway or Proxy when Client is connected to corporate LAN.

6. **Does SWS-H also scan Intranet traffic?**

   No. traffic destined to the LAN would bypass SWS-H and be sent directly.
7. **How is the SWS-H client provisioned to the end client?**

SWS-H Client provisioning includes installation of a small application, as well as a user certificate. Both can be provisioned in one of the following three ways:

1. Via a provisioning email that is automatically sent from the Policy Server to the target user.
2. Manually by the IT administrator on behalf of the end user.
3. An agent can be auto-installed via a Group Policy (GRO) or Microsoft SMS and users’ certificates (PKI).

8. **Can the user disable SWS-H Client?**

Administrators can define a policy preventing end users from disabling the SWS-H. They can also enforce the browsers (in V1 to Internet Explorer and Firefox) proxy settings to use the SWS-H.

9. **What is a SWS-H Client?**

Remote clients should have the SWS-H Client installed. The local client’s browsers are configured to use this client as their default proxy via a PAC file. SWS-H Client then uses a secure SSL tunnel to redirect all traffic to SWS-H Scanners.

10. **Can a user disable the SWS-H?**

Administrator can configure SWS-H to be tamper-proof, thus preventing the user from disabling or bypassing SWS-H.

11. **On which operating systems is the SWS-H Client supported?**

The SWS-H Client runs on *Windows XP, Windows Vista and Windows 7* (all editions).

12. **Is it possible for current users to use multiple logins on multiple desktops?**

Yes. Any user can use a PKI mechanism to auto enroll the target client with a user certificate. Users would not be able to use SWS-H from a non-provisioned machine. In future releases, M86 may also limit the number of concurrent connections per user.
13. Can PAC files be centrally managed for global users?

Yes, SWS-H uses GEO DNS to redirect traffic to the closest datacenter.
1. *Must SWS-H Clients also be used in branch office deployment?*
   
   No. All client traffic is routable to M86’s SWS-H in proxy mode, either directly from the browsers or from a downstream proxy.

2. *When should the SWS-H Client be used at branch offices?*
   
   It is recommended to deploy SWS-H Client on unmanaged computers or computers deployed in workgroup environments.

3. *How does SWS-H authenticate end-users in a branch office deployment?*
   
   SWS-H can be configured to accept authentication delegation from a downstream proxy or can be configured to identify logged-on users (by using HTTP Error 407 - Proxy authentication required).

4. *What time zone does SWS-H use?*
   
   Time-based policy does not relate to the client time zone but to the actual scanner time zone to which the client is connected. Customers may have scanners both in the US with the US time zone (only one per region) and in the EU with the EU time zone (only one per region).
SWS-H Hybrid: Technical Details

1. When is the on-premise Secure Web Gateway the recommended solution?

M86’s on-premise Secure Web Gateway is recommended for large enterprises with hundreds of users at corporate headquarters with a local IT staff. This provides reduced TCO as well as better latency and control.

2. What makes M86’s SWS-H Hybrid for the borderless enterprise such a unique solution?

- It is only available solution that allows IT administration to centrally manage the policy for both Secure Web Gateway appliances and Secure Web Gateway virtual cloud scanners.
- It is the only solution where remote users can take advantage of the cloud service when roaming, and the on-premise appliance scanners when connected to organization LAN.
- It is the only solution that archives logs on-premise. As such, internal and external Internet usage can be combined in reporting and management overviews.
- SWS-H offers the best integration with the IT infrastructure currently available on the market. It offers full AD integration, can be monitored by enterprise monitoring tools (such as Tivoli or HP Open Viewer) and allows administration roles based on domain groups.
Deployment

1. **What is Amazon EC2?**

   M86 SWS-H is hosted within the Amazon Elastic Compute Cloud (Amazon EC2). For more details about EC2 visit: [http://aws.amazon.com/ec2/](http://aws.amazon.com/ec2/)

2. **What is the latency impact when using SWS-H?**

   Customers using SWS-H in the US, Europe as well as Egypt and Singapore have experienced impressive performance.

   **HMSHost:** “With the cloud solution, we will have better control of our roaming users and all that with a stunning performance…”

   Branch offices and remote workers currently using VPN to access the Internet should experience notable improvement when switching to SWS-H.

   Currently, Amazon has two datacenters; one in North America and one in Europe (Ireland). Therefore, customers from these continents will experience the highest rate of performance. Moreover, customers from other continents should not experience any performance degradation whatsoever when browsing websites hosted in Europe or the US.

   In order to offer the best performance, the SWS-H Agent automatically connects to the nearest available scanner, be it in the cloud or in the corporate LAN.

   The outstanding Internet backbone and high-throughput available in the Amazon datacenters is one of the main reasons the M86 SWS-H browsing experience and performance is so remarkable.

   We encourage customers from all over the world to experience M86 SWS-H performance by joining the M86 SWS-H Trial.

3. **What is the SWS-H Scanner performance and sizing?**

   Amazon offers different type of Instances. To learn more about Amazon Instances, please visit [http://aws.amazon.com/ec2/#instance](http://aws.amazon.com/ec2/#instance)

   The performance of one Medium-Type-High-CPU-On-Demand Instance would be slightly better than the NG-5000 appliance. The sizing of M86 Cloud should be based on the NG-5000 with additional factor of 10%.
4. **How many scanners are needed?**

Customers can start with only one scanner and add more scanners (as explained in the performance & sizing specification). Global customers should consider using scanners both in the US and EU datacenters.

It takes only minutes to add and remove scanners, therefore customers are free to add or remove scanners according to their needs.

5. **Which version of the NG Policy Server supports the SWS-H?**

Customer should run version 9.2.5 or above of NG Policy Server or All-In-One appliance.

6. **What is currently *not* supported in SWSH?**

The following network topologies will work within the local network, but currently not in the cloud:

- **ICAP**: Server settings required to enable communication between a third party ICAP client with the respective M86 ICAP server service/device.
- **FTP**: The Scanning Server FTP screen displays the FTP definition for the specified device. The FTP area allows you to configure your organization's FTP settings.
- **WCCP**: Protocol which enables WCCP enabled routers (and switches) to redirect traffic to other WCCP enabled servers, without the need for the users to configure their browsers or any other proxy settings.
- **Caching**: Using an HTTP caching element in the system ensures that content delivery to end-users is accelerated. When content is delivered from a local cache after download, there is no need to reload identical content for each user's subsequent request, therefore reducing the end-user's response time.

**NOTE:** The above mentioned topologies may be implemented in one of the upcoming major releases.
Competition

1. Where can I find information about the competitive landscape and SWS-Hs added-value?

For more information about M86’s SWS-H, its differentiators and the competitive landscape, please refer to the following two documents available on the M86 Sales Portal:

1. SWS-H Battle Card
2. How Do M86’s Web Security Solutions differ from…?
Business Model and Pricing

1. What is the SWS-H Pricing and what is the SWS-H business model?

   For information on SWS-H pricing and the SWS-H business model, please refer to the following two documents available on the M86 Sales Portal:

   1. SWS-H Business Model
   2. SWS-H Pricing
Quality of Service and Service Level Agreements

1. **What is the uptime of the SLA?**
   Amazon EC2 service offers 99.95% availability for each EC2 Region. Customer may choose to have scanners hosted in different EC2 zones within the same region, as well as in different EC2 regions in order to enjoy maximum uptime.

2. **Who manages and monitors the scanners in the cloud?**
   M86 offers two options for end customers:
   1. Managed by the customer’s IT: Managing the scanner in the cloud is easy. To reduce TCO and for maximum privacy, customer IT can directly manage the scanners in the cloud.
   2. Managed by MSSP: Customers can outsource cloud management to an MSSP certified by M86.

3. **What happens when the SWS-H Scanner is unreachable by the Client?**
   In that case, the SWS-H Scanner will try to connect to an alternate scanner. If no other scanner is available, SWS-H Client will continue to look for available scanner and when found, it will redirect the traffic to this scanner.

4. **What happens when the SWS-H Scanner is unreachable by the Policy Server?**
   In that case, the scanner will continue to run with the last known policy. Logs will be stored locally until connection is reestablished. If desired, IT admin can be notified, via system alert or email, when this problem occurs.

5. **How do I keep my SWS-H with the latest updates?**
   Just as with the NG appliance, the Policy Server automatically manages updates installation on all the target scanners (appliance and cloud)
6. **How do I upgrade to upcoming SWS-H versions?**

Administrators can easily schedule the time to upgrade to a newer version. This whole process normally takes less than an hour. There is no downtime when upgrading to a new version.

7. **What should a customer having a problem with a scanner-in-the-cloud do?**

Troubleshooting scanners in the cloud is even easier than troubleshooting appliances. The administrator can restart the scanner remotely or replace the scanner with an alternative one. This is done by launching an alternative scanner instance.

8. **Is there a customer support system in place?**

In case of problems and issues relating to the Amazon Platform and Payment service, customers are advised to contact Amazon support at: https://developer.amazonwebservices.com/connect/support.jsa.

Customers can purchase AWS Premium Support at: http://aws.amazon.com/premiumsupport/

M86's SLA for both the appliance and the cloud based solution in defined in the following document: http://www.M86.com/objects/brochures/M86_Product_Support_Policy.pdf

9. **How many SWS-H datacenters are available?**

SWS-H is exclusively running on EC2 data centers. The current two EC2 data centers are located in North America and in Europe (Ireland).

10. **Is there a new EULA for SWS-H?**

A new EULA is presented to a user when manually installing SWS-H Scanner.
Compliance and Security

1. How does SWS-H help protect data privacy and integrity?

All traffic sent from the SWS-H Client is encrypted, thus preventing any external parties from eavesdropping on traffic sent to the SWS-H.

All SWS-H logs are securely completed at the organization’s headquarters, and are based on the security and the privacy regulations defined by the organization.

Furthermore, neither M86 nor Amazon employees can access any customer environment. Only customers IT administrators can access the scanners in-the-cloud, and only administrators with explicit permissions can view users Internet traffic logs and reports.

Since all traffic sent to the SWS-H is both encrypted and authenticated, organizations can better control the protection of sensitive information as required by Sarbanes-Oxley (SOX) and other compliance regulations.

2. Is SWS-H a secure environment?

SWS-H is the most secure Web Security Service environment out there. Unlike other cloud-based solutions that only offer a multi-tenant environment to all customers, SWS-H offers a dedicated cloud environment per customer. This isolated cloud environment is protected by a strict firewall policy in-the-cloud, preventing users of one customer the ability to infringe on another customer’s environment. This isolated cloud environment should be seen as an extension of the customer’s own DMZ environment.

All remote workers are forced to authenticate using strong mutual certificate authentication. Moreover, all management traffic to and from the cloud is securely encrypted. No private or sensitive data is kept in the cloud, including user passwords and emails.

3. Is EC2 certified by SAS 70 Type II?

Amazon is working with a public accounting firm to ensure continued Sarbanes Oxley (SOX) compliance and to attain certifications such as recurring Statement on Auditing Standards No.70: Service Organizations, Type II (SAS70 Type II) certification.

For more information on SAS 70 Type II certification: [http://developer.amazonwebservices.com/connect/entry/default.jspa?categoryID=152&externall D=1697](http://developer.amazonwebservices.com/connect/entry/default.jspa?categoryID=152&externall D=1697)
4. Is SWS-H PCI-Compliant?

SWS-H doesn’t handle any credit or debit card data, and is therefore not subjected to PCI regulations. PCI is mainly required for e-commerce services. Nevertheless, SWS-H does meet PCI DSS requirements including; firewall (via EC2 Security Group), secure network (encryption), strong access control (certificate authentication), and using logs to track all network access and letting customers archive these logs in secure locations within their corporate network.


5. Can customers visit and audit EC2 datacenters?

No, since physical access to Amazon’s operations building and the data centers is restricted to authorized personnel only.

6. How is SWS-H built to reduce the impact of a DDOS attack?

SWS-H Scanners ignore requests with invalid certificates. The EC2 security group (the EC2 firewall) would block all requests to unauthorized ports.