Managed Security Services (MSS) based on Provisioned Security Services (PSS)

Eyal Adar und Dan Sarel

IP VALUE

Abstract The paper discusses the reality of Managed Security Services today and their drawbacks. It then moves on to propose a solution to the most burning problems. The solution, Provisioned Security Services, is based on the premise that providing a strong provisioning platform, which automates processes and integrates into providers' networks, will allow large providers to become key players in the area of managed security services. Architecture of an actual PSS solution is provided and briefly discussed.

1 Managed Security Services

Data security is a complex issue, becoming more complex as the number of attacks and their sophistication grow. Good security experts are hard to come by, and most small to medium enterprises cannot afford to keep a security team in-house.

As a result we see that more and more enterprises move to outsource the security functions (often as part of outsourcing the entire IT functions or major parts of it).

As with other specialized areas, a major benefit for companies that outsource security, if high-level professional companies are used, is receiving best practices security at a relatively low cost.

This trend has led to a growing new market. In Europe, in the US and elsewhere many Managed Security Services companies have sprung up, helping companies keep their data secure.

Among the managed security services providers are new dedicated companies as well as older companies from different areas: security product vendors, consultants, ISPs and Telephone companies.

These companies usually provide:

- Managed Firewall and VPN services – providing network perimeter security as well as secure connectivity for mobile users and among sites.
- Content filtering
- IDS management
- Managed anti-virus (typically using gateway products)
- Network Monitoring (using the above products and management tools) and incident response
- Some companies also provide periodic vulnerability testing, patching and escalation

Already starting to show up and expected to significantly grow in the future are the following services:

- Authentication services management
- PKI management
- Integrated security logging – drawing, synchronizing and analyzing logs from different enforcement products)
- Company-wide security policy management
- And many other services

2 Managed Security Services Limitations

Most products that the managed security services providers rely on were not designed to interface with other products. In large enterprises we see a lot of home-grown solutions that help integrate the security products. Managed security services are weary of providing such solutions since they require a different solution for each customer, making it highly uneconomical.

Some of the new managed security services companies, usually set up by bold innovative highly professional personnel, tackle the problem using innovative techniques such as planting their own agents within the software and hardware provided by vendors. Others rely more on the vendors' initiatives and partnerships that help integrate at least some of the security products.

This limitation becomes more severe for the larger providers, whose businesses rely on quickly integrating custom-made services and products, rather than spending time and effort tailoring different solutions for different customers.

There is another reason that large providers find it very difficult to provide MSS. Most designers of security products had the enterprise security personnel in mind. Answering providers' needs, or integrating the products in providers' systems were not originally seen as top priority.

As a result of this "bias", most products have no means of integration with back office services and components (CRM, HR, billing, etc.) and no automation of tasks. The products often suffer scalability limitations. The end result is that most work is done manually, services are not automated and integrated and it is still painful, expensive and requires lengthy processes to add new services.

These are all problems that are familiar to anybody who has been thinking about Operation Support Systems (OSS) in general. However, security products add their own limitations.

Security products are relatively young. Their relative complexity (having to deal with standards that are still in development and change all the time, dealing with complex technologies such as encryption, PKI, etc.), have led to major delays in adding the basic features that providers need (such as integration into back office systems) to the products.

Another major obstacle is the fact that there is no industry-wide adoption of standards for management and communication with security products. Most vendors are still trying to

win as much market share as they can, which often translates to lack of cooperation among vendors.

Some of the more serious attempts to standardize management and communication among products are still bound to specific vendors or vendor consortia, making life extremely difficult for providers that need to cope with a multi-vendor environment and with situations where the products used by their customers are not necessarily of their own choice.

In summary, MSS used to be provided by small companies (even if the main contractor was a big player). The Big players (typically, xSPs) are entering the market, and finding that the products were not designed to answer their particular needs. New solutions are needed for the service providers in order to bridge these gaps.

3 A Word about the Business Needs

The providers have, of course, a good reason to enter the market. It is a well-known fact that competition between the providers has dramatically reduced the prices of basic services, and in order to survive they must identify new sources of revenues

Security has been singled out as a major player since it is relatively immune to changing financial climates (companies do not see security as a luxury they can do without when times get rough). And as we said before, companies are willing to pay a premium in order to outsource security.

Roll-out of many new services is the key growth driver for all service providers (fixed-line, mobile, hosting, corporate), but so far rolling out security services, for the reasons we have quoted before, has been difficult to do.

4 PSS Closes the Gap

Theoretically, if all products could come of age quickly, and standards quickly put into place and adopted by all vendors, providing MSS would have been as easy as providing a new phone line or access to the Internet. However, this will not be the case for quite some time.

A new infrastructure for the security services is therefore needed in order to complement the existing products. It must address:

- Integration into the provider's workflow
- Automation of as much of the processes as possible
- Integration into the provider's services

We call the new infrastructure "PSS," or Provisioned Security Services.

The vision is quite simple. We imagine service providers being able to deliver to thousands of enterprises a pre-integrated service bundle consisting of access control services, virus protection, encryption services, authentication services, etc. all just by the click of a button with immediate availability to the customer and with total transparency.

PSS will enable service providers to generate new revenue streams and cut costs through automated delivery of a wide range of security services

5 The PSS Challenge

Even though the vision is simple, the challenge is not small. Turning an application into service requires integration with many sub-systems.

As more applications are added, the integration becomes more complicated. The following diagram depicts the complexity of the integration. One must remember that each of the black arrows is not a simple connection. It often requires some programming and at times much more.

For example, many of the security products do not have any interface that can allow proper billing (some products do not have the granularity and reporting abilities that allow the provider to find out each customer's use of the service). This not only complicates things, but also makes the task nearly impossible to achieve.

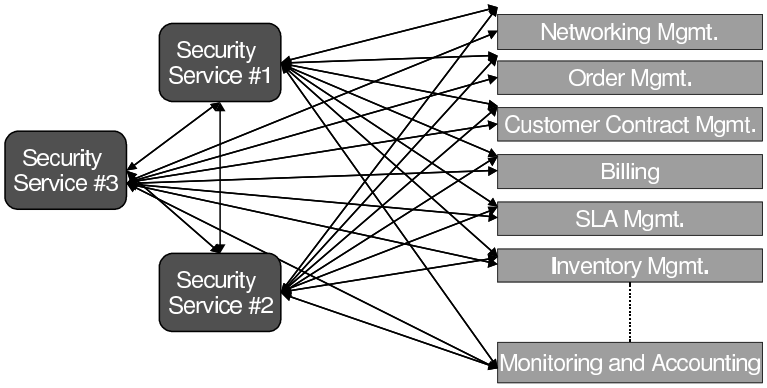

Figure 1: PSS Challenge

6 The PSS Solution

The solution comes in two steps:

1. Pre-integrate the new application with supporting sub-systems.
2. Automate the entire service workflow and provisioning process

And this is what it looks like:

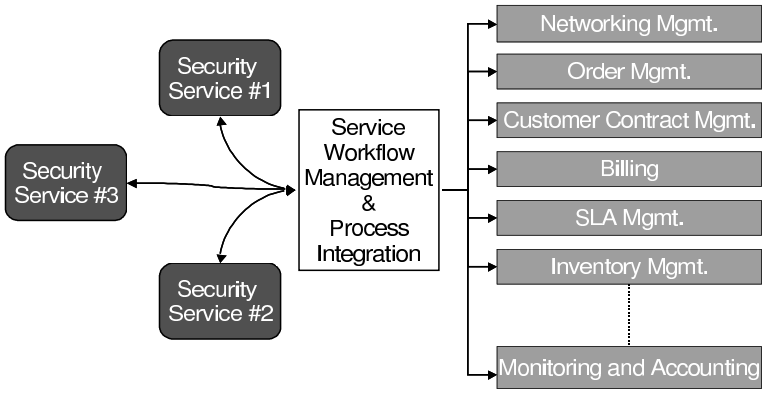

Figure 2: PSS Solution

The PSS solution adds a new layer of process integration. The layer must be smart enough to be able to communicate with the providers' systems as well as with the security enforcement products. It eliminates the need, which is the current major obstacle, of having both layers communicate directly.

In the reality of today's security service offering, this is what the high level of PSS will look like:

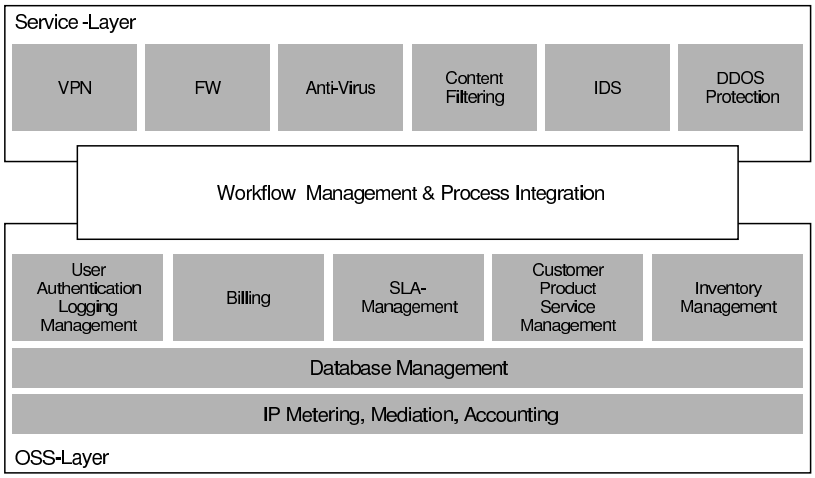

Figure 3: PSS Solution Overview

7 PSS - Implementation

The following diagram provides an overview of our own PSS platform, better known as premioss^{TM}. We offer it as an example of how PSS can be achieved.

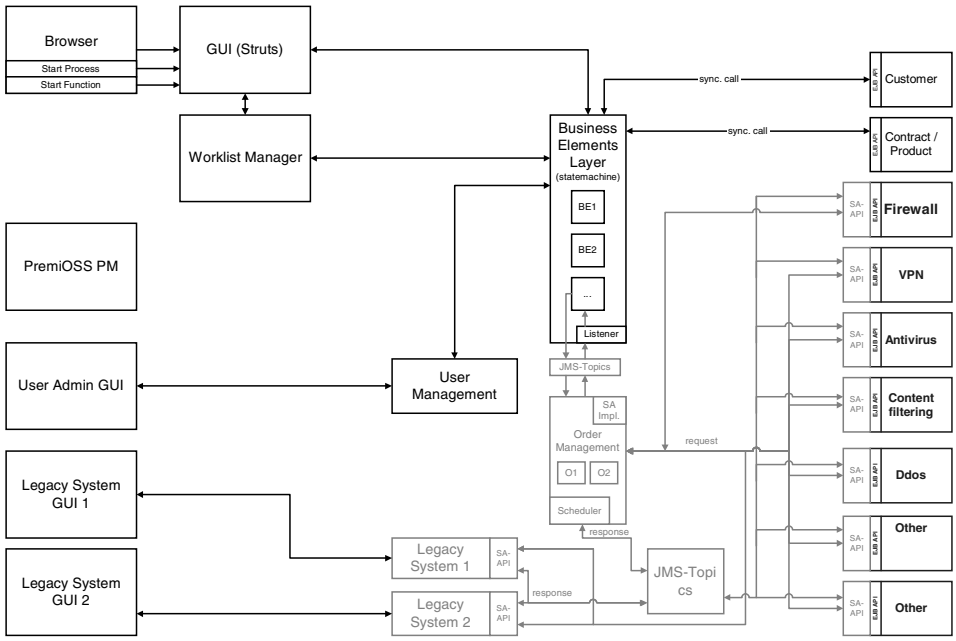

Figure 4: PSS Solution Overview

premioss^{TM} was designed to solve OSS problems in general. However, its design proved to be a perfect fit for security services. We will not go into much detail about the architecture here, however we will discuss a few of the major processes that allow this design to efficiently provision security services.

One of the most important issues is the choice of a robust framework for communicating with different components that communicate in different ways. We have chosen to join the OSS/J initiative in order to achieve such a framework.

The core of the premioss platform is purely java based, using state of the art commercial J2EE platforms. However, OSS systems have to communicate with many different systems, which are often not Java based or use proprietary interfaces. To handle so many different proprietary interfaces is a very complex task, which takes up many resources.

To reduce this complexity the OSS/J initiative was founded. It is a body of Telecommunication industry leading players and experts with the goal to define and implement an open, standard set of APIs for Operation Support Systems using Java technology. This initiative is run under the conditions of the Java Community Process, which governs the

evolution of Java Technology. In order to focus on business and application specific issues, the Java Platform Enterprise Edition was chosen as the technology platform for all implementations, enabling the robustness needed for large providers.

The hardest task, which is perhaps harder with security products than other products, is to have a transparent system so that the provider's operator does not have to know what products are enforcing the services, or for that matter what a particular service means in terms of the underlying technology. For example, if an operator is required to provide high access control security to a particular customer, she does not have to know that this is translated into a set of strict firewall roles.

In another example, if an operator is required to connect new mobile users to a company's network, he does not have to know that this will be done using a specific firewall on the customer's network, using a particular client on the mobile user's laptop. Of course, the operator does not have to know that IPSEC will be used, or that the encryption used will be 3DES with SHA1 authentication.

However, this knowledge cannot be completely ignored. The system must still make the decision to use this particular set up. The system is designed to be able to translate the operator's command to the proper technical instructions. Furthermore, in its interfaces to the actual enforcement points (the actual security products), it keeps the knowledge of how to translate this into the particular commands and particular communication methods that the enforcement points expect.

Perhaps most importantly, the system enables keeping the combined knowledge of all processes, be they security service related or processes that involve other IP based technologies and it allows this knowledge to be forwarded to other systems (such as billing, CRM, etc.).

Among the services that the premioss is designed to provision are access control, VPN connectivity, anti-virus protection, content filtering and a new service that MSS providers are expected to offer in the near future – protection against DDOS attacks.

8 PSS Advantages

PSS shortens processes by automating as much as can be automated. Automation has its limits of course, and sometimes there is no alternative but to send a technician to configure some basic functions. The PSS system can help here too by making sure that the proper systems produce the necessary work orders, the follow ups, etc.

PSS can also dramatically shorten the time it takes to offer new services. If built correctly, adding a new service is merely adding a new module to the system, and once the business parameters are decided upon (pricing, supported products, marketing, etc.), it can be a matter of days before a new service is up and running and offered to customers.

Furthermore, scalability problems can be reduced, both in terms of subscribers and services, not only by automating the processes, but also by the ability of duplicating many system components.

Management costs can be significantly reduced using a central management rather than many management systems, each addressing a service, or worse yet, each managing a particular product, which is usually the case with security products.

Service provisioning is turned into a single process, rather than many processes, providing much better control.

9 PSS – Summary

PSS is a single application that manages all services:

- Provisioning of new security services and users
- Provisioning of all surrounding workflow processes needed (billing, CRM, etc.).
- Provisioning is made within the workflow process
- Provisioning is done transparently and easily – most work is done through one console, the hard work is done automatically in the background

Finally, a good PSS system creates the foundation for efficient MSS.

10 Examples

The first example is very common in MSS and often requires specialist intervention as well as numerous procedures that result in a costly and inefficient process. Here the provider is asked to create a secure connection between two partners.

After some research the provider realizes that this will have to be done using the different parties' firewalls, which happen to use different vendors' products. For the sake of the example, let's say that once is a Cisco Pix and the other is a Netscreen appliance.

Today, the following will happen (this is a shortened list in reality there are many more steps):

1. Bob has to access the Netscreen management console to manage company "A"'s firewall
2. Bob configures the firewall to create a tunnel with company "B"'s Cisco PIX (about 10 commands, using either a WebUI or CLI via SSH)
3. Bob configures the firewall to allow host "A" from company "B" to access the tunnel (quite a few more commands, which include specifying the protected networks, the particular tunnel settings – encryption method, authentication method, etc.)
4. Alice goes to the cisco Pix management software, repeats the above steps (very different commands, using different method of communications) for Site "B." What makes this process even longer is the fact that it involves interoperability between two different products, which requires expert knowledge that Bob and Alice may not have.
5. Wilma will use another station and update the CRM system for each customer after receiving the information from Bob and Alice.
6. Another person will access the billing system and update the billing database regarding the new service.

7. Etc. etc. etc.

Many providers take days in order to sort out the technical parts and a few more hours to get all the other systems updated.

With PSS the picture should be different. Our vision suggests the following:

1. Jane goes to the PSS console
2. Using simple GUI she ”connects” the two sites
3. All done

In another example that shows the strength of the PSS system in translating business needs to action we discuss how access control services may be provided. A provider may decide to give customers the choice of having low, medium and high level security.

The provider has made several decisions on what each security level means. For example, low level means allowing all traffic in and out of the customer's network but protecting against known attacks; medium security may mean allowing all outbound communications and not allowing anything, other than SMTP, in; while high level means allowing only specific protocols out (e.g. HTTP, DNS, SMTP) and specific protocols in, but only to the DMZ or to specific servers.

The system will have one input – the operator will click the level of security for a new customer. However, this will automatically start quite a few processes. One process will actually configure the customer's firewall (after looking up its IP address, its initial login and password, the product involved, its current version and where applicable its current configuration). This process will end when the correct adaptor is selected, sends the correct commands and receives the desired results.

Depending on the provider's workflow the next stage may be a message to the billing system to start billing the customer according to a contract found in another database and the security level that was chosen. In some cases a message will be sent to an operator who will call the customer to inform of the service activation. Depending on the provider there may be many more steps, all can be automated by the PSS system.

The devil is of course in the details. The system must have the means (i.e. the databases) to determine the customer's assets as well as the necessary information regarding the networks involved. It must also be able to communicate correctly with the products (use the correct protocol, and the correct commands not only for a particular product, but also for the specific product version), and provide alerts when the process does not go according to plans.

These are only a few of the necessary conditions to make PSS happen. It is not an easy task, but once a PSS system is configured correctly, processes can be easily replicated among customers and providers can reap the benefits quickly.