Global Information Assurance Certification Paper

Integrated Security in a corporate environment

By:

Bernd Bilek

GSEC Version 1.4b

22. April 2003

1 Introduction

In this short paper I'd like to point out the benefits of implementing an integrated security strategy. Furthermore I'd like to demonstrate how important it is to use software and hardware products which do support this approach and want to show where the advantages are to have a common and centralized management, which is a part of the aim to implement integrated security in the company.

In this short paper I cannot cover all aspects of integrated security. Therefore I will focus on some aspects, like integrated security on the client, the gateway and the centralized management as a part of the integrated security approach.

2 The problem

Are my information secure? This question is much older than computer based course of business. But when talking about the protection of digital data the whole thing is getting more complex.

In former times we also had tools to protect our assets. We had thick fat locks and a watchman, alarm bells when an intruder enters a secure zone, Today: the locks and the watchman are replaced by a firewall and the alarm bells by an intrusion detection system. Only experts are aware how these technologies work it detail and have the knowledge to understand what a message in a firewall log means.

This causes many companies not to make additional investments into IT security, because the products are to complex and they do not integrated

3 What is integrated security

The differentiator between integrated security and distributed security is as follows:

- aggregation of security relevant information
- correlation of security relevant information
- central data store of security relevant information
- information exchange between the components which are relevant to the company security, e.g. different products/applications
- one central console in terms of management, alerting, etc

In other words: “We defined it as a set of applications that work in concert to provide a total security solution”[1]

In the course of the paper I will give some examples of the above mentioned. This will demonstrated the information flow and the “work together” of enterprise products.

Furthermore integrated security strengths the total enterprise security, because you gather additional information and you get a total overall overview of your enterprise security at any given time.

4 Importance of integrated security

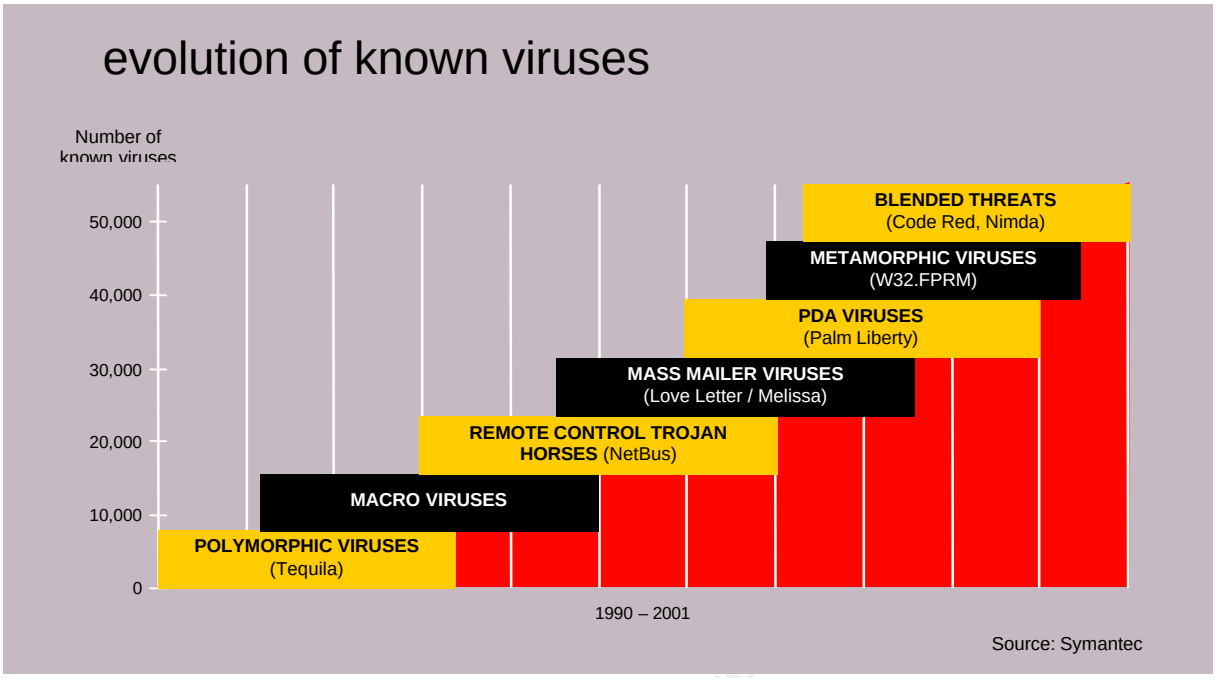
The threat potential, into which companies and enterprise do face, is constantly changing. In former times it was fairly easy to categorize threats. We were able to say, that a certain aggression was caused by a virus a worm a trojan horse or by a selective attack caused by a cracker/hacker. For those kinds of attacks there are the appropriated products available.

AV scanner, host based/network based IDS systems, firewalls and so on are making still a good job as standalone applications, but they’re making a centralized management of all components more and more complex. The network speed is increasing more and more, more data are occurring in the log files of the security products, which lead to the following:

- it is getting harder to obtain high quality data in terms of security
- you need to hire additional IT staff to get all the relevant data of all the implemented security products
- additional costs

But there is a second very important reason which is in favour for integrated security:

The security arena has seen a remarkable evolution in security threats. More than ten years ago, we saw the emergence of polymorphic viruses.
From this chart (**Graphic 1**) we can see that in recent years the number of security threats has increased exponentially and the threats we see today are now more sophisticated than ever before.
Previously, threats were handled on a “one threat, one cure” basis. Today, we are faced with a different and even more complex scenario. We have a new type of threat which can be a combination of virus, hacker attacks and denial of service threats. This is called a ‘blended threat’. The very first examples of blended threats occurred last year with CodeRed and Nimda.



Graphic 1

Against "something" which is a virus and a worm and a selective attack in one thing, there is no point product, which can help you in protecting your companies' assets.

What do we need now? You will need a concentrated security strategy[2], where the whole organisation of a company should be considered. The second thing, where I'd like to put my focus on is the technology part. An up-to-date security management must consist of integrated and dynamic solutions, which are able to protect the enterprise against today known threats and against treats which will come up in the future.

Instead of using and deploying point products we need to choose the integrated security approach on each level of the network/company. In the following chapters I'd like to cover integrated security on the client/desktop on the gateway and in terms of centralized management, meaning to integrated different products from different vendors into one central management console.

5 Integrated security – the client

When talking about integrated security there are different points of view, but there are still some basic points common.

- integration of products/applications
- centralized management
- correlation of events

The author has chosen the product **Symantec Client Security** (SCS), to demonstrated integrated security on the client. At this point it is the only product, which has fully integrated applications, one installation routine and one central management console.

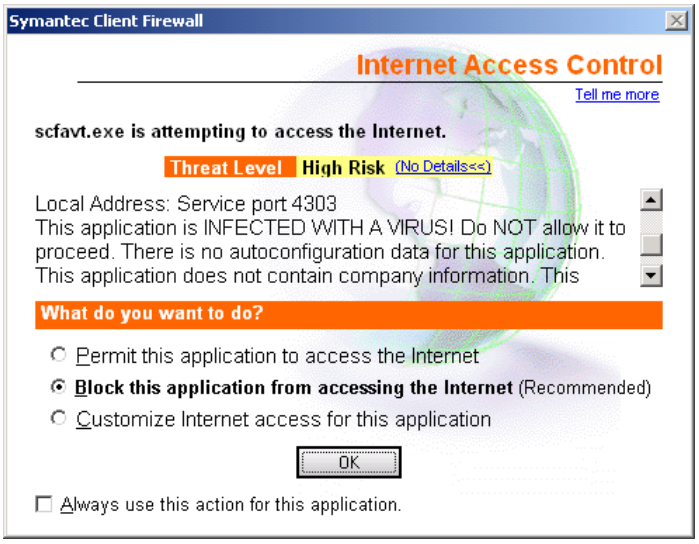
What is Symantec Client Security? It is software, which is installed on the client inside the company, meaning on the desktops and on the laptops of roaming users. This software incorporates three functions:

- Antivirus
- Client firewall
- Intrusion detection

Until now, customers have deployed multiple security technologies from multiple security vendors. This leads to possible compatibility issues and potential holes in security that will allow a complex threat to spread[3]. What are needed are integrated technologies that are aware of each other and can take appropriate action when a complex threat is encountered.

CLIENT SECURITY POLICY ENFORCEMENT Typical client firewall products scan Incoming and outgoing traffic against firewall and applications rules. If a file coming through the firewall is infected with a virus the typical firewall is going to let it come through. Firewall technology within Symantec Client Security works seamlessly with antivirus technology to protect the client from viruses, even if the administrator or user has configured real-time virus protection technology in the "off position." When the firewall encounters a file it will call the antivirus scan engine to check for viruses (**Graphic 2**). If a virus is found the antivirus technology will instruct the firewall to raise the threat level to "high" with a default action to "block" the file from entering or leaving the system.

Through integration of client firewall and intrusion detection technologies, scanning and comparing all incoming and outgoing traffic with known sets of signatures enables the intrusion detection technology to instruct the firewall to block an unauthorized intruder's offending IP address for up to 30 minutes.



Graphic 2

For Example:

Firewall technology will initiate an antivirus scan even when AV has been turned off! Intrusion Detection technology will instruct Firewall to block traffic from malicious sources

Symantec Client Security Architecture

The Symantec Client Security framework is composed of five key components designed to provide benefits to customers. Each of these components helps to reduce the IT resources needed to manage various client security technologies and ultimately reduce the total cost of ownership.

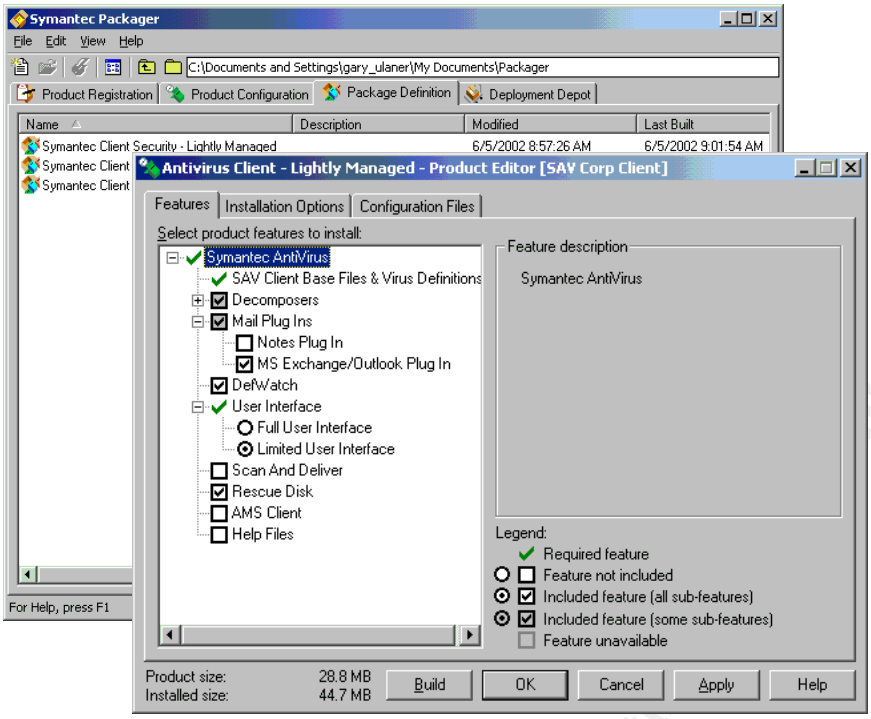
The key elements of Symantec Client Security include:

5.1 Integrated Protection

Symantec Client Security provides integrated antivirus, firewall and intrusion detection protection that provides a heightened level of protection for all workstations.

5.2 Integrated Deployment

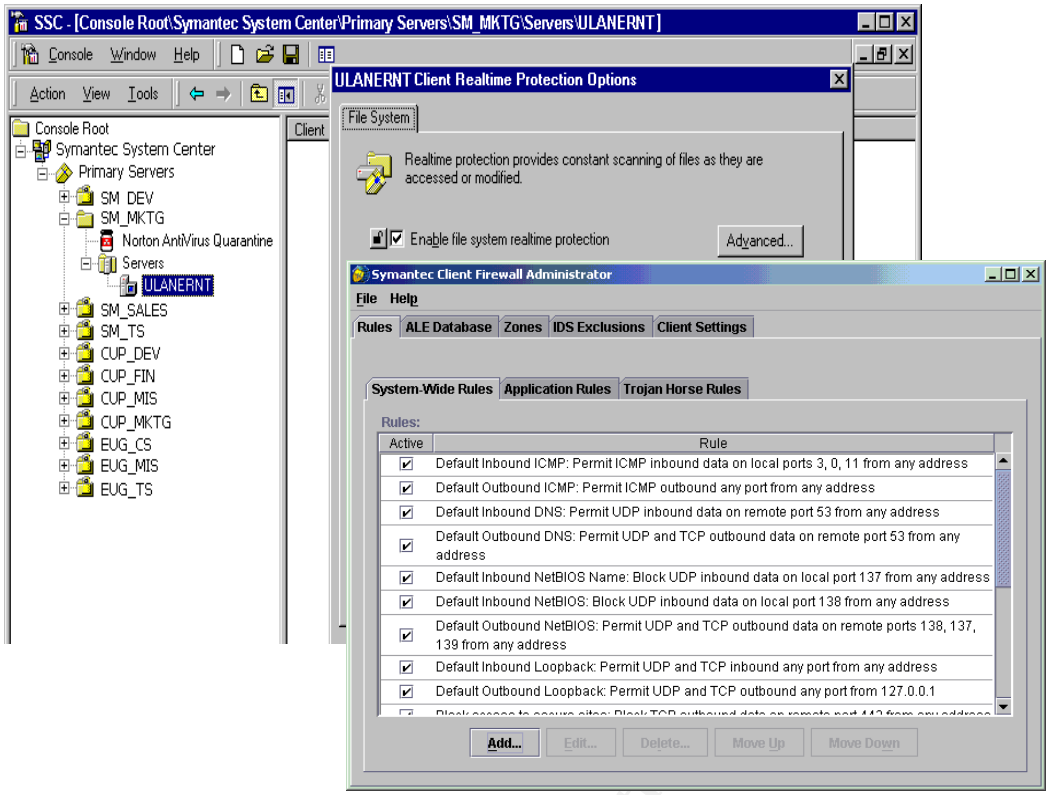
Symantec integrated deployment allows for three pre-configured installations; fully managed, lightly managed, and thin client. These flexible installation options allow organizations to customize the security posture for individuals, work groups, or the entire organizations while reducing the time and cost required to deploy tailored security at the client (**Graphic 3**).



Graphic 3

5.3 Common Management Console

Symantec Client Security includes Symantec's proven management infrastructure, Symantec System Center, to deliver a managed security client. Administrators will be able to completely configure, install, manage, and update all the security components for the workstation, (antivirus, firewall and intrusion detection), and virus protection for the network server from one management console. This console has a hierarchical infrastructure, including policy management with settings lockdown and the ability of group management. This helps to reduce the IT staff resources required to monitor and manage multiple client technologies (**Graphic 4**).



Graphic 4

5.4 Integrated Response

Symantec integrated response provides a single updating mechanism for antivirus, firewall and intrusion detection from a common management console, allowing organizations to respond faster to security outbreaks, minimize the impact on network bandwidth, and reduce update costs.

5.5 Integrated Support

Symantec Client Security is backed by an integrated support department that provides round-the-clock (24x7x365) response via telephone, Internet[4], and wireless alerting. Symantec support proactively researches new threats and provides fast updates to protect against new attacks, while also providing a single client security support base to ensure rapid resolution.

This is one possibility to roll out integrated security. But as mentioned at the very beginning of that paper, there are more starting points. The next one I'd like to mention is the approach to install a gateway device, which has integrated security capabilities.

6 Integrated security – gateway

At the gateway we are facing the same challenges like on the client: cost efficiency, central management, etc. But this is not the only challenge – we are talking about increasing the security and not just about lowering the costs.

Blended Threat Example: Nimda

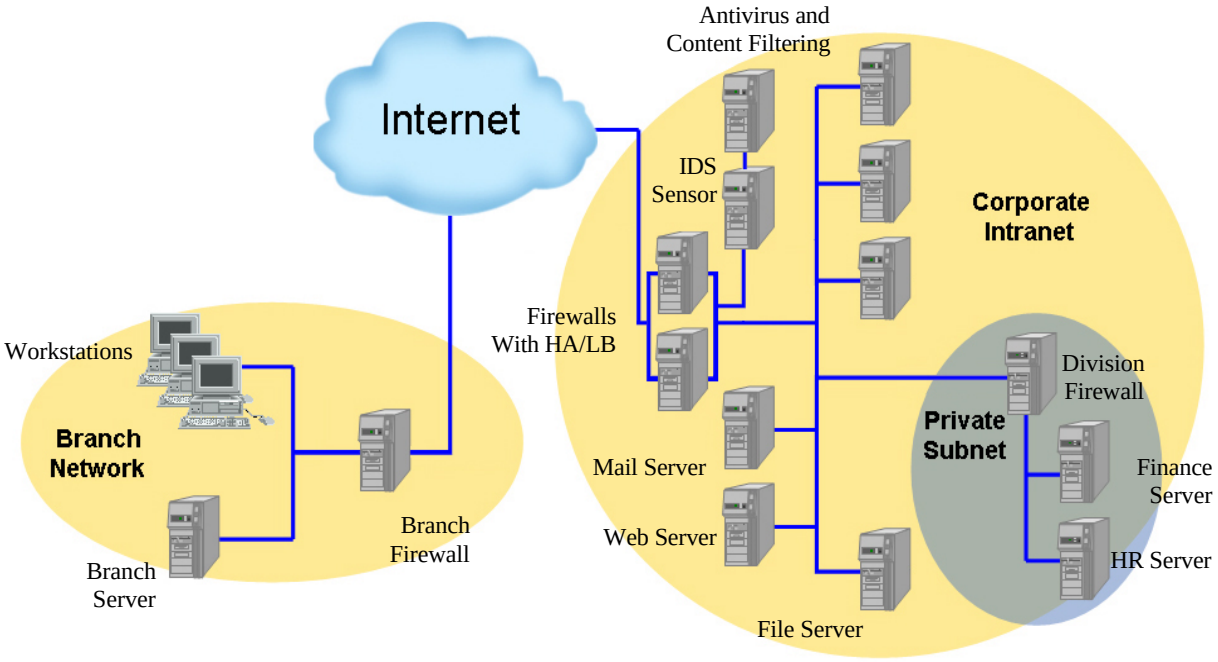
In many ways, Nimda was the virus "heard round the world" because it fulfilled the nefarious promise of worms and viruses to attack resources through multiple paths. This ability creates an environment where any vulnerability can be exploited dynamically. Nimda focused on four different vulnerabilities[5]:

- The IIS Web Server Unicode Web Traversal exploit
- A download .eml file from an infected web site
- E-Mail propagation
- Shared folders in file systems

In all, it demonstrated properties of a virus and an intruder attack, attempting to exploit vulnerabilities normally protected by antivirus software, intrusion detection systems and firewalls. It is clear, that all of these threats and their corresponding security solutions must be deployed in concert to ensure that security is maintained throughout the enterprise.

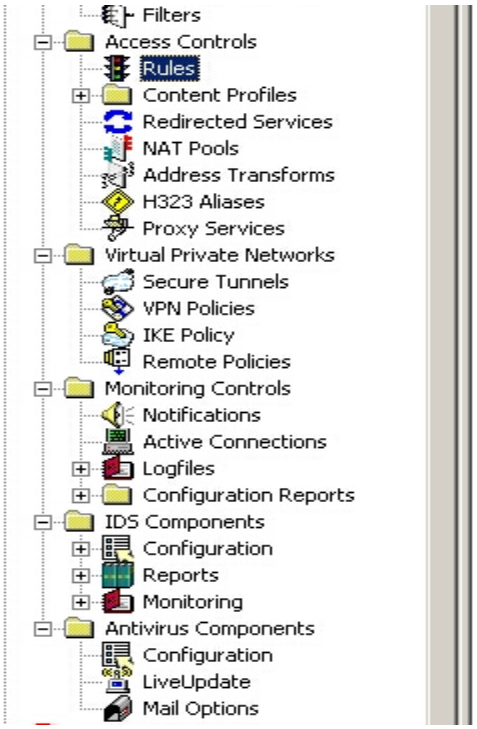
But how can this be done on the gateway? Multiple standalone systems/appliances, which have one central console and shifting the traffic back and forth? No, this not the proper way to deploy integrated security at the gateway.

Today we see very often distributed (**Graphic 5**) security products in the enterprise. Dedicated IDS sensors, firewalls at the perimeter and AV and content filtering (CF) in the demilitarized zone (DMZ).



Graphic 5

Now going back again to the integrated security approach. Best would be to have a box or device which incorporates multiple functions in one device and gives us scalability on top. All this functionality should be manageable through one central GUI (**Graphic 6**).



Graphic 6

Symantec Gateway Security is one of those devices. This appliance is the first integrated gateway security appliance that combines:

- Firewall
- Virtual Private Networks
- Intrusion Detection
- Anti Virus
- Content Filtering

What is Symantec Gateway Security, besides combining 5 functions in one appliance? Starting with the firewall engine it is the award winning Symantec Enterprise Firewall which is adapted to this hardware. The key factors of this firewall are as follows:

6.1 Firewall[6]

- Application Proxy Firewall
- Best fit rule generation
- Automatic and persistent system hardening
- IKE/IPSEC VPN
- ICSA certified/Checkmark certified

An application proxy firewall is the proper technology, when fighting against blended threads. Due to it's proxy based approach it splits one physical connection (client -> internet) into two connections (client -> firewall -> internet) and has the ability to determine every type of traffic which is not RFC conform. Besides that the firewall engine has the capability to see and to filter buffer overflows. This helps us, in building a gateway device protecting us against threats like Nimda and Code Red.

6.2 Virtual Private Networks

Most companies are using VPN technology to avoid the high costs of leased lines. When choosing a VPN gateway it is installed in most cases in parallel to the firewall (additional hardware/different vendor/different GUI) or it resides in the DMZ behind the firewall (firewall reconfiguration necessary/opening additional ports/compatibility issues with standard VPN).

Why not using the VPN functionality directly on the gateway? The benefit of doing so is not just utilizing the same GUI for the firewall configuration and the VPN configuration it

is furthermore the advantage to use the same entities and objects defined for the firewall communication with the VPN tunnels. And on top of that we use the proxy approach even in the VPN module.

All in all we see that we can save a lot of time and resources, which leads to an optimized security and cost management.

6.3 Intrusion Detection

The Intrusion Detection (IDS) Module is a bit different from the IDS systems which are common. In the wild most IDSs are “pass by” or “host based”. This means, in the case of the pass by based technology that the network interface card is put into promiscuous or stealth mode and is able to see all the traffic which is following in a segment. The host based IDS is working in that way, that each system which should be monitored has a agent installed and also a set of policies. When someone violates the policy which is applied to the agent it is counted as an intrusion.

On the Symantec Gateway Security we are talking about a pass trough IDS[7]. This means, that the Symantec Gateway Security sees all the traffic flowing through itself. This traffic is seen in real time and in the case the appliance is finding any traffic; tat matches an IDS signature it can be configured to start predefined actions, like alerting the admin, etc. Here again Symantec is using signatures which are going to be updated automatically. This is done via live update, a mechanism which ensure, that the system always has the up-to-date signatures applied.

6.4 Antivirus

Symantec is using in this appliance the Symantec Scan engine. This can scan incoming and outgoing SMTP/HTTP/FTP traffic on per rule basis. This technology is used at big search engines to scan their mail traffic (Yahoo!). What are the key factors of this piece of the integrated security appliance?

It has the same update mechanism like the IDS system on the appliance. With this mechanism the AV pattern files are update. It is highly customizable how and when the update process should take place. It can be configured to fetch the updated pattern files automatically. With the same live update procedure also the scan engine can be updated – this happens without any downtime because of Symantec’s AV architecture (NAVEX!). The benefit is that there is no downtime because of any updates on the system.

As an add on the AV portion is doing additional SPAM filtering. This extends the SPAM filtering capabilities of the SMTP daemon/proxy (part of the firewall) which is running on the appliance

6.5 Content Filtering

Last but not least this appliance can be configured as a content filter. This is working as a subscription service and valid for one year. And again: all updates on the lists occur seamless and automatic. Once a day all updates are downloaded and applied to the Symantec Gateway Security. This content filter can be applied on a per rule and per user basis. The nice thing, when talking about integrated security and costs is, that there are no modifications of the client browser necessary – in other words this content filter is transparent to the user.

At this point I'd like to summarize the benefits:

We have here an appliance (better for remote management/in the case of a hardware failure quick replacement), which can fully automated update its IDS and AV portion. The product has an application proxy firewall, which is protocol aware and is able to determine which connections are RFC conform or do violate these standards. All these function are managed through one central GUI.

The last point I'd like to cover here is scalability. As we all now hardware has limited resources (processor speed, main memory, etc.). This appliance has the same limitations, but the solution is scalable due to the fact, that we can cluster two or more units and can replicate the configuration from one box to the other(s).

Again we see: Increase of security, because there is no downtime and no possibilities to make configuration errors, less costs because of easy administration and last but not least: One single contact in terms of supporting this device -

As mentioned in the section above all hardware have their limitations – this is probably one of the reasons not to choose an integrated appliance at the gateway. Imagine there are companies which have 155-622 Mbit uplink to the internet, having a data transfer volume of multiple terabytes. There are no integrated appliances which can handle this amount of traffic – most firewall appliances are not able to do this.....

7 Security Management in the Enterprise

... but does this mean, that they are not able to build an integrated security solution? The bigger the site, the less secure? No definitely not, but there a different challenges to manage the implementation of an integrated security solution.

Remember the picture of section 6. “Integrated security – gateway” showing the distributed approach of security components. This is in nearly all bigger sites the case. The components are distributed over multiple site (headquarter/branch office) and are also distributed within one site. In chapter 6 we had the ideal situation that all components are originating from one vendor. This will probably never happen, even if a vendor has all the best of bread products in each category – the reason here for is, that companies want to have different products from different vendors ... in the case the AV product from vendor A fails at the gateway, there is a big probability the client AV software of vendor B will identify the threat. In the wild we also see multi tiered firewall concepts – Firewall (A) from vendor (X) on an operating system (M); the second firewall (B), which comes directly behind firewall (A) is purchased from vendor (Y) and installed on the operating system from (N).

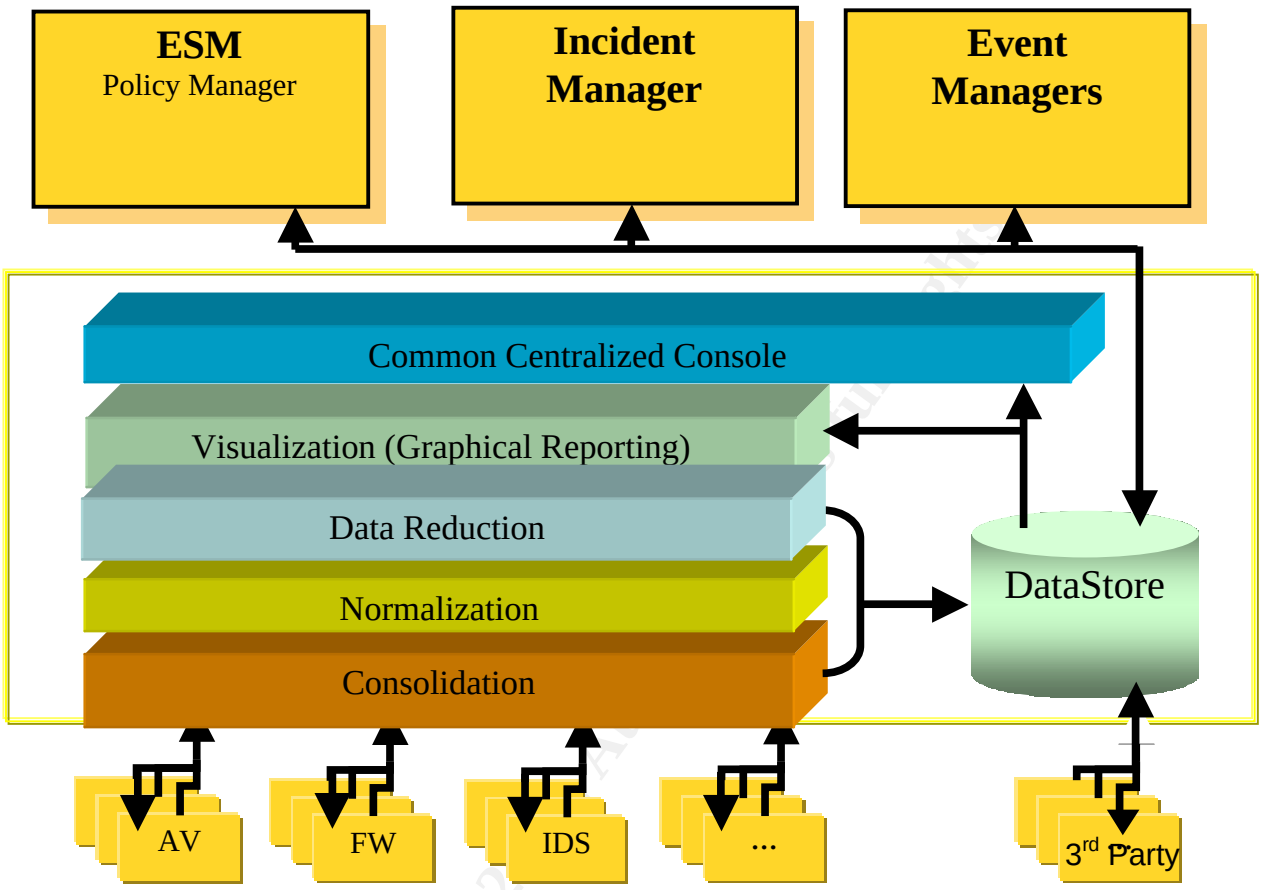
We see that there are more reasons to go for a distributed solution, but how can we now implement integrated security?

There are different vendors which have some products out covering that area. But to my knowledge there is only one product/architecture on the market which is doing this kind of integration in regards of security and not the basic management of software inside an enterprise.

Symantec Security Management System is the architecture which is enabling enterprise wide integrated security. But where is the benefit in detail?

- Improves an enterprise’s overall security posture
- Simplifies complex security infrastructures
- Increases response effectiveness
- Helps ensure business continuity
- Delivers a higher return on security investment
- Reduces total cost of ownership

Visualizing the solution

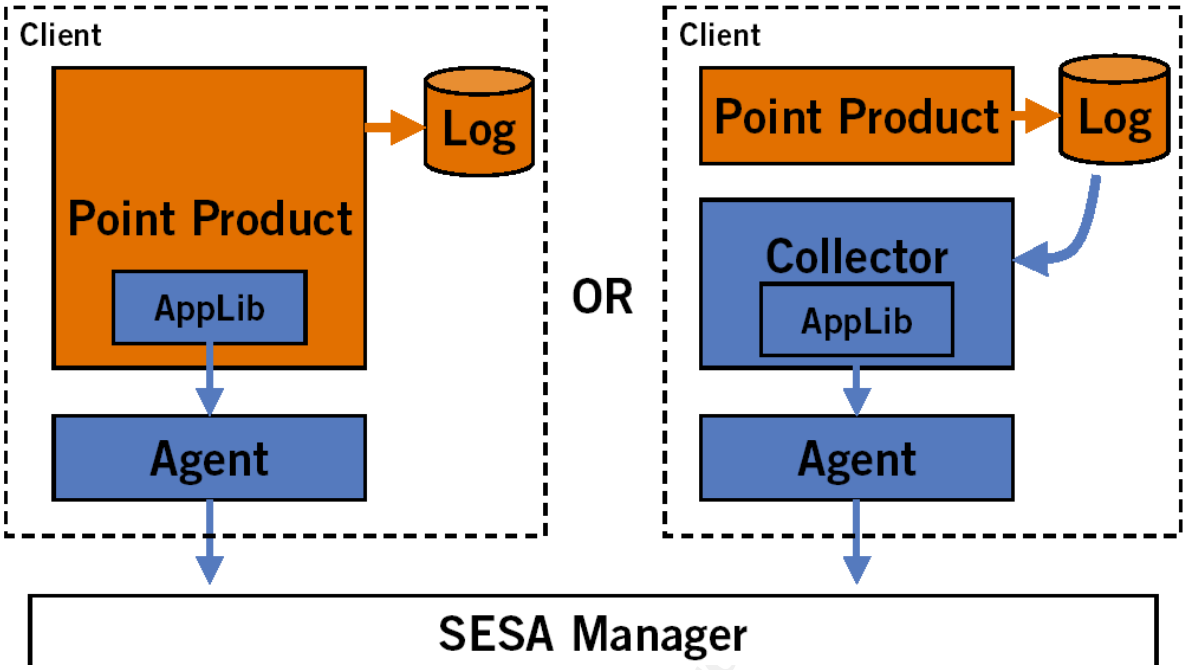


Graphic 7

I'd like to use the above picture (**Graphic 7**), to explain how this solution is working. I want to start at the bottom of the picture. There we see the point products like Antivirus (AV), Firewall (FW), Intrusion Detection (IDS), etc. And 3rd party. This is one very important point to mention here. This solution is working with Symantec products AND with 3rd party products from different vendors in the security field. The range of supported products and vendors is growing from month to month. Later one I will give an overview of the actual support software and hardware.

But how does this point product integration work? Is there a server application which is trying to identify all clients in a network and then integrating them into its database? It is not that easy, but not as complicated as some may assume.

Depending on the product and the product version there different ways to make a client talking to the central management system.



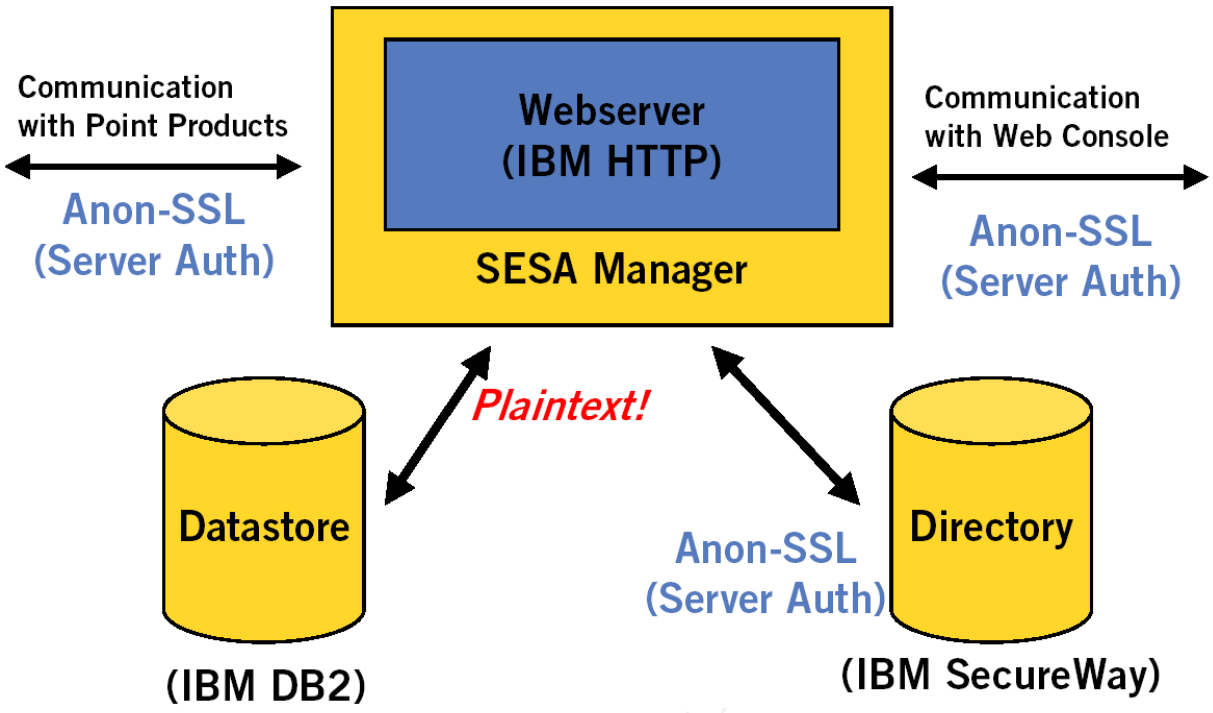
Graphic 8

As we see in **Graphic 8** there a different pieces which are needed to make point product being a part of this construct. On the left side we see a “native” product. This means, that there are two pieces which necessarily need to be installed on the client maschine:

- The product itself
- The agent which handles the communication with the SESA manager

The SESA manager is the **S**ymantec **E**nterprise **S**ecurity **A**rchitecture Manager. But what happens then, after the manager received the data? How is he communicating with the rest of the architecture?

At this point I’d like to introduce the missing components of the architecture. As you see in the picture below (**Grapic 9**) the manager itself is communicating with multiple systems, which may be installed on one machine or can be installed also distributed. When talking about multiple systems I’m talking about the data store, which actually is a DB2 database and the directory (IBM secureway). On the left side we see the communication to the point products which occurs on Port 443 (SSL) and on the right side we see the communication with the console – also on port 443 communication. The communication with the data store happens on port 50000 and the information exchange with the directory goes on port 636.



Graphic 9

So where is the real benefit for a company when implementing this type of integrated security?

Going back to one of our initial examples: NIMDA or Code Red. How would this type of attack be seen in distributed security architecture, not choosing the integrated way?

- Our Firewall might see some traffic which is unusual (buffer overflow attacks against a web server e.g.)
- The IDS system probably will see any unusual port activity against some machines
- Host based IDS will probably detect some violations against the setup policies
- The AV scanner will find a virus/worm/etc.

In most bigger companies there different administrators for different zones. A typical assignment is the network group, the server group and the client group. This leads to the following information flow:

- network group get an alarm because of the firewall activity
- server group will also get an alert because of the host based IDS
- the client group will be also alert because of the AV outbreak
- etc.

Multiple groups will work on the same issue without knowing, that this is one “blended threat” which is causing all the systems to send alerts. No central management console, where all the single applications will log into and provide additional benefit with the following:

- Consolidation
- Normalization
    - Same event types
    - Different format, different words on different products
    - Different languages
    - Tokenizes data
    - On console, can be view in local language, regardless of source locale
    - Data, time format conversion
- Data Reduction
- Some filtering can take place at point of collection
- Visualization
    - Reports and Alerts

8 Conclusion

Integrated security is not a matter of size of the company. This approach can be embedded at any size of a company, depending on which products and which security strategy is chosen. There are some products out, which this integrated security embedded. For instance the Symantec Client Security is as a product an integrated security solution. But when going into larger accounts and bigger sites, which may probably also use client security they can integrated this product/solution in the Symantec Security Management System, by installing the missing piece of software.

Integrated security can grow with the company size – integrated security is not just a product, it is furthermore a philosophy which is realized with the proper products.

References

[1] http://www.networkcomputing.com/1124/1124f2.html
[2] http://www.usm.edu/InfraGard/pdf/Best_Practices.pdf
[3] http://enterprisesecurity.symantec.com/article.cfm?articleid=1428&EID=0#why
[4] http://securityresponse.symantec.com/
[5] http://www.softwarespectrum.com/intouch/edition25/Symantec.asp?subsection=Symantec
[6] http://www.computerlinks.de/open/pdf/symantec/SEF%207_0%20Datasheet.pdf
[7] http://www.blackhat.com/presentations/bh-usa-02/5