



July 2004

A white paper
commissioned by
Astaro Corporation
Document #204128

Measuring the Value of Integrated Perimeter Security

A hands-on study measuring the time to deploy and manage an integrated security solution compared with two "best-of-breed" alternatives - Astaro Security Linux versus Check Point and Juniper Networks/NetScreen

Statement of Licensing Info and Acceptable Usage

Entire contents © 2004 The Tolly Group, Inc. All rights reserved.



For additional information on acceptable usage of this document (Tolly Group Document #204101) contact The Tolly Group at (561) 391-5610 or via E-mail: sales@tolly.com.

Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein is believed to be accurate and reliable. The Tolly Group shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

All excerpts from this report must be approved by The Tolly Group in advance of publication or use in any public materials.

Tolly Group Services



With more than 15 years experience validating leading-edge Information Technology products and services; The Tolly Group has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy.



Launched in 2003, The Tolly Group's "Tolly Verified" service provides in-depth, vendor-neutral certification of an array of features, functions and performance characteristics in technology disciplines as diverse as WLAN Switching and Anti-spam. See our "Tolly Verified" Home Page.



Our "Up-to-Spec" service provides the custom testing complement to the "standard", granular tests offered in "Tolly Verified". See our "Up-to-Spec" Home Page.



The "First & Foremost" designation is awarded to products that are the "First" to demonstrate specific performance or functionality in The Tolly Group's labs. Products also may earn a "Foremost" designation by demonstrating record performance or improved functionality that exceeds other products previously tested and certified by The Tolly Group. Such products are deemed the "Foremost" in their category by performance or by functionality. See our "First & Foremost" Home Page.

Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

This document was authored by:

- Kevin Tolly,
President/CEO
The Tolly Group
- Charles Bruno,
Executive Editor
The Tolly Group

Table of Contents

- 4 Overview
- 5 The Test Scenario
- 7 First-Year Security Effort
 - 7 Implementation
 - 8 Host/Server Definition
 - 9 Integration Challenges
- 11 Recurring Administrative Support
- 13 The Value of Integration
- 16 Appendix A: Upfront Implementation Tasks, Solution Worksheets
- 18 Appendix B: Ongoing Support Tasks, Solution Worksheets

List of Figures

- 6 Figure 1. Product Lineup by Application Type
- 8 Figure 2. Time to Deploy – Upfront Hours Required to Install
- 12 Figure 3. Time to Maintain – Monthly Hours

How Much is Integration Worth?

Overview

There is a perennial debate in the information technology community about the relative merits of "integrated solutions" versus a "best-of-breed" approach.

Is it better to acquire several related technologies from one vendor, already integrated, or to select a series of well-known products from different vendors?

Occasionally the marketplace will deliver a verdict on this question, as with the triumph of Microsoft Office and other office suites over separate personal productivity packages.

However, rarely if ever has an independent testing organization attempted to measure the actual value of integration as it pertains to a series of complementary technologies.

In this study, Astaro Corporation commissioned The Tolly Group to conduct a number of "hands-on" exercises designed to examine the technological and the cost differences between deploying an all-in-one network security solution versus a string of security point products.

Engineers compared Astaro Security Linux versus two solution sets, one anchored by Juniper Networks (formerly NetScreen Technologies Inc.) firewall/VPN products, and the other anchored by Check Point Software Technologies, Inc. firewall offerings. Both solutions utilized anti-virus and anti-spam software from Trend Micro Devices, Inc. and URL/content filtering software from Websense, Inc.

These test exercises were intended to compare the effort and complexity required to deploy and to manage a comprehensive perimeter security solution for a typical medium-sized business for a period of 12 months.

The objective was to provide for the solution to common business security requirements such as firewall/packet filtering, VPN connectivity, Internet content filtering including, anti-spam, anti-virus, and URL filtering.

The results were quite dramatic. The "best-of-breed" combinations took more than 3X times as long to deploy and to configure. On an ongoing basis, the "best-of-breed" solutions required roughly a 2X to 2.5X more effort to manage than the integrated solution.

According to IDC Research, the firewall market constituted a \$3.8 billion market in 2003 and is expected to reach \$5.5 billion in 2005. The market for secure content software solutions will grow from \$2.9 billion to \$4.1 billion in that period. Analysts are predicting the highest rate of growth for integrated security solutions.

Key Findings:

- "Best-of-breed" combinations took 2.9X to 4X more time to configure and deploy than the integrated solution.
- "Best-of-breed" combinations consumed 1.8X to 2.4X more time to manage on an ongoing basis compared to the integrated solution.
- There is a clear value to pre-integrated solutions including benefits of a single user interface, one integrated update mechanism and one set of management tools.

The Test Scenario

The Tolly Group's engineering team constructed a microcosm of a security solution designed to support an organization with 1,200 employees comprised of a main office with 750 employees and three satellite offices with between 100 and 250 users each. (While Tolly Group engineers did not build out such a network, they did evaluate the security solutions in the context of supporting such a network.)

The scenario of a medium-sized business was chosen because organizations of that size need a full range of security applications – firewall, virtual private network, anti-virus, spam blocking, and URL filtering – yet do not have the luxury of specialized IT security personnel. Therefore the need is especially acute to maximize the productivity of the systems administrator or IT manager. The results of the test should accurately scale up and down to larger and smaller organizations, however.

Tolly Group's engineering team performed tests reflecting a range of activities and attempting to answer the following questions:

- **Installing and configuring security software packages.** What are differences in deployment effort required to deploy an integrated network security solution versus individual security point products?
- **Setting up the administrative processes.** What are the differences in a comprehensive integrated security suite versus security point products to handle such functions as back-up and change control? What differences are observed in performing routine administrative activities over the duration of the simulated test period?
- **Software updates/distribution.** What are the variances in the processes for updating software with patches, new virus signatures, etc.?
- **Managing change.** How much effort is required to perform administrative activities like adds/moves/changes, policy updates, and the like?

The tests were conducted with three sets of perimeter security products:

- Astaro Security Linux, a pre-integrated package that delivers firewall, VPN, spam blocking, virus protection and URL filtering.
- A selection of products based upon Juniper Networks/NetScreen firewall/VPN gear, anti-virus and anti-spam software from Trend Micro, and URL filtering software from Websense, Inc.
- A selection of products based upon Check Point Software Technologies, Inc. firewall and VPN software, anti-virus and anti-spam software from Trend Micro, and URL filtering software from Websense, Inc.

Both the Juniper/NetScreen and the Check Point products were paired with the Trend Micro and Websense offerings because the latter two

Figure 1. Product Lineup by Application Type

Product Lineup by Application Type			
Application	Integrated solution	Solution set #2	Solution set #3
Firewall	Astaro Security Linux	Juniper Networks/NetScreen	Check Point
VPN	Astaro Security Linux	Juniper Networks/NetScreen	Check Point
Anti-virus	Astaro Security Linux	Trend Micro	Trend Micro
Spam blocking	Astaro Security Linux	Trend Micro	Trend Micro
URL filtering	Astaro Security Linux	Websense	Websense

products represent likely choices for deployment by users. Moreover, in Check Point's case, the products support the company's OPSEC open security multivendor security framework.

The objective was to examine the productivity implications of deploying a fully integrated perimeter security solution from one vendor, versus a selection of so-called "best-of-breed" packages that organizations must integrate on their own. The Tolly Group examined the staffing time implications of deploying and supporting the solutions in a medium-sized network for an initial one-year period. The analysis focused strictly on personnel costs for deployment and ongoing support of the products tested; the analysis did not factor in upfront hardware investments, software costs, training or other tangential expenses.

Because the project focused on provisioning security services rather than benchmarking performance or validating specific functions, The Tolly Group did not need to invoke the vendor interaction aspects of its Fair Testing Charter.

Tolly Group engineers performed the evaluation in two phases:

One test group assessed the processes involved with upfront deployment of the integrated solution versus the two manually-integrated "suites." This comprised 13 initial setup processes, including:

- Configuring DHCP servers to provide addresses to local clients
- Configuring hosts/servers on the network
- Activation of the HTTP proxy for caching of Web content and URL filtering
- Configuration of the DMZ interface and definition of a Web server host IP address on the DMZ network
- Creation of a Quality of Service (QoS) policy to allow maximum bandwidth for HTTP traffic to the Web server
- Creation of packet filter rules to allow specific traffic on specific ports to designated hosts or servers defined on the internal network
- Configuration of a net-to-net VPN between two firewalls
- Backup of the entire configuration
- Re-installation of the full solution and re-application of the backed-up configuration on a new system (simulating backup and reinstallation in the event of a catastrophic event).

In addition to the initial implementation tasks, Tolly Group engineers subjected the three perimeter security solutions to a bevy of administrative support processes that would normally be conducted on a periodic basis.

The list included more than a dozen administrative functions that likely would occur at a company of the size specified for the scenario, including:

- Addition and removal of users on a monthly basis
- Addition and removal of users to existing content filtering profile(s)
- Definition of a new Web server or E-mail server
- Configuration of Web and/or E-mail server access on the DMZ interface, and addition of DNAT and QoS rules
- Addition of a new employee type with new security policies
- Configuration of automated backup of the complete system configuration, including packet filtering, URL filtering, anti-spam, and anti-virus services.

First-Year Security Effort

With any major IT discipline there are a multitude of upfront activities as well as recurring tasks. For the purpose of this white paper, we have simplified the assessment to focus on the front-end implementation labor for the software products tested, and also a selection of the ongoing maintenance and administrative support activities that would be common across a one-year period from point of installation.

Implementation

The initial deployment efforts related to implementation of the integrated package begins to reveal a common theme in the comparison to multiproduct solutions.

The Tolly Group found there could be anywhere from a 3X to 4X time premium to pay when installing, configuring and integrating the components of a "best-of-breed" solution.

Tolly Group engineers measured 13 implementation steps, recording the amount of time required to install the various products at a headquarters and at three remote sites.

Engineers recorded the amount of time required for such tasks as:

- Configure the DHCP server to serve the internal network and allocate IP addresses for workstations on the private network.
- Create a QoS policy to allow maximum bandwidth for HTTP traffic to the Web server.
- Create packet filter rules to allow specific traffic on specific ports to designated hosts or servers defined on the internal network.

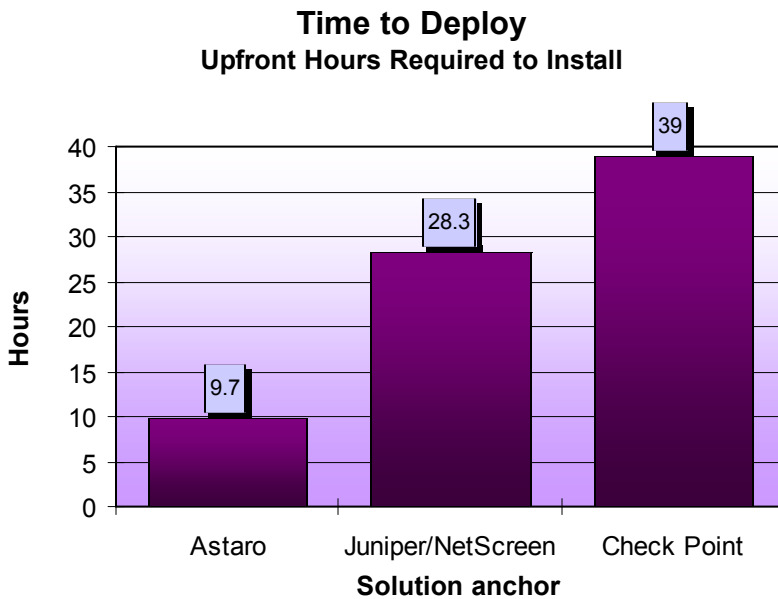
- Configure a net-to-net VPN between two firewalls.
- Backup the entire configuration, then re-install the full solution and re-apply the backed-up configurations on a replacement system.

(The full list of upfront personnel effort for all three solutions tested is available for viewing in Appendix A: Upfront Implementation Tasks.)

The implementation exercise conducted by Tolly Group engineers shows that the integrated solution, Astaro Security Linux, required just under 10 hours of effort to install, versus 28 hours for the Juniper Networks/Trend Micro/Websense bundle (firewall and VPN resided on a NetScreen-208 with other components running on a PC) and 39 hours for the bundle anchored by Check Point Software (all components running on two PCs.) See Figure 2.

The most sizable difference between the bundled point products and the integrated solution was in the area of backup and re-installation of the full solution.

Figure 2. Time to Deploy – Upfront Hours Required to Install



For Astaro Security Linux, the backup and re-install was fairly painless, taking just 20 minutes per site when the procedure was conducted across all four sites. The Juniper Networks and Check Point solutions did not fare nearly as well. Both solutions required 180 minutes (or three hours) of configuration backup, software re-installation, and re-application of configurations.

Part of that disparity results from the difference between Linux and Windows operating system environments. With Astaro Security Linux, the OS and the integrated applications are installed together with minimal user intervention, instead of needing to separately install and configure the underlying operating system.

The work for installing either the Juniper Networks-anchored solution set or the Check Point-anchored solution set was the same – more than 9 times the effort of installing the Astaro Security Linux offering.

The vast majority of those installation minutes were spent on re-installing the Microsoft OS components.

Host/Server Definition

Definition of server and host entries was another installation process that demonstrated the vast differences in complexity of the bundled solutions versus the relative simplicity of the integrated product.

Defining host/server entries takes just two minutes per device with Astaro Security Linux versus five minutes per device with Juniper Networks/NetScreen and 10 minutes per device with Check Point. That translates into a cost delta of almost five times between Astaro and other products tested.

Here, Tolly Group engineers used the three product sets to define 30 host/server entries for the headquarters site and five for each of the three remote sites, for a total of 45 entries. With Astaro Security Linux, each server/host definition required only two minutes each. That number jumped to five minutes each for the Juniper Networks solution and 10 minutes each for the Check Point solution.

For Astaro Security Linux, the server/host definition process consumed 90 minutes for 45 devices. With the Juniper Networks solution, the same task consumed 225 minutes, or 2.5X more minutes than with the integrated alternative.

Since the Check Point-anchored solution required 10 minutes per device definition, or 450 total minutes (7.5 hours of total configuration time), the total work for defining 45 host/servers was more than five times the effort for the same task with Astaro Security Linux.

Integration Challenges

In implementation process after implementation process examined by The Tolly Group, a common thread emerged to explain the vast differences in implementation time between the single-vendor package and the other two solutions – complexity due to lack of integration.

Astaro Security Linux is a fully preconfigured, all-in-one offering with tight coupling among firewall, VPN, URL filtering, anti-virus and anti-spam modules.

The Juniper Networks/NetScreen software, running on a NetScreen-208 appliance, was integrated with the Trend Micro and Websense products installed on a PC with the Windows Server operating system. For Websense, the install and initial configuration took more than one hour. When trying to integrate Websense with Juniper Networks, neither company provided sufficient documentation to aid with the process. And both companies pointed to each other when approached for help. After spending about five hours and having no luck with either company's documentation, Tolly Group engineers called Websense tech support. After an hour on the phone with tech support and two support persons, the integration between Websense and Juniper Networks was accomplished.

The integration of Trend Micro with Juniper Networks was much easier, because this "integration" was much more loosely coupled. For the anti-virus software, it took a little bit over an hour to install and configure all the required packages. OfficeScan v5.5 was installed and used for client anti-virus. Server Protect v5.56 was installed and used for server anti-virus. Each client must have the software downloaded and installed on the machine itself. The

A Tolly Group engineer invested 10 hours wading through and reading documentation trying to install and configure the Check Point software. The product's user interface and documentation are not user friendly.

anti-spam software, Trend Micro InterScan Messaging Security Suite v.5.5, took a little bit over an hour to install and configure.

The Check Point solution was much more involved and confusing.

For the Check Point-anchored solution, The Tolly Group used a Check Point NG with Application Intelligence (R55) for firewall and VPN, Websense 5.1 for URL filtering, Trend Micro OfficeScan 5.5 for client anti-virus, Trend Micro Server Protect 5.56 for server anti-virus and Trend Micro InterScan Messaging Security Suite 5.5 for anti-spam. The entire solution was software based and was installed on two PCs both running Windows 2000 Server with Service Pack 4.

The Check Point package was installed on one of the two PCs, with the other packages being installed on the other PC. We churned through more than 2 hours to format the hard drive, install the server operating system, install drivers, and check for and install Windows updates.

Then Tolly Group engineers spent 10 hours reading documentation and trying to install and configure the Check Point firewall and VPN gateway.

As Tolly Group engineers soon learned, Check Point does not provide tech support for the evaluation software version used for this project. In order to obtain any type of tech support one must have a support contract – but Check Point officials contacted said the company does not sell support contracts to customers of its evaluation code. However, the company would allow The Tolly Group to purchase support on a "per-incident" basis at a whopping \$445 per incident.

Engineers balked and brought in a Check Point consultant to aid in configuration and installation. The Tolly Group and the third-party consultant burned 16 hours (two people each working eight hours) working on installing Check Point- and all this was even before integrating the Trend Micro and the Websense products with the Check Point software.

Near the end, the consultant had to call a Check Point instructor to figure out some of the integration issues.

Once the Check Point software was installed, Tolly Group engineers were greeted with a user interface that looked more like a Microsoft Visio screen than it did software for performing firewall and VPN functions. Engineers did not find the GUI to be intuitive.

From an integration standpoint, the Websense install and initial configuration took over one hour. During the installation process you could choose what type of integration software or appliance you were using. Luckily for the engineers, there was an option for integrating with Check Point. After installing Websense and

creating some rules on Check Point, the integration process with Websense was completed.

Finally, engineers came to the integration of Trend Micro. This was much easier because the "integration" was less involved. For anti-virus, it took a little bit over an hour to install and configure all the required packages. OfficeScan v5.5 was installed and used for client anti-virus. Server Protect v5.56 was installed and used for server anti-virus. Each client/server must have the software downloaded and installed on the machine itself. Anti-spam took a little bit over an hour to install and configure the Trend Micro InterScan Messaging Security Suite v.5.5.

While Tolly Group engineers wrestled with the "best-of-breed" solutions, they experienced no such trials and tribulations with the integrated package.

Astaro Security Linux installed in 15 minutes off of a bootable CD-ROM onto a completely empty hard drive. Another 20 minutes was required to get the software up and running and to allow traffic to pass through to clients. The management interface, which Astaro calls WebAdmin, is nicely arranged and accessed via a secure Web browser (HTTPS). When you log in, you encounter a breakdown of each menu item and its purpose. Each menu item is self-descriptive. Clicking on a menu item gives you a breakdown of all sub-menus along with a short description of each. If you need help with a particular function, clicking on a blue square with a question mark inside gives you a very descriptive pop-up window. If more help is needed you can proceed to Astaro's online documentation at <http://docs.astaro.org> or browse the company's user bulletin board at www.astaro.org.

Recurring Administrative Support

The upfront deployment efforts tell only a part of the story when comparing an integrated solution to the "best-of-breed" combinations.

The first year's time expenditure to deploy and support the solutions revealed that there is a chasm between the support requirements for Astaro Security Linux and the Juniper Networks- and Check Point-anchored solutions.

Figure 3 shows that the monthly effort required to manage the integrated solution was 50% less than one of the point product sets and 62% less than the other.

Looking at the 16 monthly administrative functions examined by Tolly Group engineers (See Appendix B, First-Year Administrative/Support Tasks), it becomes clear that again there is a level of complexity affiliated with the joint administration of multiple point products.

For example, the Check Point solution required 33% more time to handle user moves, adds, and changes. That equates to two hours monthly, or 24 hours per year. Both the Juniper Networks and Astaro solutions required 16 hours annually to complete the same tasks.

One of the major discrepancies between the integrated package and the other solutions appears in the process for configuring a monthly backup of the complete system configuration. This involved the backup of information associated with the packet filtering, URL filtering, anti-spam and anti-virus services.

Because of the tight services integration implemented in Astaro Security Linux, the product required just two minutes to configure a monthly backup. Since the backup is conducted across all four sites (headquarters and three remote locations), the Astaro offering completed the task in eight minutes each month, or 96 minutes over a year.

By contrast, the Juniper Networks-anchored solution accomplished the configuration of monthly backup in 15 minutes per site, or 60 minutes for the four sites, for an annual time requirement of 720 minutes. That's more than 7 times the effort of configuring the backup with the integrated package.

The gap widens even further when we look at the Check Point-anchored solution. Here the same task took 30 minutes per site, or two hours for all four sites on a monthly basis. On an annual basis that works out to 960 minutes – 10 times the work of supporting the same process with Astaro Security Linux.

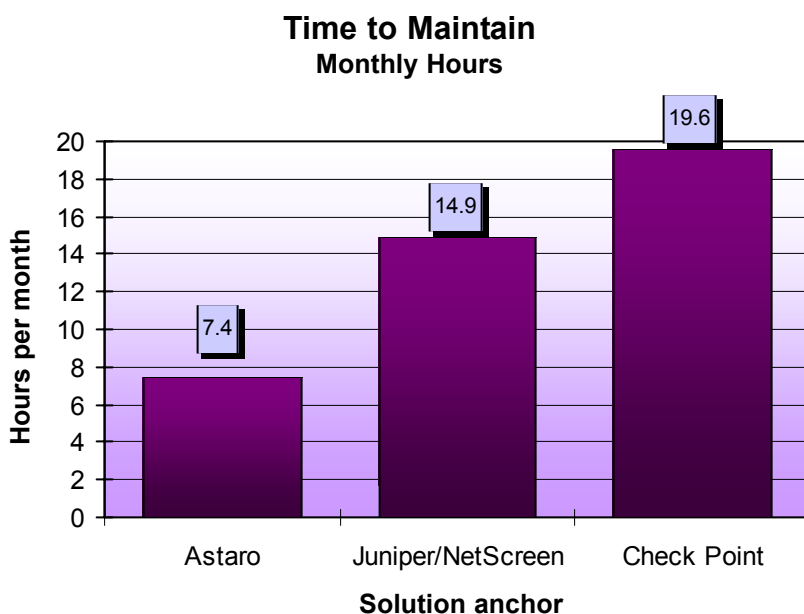
Time and time again, the complexity created by manually integrating multiple products became strikingly evident.

Seemingly simple processes, such as verifying that all systems have all software patches and updates, jump out as a key differentiator between the integrated package and the other solutions tested. This was a five-minute task with Astaro's software, played out across the four sites for 20 minutes total on a monthly basis. With Astaro, users receive auto alerts for automatic software updates.

With both the Juniper Networks-anchored solution and the Check Point-anchored solution, the same verification task chewed up 30 minutes per site, or two hours across the four sites – or six times the effort of the software update using Astaro.

A large factor in this disparity is the fact that Check Point does not provide users with the option of auto-

Figure 3. Time to Maintain – Monthly Hours



Check Point does not provide users with the option of automatic software updates or automatic backups of the configuration file. Astaro Security Linux does. There are considerable cost ramifications due to this.

matic software updates or automatic backups of the configuration file. Moreover, Websense does not provide users with the option of automatic backups of the configuration file. Also, users must halt all Websense services in order to accomplish either backup or restoration. Trend Micro does not provide users with the option of automatic backups of the anti-spam configuration file.

Lastly, if an integration server ever crashed and users face the prospect of rebuilding it, the task would consume at least three hours to reinstall Windows, apply all necessary updates, reinstall all integration packages, and apply the backups. That is, of course, if the user remembered to perform all of those manual backups.

With Astaro Security Linux, the auto backup configuration is handled once, and then it runs automatically, backing up data from the integrated services.

The Value of Integration

The IT staffs in medium-sized businesses, and even in large-scale enterprises, face the challenge of effectively deploying security in an integrated and efficient fashion across a company's enterprise network.

They may elect to roll their own, in effect integrating key component parts for firewall, VPN, URL filtering, anti-virus and anti-spam into a cohesive suite of applications that play well together.

The Tolly Group attempted to do just that in a simulated medium-sized business, in effect taking brand name firewall/VPN products from Juniper Networks/NetScreen and from Check Point and marrying those products individually to anti-virus/anti-spam offerings from Trend Micro Devices, and URL filtering from Websense.

Our staffing evaluation of the Juniper Networks- and Check Point-anchored solutions shows that users pay a prohibitive first-year penalty when they elect to integrate several products into a security suite for SMB or larger networks. For first-year implementation and ongoing support activities, the Juniper Networks-anchored solution requires almost twice the effort as the Astaro Security Linux offering. The Check Point-anchored solution took more than 2.5 times the work of Astaro Security Linux.

The penalty derives largely from the enormous complexity of integrating the various security offerings, as well as the limitations imposed by using Microsoft operating systems as the base operating environment.

Some users may ask, "Why does integration mean so much?" The answer lies in the complexity that users face when they roll their own suite of

security products. The single installation process, for example, means that administrators don't waste time re-installing operating system platforms, in addition to applications.

The single user interface of an integrated solution means personnel learn just one GUI, which makes administration easier, and faster. And a single update mechanism on an integrated suite means software updates can be automated, taking the personnel effort out of the equation.

The Tolly Group evaluation confirms that Astaro Security Linux is extremely easy to deploy and manage, because it is a truly integrated solution, not a "suite" of disparate products. The complete package works with:

- One installation CD, installable in 15 minutes
- One user interface for administration
- One set of management and reporting tools
- One integrated update mechanism

The Astaro solution is extremely cost-effective because it provides a full set of security tools for the price of a firewall and because the deployment and management costs are so low.

From a deployment perspective, the integrated solution requires one-third the number of hours to install as does its nearest competitor – the hybrid suite anchored by Juniper Networks.

The numbers are equally compelling in the integrated package's favor when considering the ongoing support costs over the first year after installation.

For a selected group of management tasks, Astaro Security Linux would require just about 71 hours of effort the first year – factoring in implementation and 12 months of support.

Compare that to the 137 hours that would be required to cover 12 months of the same support activities for the Juniper/NetScreen-anchored solution – almost twice the monthly administrative effort required to support the Astaro offering.

For the selected tasks that were tested, the Check Point solution set required 184 hours (implementation and 12 months of support) to manage over the first year. That works out to a 160% hike over the time required to support Astaro Security Linux.

Measurement issues aside, Tolly Group engineers wrestled constantly with both the Juniper Networks/NetScreen and Check Point solutions and the integration that had to occur between those products and the other security point packages from Websense and from Trend Micro.

Tolly Group engineers chronicled enormous pain experienced trying to learn user interfaces, understand nuances of security integration, and deal with confusing documentation or a lack documentation.

Systems administrators and IT managers need to tread carefully. While they can roll their own suite of security offerings, the degree of complexity and pain - which ultimately translates into dollar cost – seems to far outstrip any perceived advantage.

Tolly Group engineers experienced no problems from the Astaro Security Linux during the installation or the support stage. The product seems especially tailored for the needs of medium-sized businesses and other organizations with hard-pressed IT staffs. Astaro has done all of the integration work; users just deploy the product in minutes and avoid the mess that suite integrators are likely to face.

###

Appendix A: Upfront Implementation Tasks, Solution Worksheets

Astaro Solution				
Step	Implementation process	Unit time per site (minutes)	# sites	Total time (minutes)
1	Configure the DHCP server to serve the internal network and allocate IP addresses for workstations on the private network	5	4	20
2	Define additional entries for hosts or servers on the internal network (assumes 30 for HQ, 5 per remote site = 45 devices)	2 min/device	4	90
3	Activate SMTP or POP3 proxies for anti virus & anti spam (anti spam for SMTP only)	15	4	60
4	Activate the HTTP proxy for caching of web content and URL filtering	15	4	60
5	Configure the DMZ interface and define a web server host IP address on the DMZ network	5	1	5
6	Create a corresponding DNAT rule to allow traffic from the Internet to access the web server	5	1	5
7	Create a QOS policy to allow maximum bandwidth for HTTP traffic to the web server	5	1	5
8	Create additional packet filter rules to allow specific traffic on specific ports to designated hosts or servers defined on the internal network	5	4	20
9	Activate the PPTP server * Enable the PPTP server using the PPTP address pool * Create a packet-filtering rule to allow access for PPTP users to the internal network resources * Create a user in the local firewall user database * Create a PPTP network connection on a windows workstation to connect to the external interface IP address of the firewall using the username and password previously created in the firewall user database	30	1	30
10	Configure a NET-to-NET VPN between two firewalls. (NOTE-remote office firewall must be up and running to complete this step)	60	3	180
11	Configure the update service for both software and for anti virus definitions	2	4	8
12	Retrieve and apply an update patch	5	4	20
13	Backup the entire configuration and re-install the full solution on the previously configured box and re-apply the configurations	20	4	80
				583 9.7 hours

Juniper/NetScreen Solution

Step	Implementation process	Unit time per site (minutes)	# sites	Total time (minutes)
1	Configure the DHCP server to serve the internal network and allocate IP addresses for workstations on the private network	5	4	20
2	Define additional entries for hosts or servers on the internal network (assumes 30 for HW, 5 per remote site = 45 devices)	5 min/device	4	225
3	Activate SMTP or POP3 proxies for anti virus & anti spam (anti spam for SMTP only)	30	4	120
4	Activate the HTTP proxy for caching of web content and URL filtering	30	4	120
5	Configure the DMZ interface and define a web server host IP address on the DMZ network	5	1	5
6	Create a corresponding DNAT rule to allow traffic from the Internet to access the web server.	15	1	15
7	Create a QOS policy to allow maximum bandwidth for HTTP traffic to the web server (Time rolled in to step 6 since they are defined concurrently on same screen)	0	0	0
8	Create additional packet filter rules to allow specific traffic on specific ports to designated hosts or servers defined on the internal network	20	4	80
9	Activate the PPTP server * Enable the PPTP server using the PPTP address pool * Create a packet-filtering rule to allow access for PPTP users to the internal network resources * Create a user in the local firewall user database * Create a PPTP net	30	1	30
10	Configure a NET-to-NET VPN between two firewalls (NOTE-remote office firewall must be up and running to complete this step)	60	3	180
11	Configure the update service for both software and for anti virus definitions	15	4	60
12	Retrieve and apply an update patch	30	4	120
13	Backup the entire configuration and re-install the full solution on the previously configured box and re-apply the configurations	180	4	720
				1,695 28.3 hours

Check Point Solution

Step	Implementation process	Unit time per site (minutes)	# sites	Total time (minutes)
1	Configure the DHCP server to serve the internal network and allocate IP addresses for workstations on the private network	30	4	120
2	Define additional entries for hosts or servers on the internal network (assumes 30 for HW, 5 per remote site = 45 devices)	10 min/device	4	450
3	Activate SMTP or POP3 proxies for anti virus & anti spam (anti spam for SMTP only)	30	4	120
4	Activate the HTTP proxy for caching of web content and URL filtering	45	4	180
5	Configure the DMZ interface and define a web server host IP address on the DMZ network	10	1	10
6	Create a corresponding DNAT rule to allow traffic from the Internet to access the web server	10	1	10
7	Create a QOS policy to allow maximum bandwidth for HTTP traffic to the web server (Time rolled in to step 6 since they are defined concurrently on same screen)	10	1	10
8	Create additional packet filter rules to allow specific traffic on specific ports to designated hosts or servers defined on the internal network	30	4	120
9	Activate the PPTP server * Enable the PPTP server using the PPTP address pool * Create a packet-filtering rule to allow access for PPTP users to the internal network resources * Create a user in the local firewall user database * Create a PPTP net	120	1	120
10	Configure a NET-to-NET VPN between two firewalls (NOTE-remote office firewall must be up and running to complete this step)	120	3	360
11	Configure the update service for both software and for anti virus definitions	0	0	0
12	Retrieve and apply an update patch	30	4	120
13	Backup the entire configuration and re-install the full solution on the previously configured box and re-apply the configurations	180	4	720
				2,340 39 hours

Appendix B: Ongoing Support Tasks, Solution Worksheets

Astaro Solution — Annual Recurring Admin Effort						
Step	Implementation process	Unit time per site (minutes)	# sites	Total time (minutes)	Frequency	Annualized time commitment (minutes)
1	Add and remove new users • Add and delete 10 users per month, including both office workers and road warriors, typical of a business network in a company that has recently experienced employee turnover	20	4	80	12	960
2	Remove or add the 10 users to existing content filtering profile(s)	15	4	60	12	720
3	Change the IP addresses of the interfaces to accommodate a move with renumbering of the networks to be used	5	4	20	12	240
4	Add a new employee type with new security policies (e.g. Regional Sales Manager) • Create a new policy for new user(s) with a unique content filtering rule set • Configure a packet filtering rule(s) to allow these users access to specific devices on the network or DMZ	10	4	40	6	240
5	Define a new web server or email server (20 events * 2 min)	2	20	40	1	40
6	Configure Web &/or email server access on the DMZ interface and add DNAT and QOS rules	15	1	15	12	180
7	Accommodate a change of ISP's (i.e. new provider) • Change the external interface configuration to Utilize DHCP from a broadband provider	10	4	40	1	40
8	Add remove VPN configurations for remote users (Road warriors) Perform this step for both remote and main office	5	4	20	12	240
9	Add new networks and hosts	1	1	15	1	15
10	Add additional POP3/SMTP server to be filtered for Anti Virus (assumes two devices per month)	10	2	20	4	80
11	Create a packet filter rule to allow access to internal network for a support engineer from a specific outside IP address	5	4	20	12	240
12	Delete the rule created in the step above	1	4	4	12	48
13	Generate reports on Web usage for internal employees	5	4	20	12	240
14	Verify all systems have ALL software patches and updates	5	4	20	12	240
15	Configure monthly backup of the complete system configuration • Packet filter • URL filtering • Anti Spam • Anti Virus	2	4	8	12	96
16	Restore full configuration backup to all components listed in the step above	5	4	20	1	20
				442		3,639
				7.37		61 hours

Juniper/Net Screen Solution — Annual Recurring Admin Effort

Step	Implementation process	Unit time per site (minutes)	# sites	Total time (minutes)	Frequency	Annualized time commitment (minutes)
1	Add and remove new users • Add and delete 10 users per month, including both office workers and road warriors, typical of a business network in a company that has recently experienced employee turnover	20	4	80	12	960
2	Remove or add the 10 users to existing content filtering profile(s)	20	4	80	12	960
3	Change the IP addresses of the interfaces to accommodate a move with renumbering of the networks to be used	5	4	20	12	240
4	Add a new employee type with new security policies (e.g. Regional Sales Manager) • Create a new policy for new user(s) with a unique content filtering rule set • Configure a packet filtering rule(s) to allow these users access to specific devices on the network or DMZ	20	4	80	6	480
5	Define a new web server or email server (20 events * 2 min)	5	20	100	1	100
6	Configure Web &/or email server access on the DMZ interface and add DNAT and QOS rules		1	20	12	240
7	Accommodate a change of ISP's (i.e. new provider) • Change the external interface configuration n to Utilize DHCP from a broadband provider	10	4	40	1	40
8	Add remove VPN configurations for remote users (Road warriors) Perform this step for both remote and main office	5	4	20	12	240
9	Add new networks and hosts (6 at HQ, 3 per remote site)	3	1	45	1	45
10	Add additional POP3/SMTP server to be filtered for Anti Virus (assumes two devices per month)	20	2	40	4	160
11	Create a packet filter rule to allow access to internal network for a support engineer from a specific outside IP address	5	4	20	12	240
12	Delete the rule created in the step above	2	4	8	12	96
13	Generate reports on Web usage for internal employees	10	4	40	12	480
14	Verify all systems have ALL software patches and updates	30	4	120	12	1,440
15	Configure monthly backup of the complete system configuration • Packet filter • URL filtering • Anti Spam • Anti Virus	15	4	60	12	720
16	Restore full configuration backup to all components listed in the step above	30	4	120	1	120
				893		
				14.88		
						6,561
						109 hours

Check Point Solution — Annual Recurring Admin Effort						
Step	Implementation process	Unit time per site (minutes)	# sites	Total time (minutes)	Frequency	Annualized time commitment (minutes)
1	Add and remove new users • Add and delete 10 users per month, including both office workers and road warriors, typical of a business network in a company that has recently experienced employee turnover	30	4	120	12	1,440
2	Remove or add the 10 users to existing content filtering profile(s)	30	4	120	12	1,440
3	Change the IP addresses of the interfaces to accommodate a move with renumbering of the networks to be used	10	4	40	12	480
4	Add a new employee type with new security policies (e.g. Regional Sales Manager) • Create a new policy for new user(s) with a unique content filtering rule set • Configure a packet filtering rule(s) to allow these users access to specific devices on the network or DMZ	20	4	80	6	480
5	Define a new web server or email server (20 events * 2 min)	5	20	100	1	100
6	Configure Web &/or email server access on the DMZ interface and add DNAT and QOS rules	30	1	30	12	360
7	Accommodate a change of ISP's (i.e. new provider) • Change the external interface configuration n to Utilize DHCP from a broadband provider	30	4	120	1	120
8	Add remove VPN configurations for remote users (Road warriors) Perform this step for both remote and main office	15	4	60	12	720
9	Add new networks and hosts (6 at HQ, 3 per remote site)	5	1	75	1	75
10	Add additional POP3/SMTP server to be filtered for Anti Virus (assumes two devices per month)	20	2	40	4	160
11	Create a packet filter rule to allow access to internal network for a support engineer from a specific outside IP address	10	4	40	12	480
12	Delete the rule created in the step above	5	4	20	12	240
13	Generate reports on Web usage for internal employees	10	1	10	12	120
14	Verify all systems have ALL software patches and updates	30	4	120	12	1,440
15	Configure automated backup of the complete system configuration • Packet filter (15 minutes) • URL filtering (no auto backup provided) • Anti Spam (no auto backup provided) • Anti Virus (5 minutes)	20	4	80	12	960
16	Restore full configuration backup to all components listed in the step above	30	4	120	1	120
				1175		8,735
				19.58		145 hours

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.



The Tolly Group, Inc.
 3701 FAU Blvd. Suite 100
 Boca Raton, FL 33431
 Phone: 561.391.5610
 Fax: 561.391.5810
<http://www.tolly.com>
info@tolly.com



The Tolly Group doc. 204128 rev. clk 28 July 04