THE TOLLY GROUP

The authoritative, unbiased source for IT certification, research and testing

WHITE PAPER

July 2004

A white paper commissioned by Astaro Corporation
Document #204128-DE

Netzwerksicherheit: All-in-One-Loesungen und Einzelkomponenten im Kostenvergleich

Ein praxisorientierter Vergleich der Installations- und Wartungskosten von All-In-One Loesungen gegenueber Komponentenloesungen - Astaro Security Linux im Vergleich mit Checkpoint und Juniper/NetScreen

Statement of Licensing Info and Acceptable Usage

THE TOLLY GROUP

For additional information on acceptable usage of this document (Tolly Group Document #204128-DE) contact The Tolly Group at (561) 391-5610 or via E-mail: sales@tolly.com.

Unternehmensbereiche

1989 - 2004 15 Years TOLLY

Mit mehr als 15 Jahren Erfahrung bei der Beurteilung und Analyse von führenden IT-Produkten und - Diensten hat sich das Testinstitut The Tolly Group weltweit einen Namen als zuverlässige und unab hängige Organisation gemacht. Wir verwenden bewährte Testmethoden und faire Untersuchungsprinzipien, um Produkte und Dienstleistungen mit der höchsten Genauigkeitsrate zu bewerten.

Tolly Verified

Seit 2003 bietet The Tolly Group mit "Tolly Verified" ein Leistungspaket an, das eine detaillierte und herstellerneutrale Zertifizierung von Features, Funktionalitäten und Leistungscharakteristika ver schiedener Technologien wie WLAN Switching und Antispam ermöglicht. Mehr Informationen finden Sie auf der Webseite "Tolly Verified".

TOLLY Up to Spec CERTIFIED

Unter dem Namen "Up to Spec" bieten wir ein maßgeschneidertes Diensleistungspaket, das die stan dardisierten Grundlagentests von "Tolly Verfied" ergänzt. Mehr Informationen finden Sie auf der Webseite "Up to Spec".

TOLLY First & Foremost CERTIFIED

Die Auszeichnung "First & Foremost" wird an Produkte verliehen, die in den Testlabors der Tolly Group bahnbrechende Performancewerte und Funktionalitäten nachweisen können. Die Auszeichnung geht nicht nur an wegweisende Innovatoren, sondern umfasst auch über durchschnit tliche Produkttestergebnisse, die in einzelnen Technologiesparten neue Maßstäbe setzen. Mehr Informationen finden Sie auf der Webseite "First & Foremost".

Darüber hinaus kombiniert The Tolly Group ihr umfassendes Technologiewissen mit fokussierten Marketingdienstleistungen, die Kunden bei der Kommunikation von Produktbenchmarks helfen.

This document was authored by:

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

Inhaltsverzeichnis

Schaubilder

Lohnt sich ein integriertes Sicherheitskonzept?

Überblick

Nach Untersuchungen des Marktforschungsunternehmens IDC Research bezifferte sich der Firewall-Markt 2003 auf ein Gesamtvolumen von 3,8 Milliarden US-Dollar und soll 2005 voraussichtlich 5,5 Milliarden US-Dollar betragen. Der Software-Markt für Content-Sicherheitslösungen wird in diesem Zeitraum von 2,9 Milliarden US-Dollar auf 4,1 Milliarden US-Dollar wachsen. Analysten schätzen, dass integrierte Sicherheitslösungen die höchsten Wachstumsraten aufweisen werden.

Ergebnisse der Studie:

- Einzelkomponenten benötigen 2,9 bis 4 mal mehr Zeit bei Konfiguration und Installation als integrierte Systeme.
- Einzelkomponenten benötigen 1,8 bis 2,4 mal mehr Zeit bei Management und im täglichen Einsatz als integrierte Sicherheitslösungen.
- Eine einheitliche Benutzeroberfläche, ein automatischer Update-Mechanismus und integrierte Management-Tools sind deutliche Vorteile einer integrierten Sicherheitslösung.

In der Informationstechnologie gibt es eine beständige Debatte darüber, ob integrierte Sicherheitslösungen gegenüber Einzelkomponenten im Vorteil sind.

Ist es besser, verschiedene verwandte Technologien von einem Anbieter als integriertes Komplettpaket zu erwerben oder empfiehlt es sich, mehrere separate Produkte bekannter Anbieter auszuwählen?

Teilweise beantwortet der Markt diese Frage wie im Fall von Microsoft Office and anderer Office-Pakete, die als Komplettlösungen separate Einzelkomponenten verdrängten.

Ein umfassender Test einer unabhängigen Organisation, die den tatsächlichen Wert integrierter Sicherheitskonzepte im Vergleich zu komplementären Technologien untersucht, hat jedenfalls bei dieser Thematik Seltenheitswert.

Mit dieser Studie beauftragte Astaro das Testinstitut The Tolly Group, durch eine Reihe praxisorientierter Tests die technologischen Charakteristika und Kostenunterschiede von All-in-One-Netzwerksicherheitslösungen gegenüber einer Reihe von Einzelkomponenten zu ermitteln.

Im Test wurde die Komplettlösung Astaro Security Linux mit zwei Einzelkomponenten verglichen, den Firewall-/VPN-Produkten von Juniper Networks (ehemals NetScreen Technologies) und Check Point Software Technologies Corporation. Beide Lösungen nutzten die Antivirus- und Antispam-Software von Trend Micro Devices sowie die URL-/Content-Filtersoftware der Websense Corporation.

Die durchgeführten Praxistests sollten ermitteln, wie groß der vergleichsweise Aufwand für ein typisches Mittelstandsunternehmen ist, eine umfassende Sicherheitslösung über einen Zeitraum von zwölf Monaten einzusetzen und zu handhaben.

Voraussetzung hierbei war, dass alle Sicherheitslösungen die heute notwendigen Sicherheitsanforderungen moderner Unternehmen, wie zum Beispiel Firewall-Paketfilterung, VPN-Kommunikation, Internet-Content-Sicherheit sowie Antispam-, Antiviren- und URL-Filtersoftware abdecken .

Die Ergebnisse waren sehr deutlich. Die Einzelkomponenten benötigten mehr als dreimal mehr Zeit bei Konfiguration und Installation. Im Langzeitversuch benötigten Einzelkomponenten zwei bis zweieinhalb mal mehr Zeit bei Management und im täglichen Einsatz als die integrierte Sicherheitslösung.

Das Testszenario

Das Technikerteam der Tolly Group simulierte den Einsatz der Sicherheitslösungen innerhalb einer 1.200 Mann starken Organisation, die aus einem Hauptsitz mit 750 Mitarbeitern und drei Niederlassungen mit je 100 bis 250 Anwendern bestand. (Die Tolly-Group-Techniker errichteten nicht das eigentliche Netzwerk, sondern beurteilten die Sicherheitslösungen anhand der in einem solchen Netzwerk anfallenden Support- und Wartungsarbeiten.)

Ein Mittelstandsunternehmen als Einsatzszenario eignete sich insofern besonders gut, weil einerseits die ganze Bandbreite moderner Sicherheitsanwendungen zum Einsatz kommt - Firewall, Virtual Private Network, Antivirus, Spamschutz und URL-Filter - und andererseits die Verfügbarkeit spezialisierten Sicherheitspersonals nicht die Regel ist. Insofern ist hier der Druck besonders groß, die Produktivität des Systemadministrators oder IT-Managers zu maximieren. Die Ergebnisse der Studie sollten sich aber stufenweise auf kleinere und größere Unternehmen übertragen lassen.

Das Technikerteam der Tolly Group führte verschiedene Tests durch, die die folgenden Fragen beantworten sollten:

- **Installation und Konfiguration von Software-Sicherheitspaketen.** Worin liegen die Unterschiede beim erforderlichen Installationsaufwand einer integrierten Netzwerk-Sicherheitslösung gegenüber Einzelkomponenten?
- **Administrationsaufgaben.** Wo liegen die Unterschiede einer integrierten Komplettlösung gegenüber Einzelkomponenten im Hinblick auf Backup und Änderungsmanagement? Welche Unterschiede sind erkennbar bei der Durchführung von Administrationsaufgaben während des Testzeitraums?
- **Software-Updates und -Verteilung.** Wo liegen die Unterschiede, wenn die Software mit erforderlichen Patches, aktuellen Virensignaturen etc. auf den neuesten Stand gebracht werden soll?
- **Konfigurationsänderungen.** Wieviel Administrationsaufwand entsteht bei häufigen Konfigurationsänderungen, wenn zum Beispiel neue User angelegt, Einstellungen geändert oder Policy-Updates durchgeführt werden müssen?

Die Tests wurden mit drei Sicherheitssystemen durchgeführt:

- Astaro Security Linux, eine integrierte Sicherheitslösung, die Firewall und VPN-Gateway mit Spam-, Surf- und Virus-Protection kombiniert.
- Ein Produktpaket, das auf Firewall-, VPN-, Antivirus- und Antispam-Technologie von Juniper/NetScreen und URL-Filtersoftware von Websense basiert.
- Ein Produktpaket, das auf Firewall-, VPN-, Antivirus- und Antispam-Technologie der Check Point Software Technologies Corporation und Anti-Spam Software von Trend Micro, sowie der URL-Filtersoftware von Websense basiert.

Sowohl die Juniper/NetScreen-Lösung als auch das Check-Point-System wurden

Schaubild 1. Übersicht über verwendete Produkte

Übersicht über verwendete Produkte			
Applikation	Integrierte Komplettlösung	Lösungspaket 2	Lösungspaket 3
Firewall	Astaro Security Linux	Juniper Networks	Check Point
VPN	Astaro Security Linux	Juniper Networks	Check Point
Anti-virus	Astaro Security Linux	Trend Micro	Trend Micro
Spamschutz	Astaro Security Linux	Trend Micro	Trend Micro
URL-Filter	Astaro Security Linux	WebSense	WebSense

wahrscheinliche Kombinationen bei der Installation gelten. Darüber hinaus unterstützen diese Softwareprodukte im Fall von Check Point den OPSEC-Standard (Open Platform for Security) des Unternehmens.

Das Ziel der Untersuchungen war, die Unterschiede bei Produktivität und Installation einer integrierten Sicherheitslösung eines einzigen Anbieters dem Best-of-Breed-Ansatz gegenüberzustellen, bei dem Organisationen alle Integrationsarbeiten selber leisten müssen. Die Tolly Group ermittelte über einen Zeitraum von einem Jahr die anfallenden Personalkosten bei Installation und Wartung der Lösungen in einem mittelgroßen Netzwerk. Die Studie konzentrierte sich voll und ganz auf die bei Installation und weiterführendem Support entstehenden Personalkosten; im Voraus anfallende Hardware-Investitionen, Software-Kosten oder andere vergleichbare Ausgaben wurden nicht berücksichtigt.

Bei diesem Projekt beschränkte sich die Tolly Group auf Dienstleistungsaspekte und arbeitete mit den betroffenen Anbietern nicht bei der Ermittlung von Benchmarkwerten oder bei technischen Funktionalitätsvergleichen zusammen, wie es die Richtlinien der hauseigenen "Fair Testing Charter" vorsehen.

Die Tolly-Group-Techniker unterteilten den Evaluationsprozess in zwei Phasen:

Eine Testgruppe beurteilte die Prozesse, die bei der Installation einer integrierten Sicherheitslösung anfallen und verglich sie mit dem Ergebnis der beiden manuell zu integrierenden Produktpakete. Insgesamt 13 Setup-Prozesse flossen in die Wertung ein:

- Konfiguration von DHCP-Servern für die Bereitstellung von Adressen an lokale User
- Konfiguration der Hosts und Server im Netzwerk
- Aktivierung des HTTP-Proxys für die Zwischenspeicherung von Webinhalten und URL-Filterung
- Konfiguration der DMZ-Schnittstelle und Eingabe von Webserver-Host-Adressen des DMZ-Netzwerks
- Einrichten einer QoS-Policy (Quality of Service) für die Bereitstellung maximaler Bandbreite beim HTTP-Datenverkehr auf dem Webserver
- Einrichten der Paketfilterregeln, um spezifischen Datenverkehr über bestimmte Ports oder Server im internen Netzwerk laufen zu lassen
- Konfiguration eines Net-to-Net-VPNs zwischen zwei Firewalls
- Backup der gesamten Konfiguration
- Neuinstallation der Gesamtlösung und Einspielen der Backup-Konfiguration auf einem neuen System (Simulation von Backup und Neuinstallation bei Systemausfall durch äußeres Ereignis).

Zusätzlich zu dem im Vorfeld untersuchten Implementierungsaufwand unterzog das Technikerteam der Tolly Group die drei Sicherheitslösungen einer Reihe von Administrationsaufgaben, die normalerweise im täglichen Einsatz regelmäßig anfallen.

Zu den untersuchten Aufgaben zählten über ein Dutzend Administrationsroutinen, die für ein Unternehmen in dem oben skizzierten Einsatzszenario typisch sind:

- Monatliches Hinzufügen und Löschen von User-Accounts
- Hinzufügen und Löschen von Usern im Rahmen existierender Content-Filter-Profile
- Einrichten eines neuen Web-Servers oder E-Mail-Servers
- Konfiguration des Zugangs zum Web- und/oder E-Mail-Server auf dem DMZ-Interface und Hinzufügen von DNAT- und QoS-Regeln
- Hinzufügen eines neuen Mitarbeiterprofils mit neuen Sicherheitspolicies
- Konfiguration eines automatischen Backups des kompletten Systems mit Paketfilter, URL-Filter, Spamschutz und Antivirendiensten

Sicherheitsaufwand im ersten Jahr

Bei jeder größeren IT-Untersuchung gibt es eine Vielzahl von vorausgehenden Arbeiten und wiederkehrenden Aufgaben. Im Rahmen dieses White Papers haben wir die Beurteilung vereinfacht und uns bei den untersuchten Softwareprodukten auf die Implementierungsarbeiten auf der Front-End-Ebene fokussiert. Bei den anfallenden Wartungs- und Administrationsarbeiten haben wir ebenfalls eine Vorauswahl getroffen und auf typische Fälle während des einjährigen Tests reduziert.

Implementierung

Die ersten Installationsarbeiten bei der Implementierung der integrierten Sicherheitslösung zeigt eine allgemeingültige Erkenntnis beim Vergleich mit Einzelkomponenten.

Die Untersuchungen der Tolly Group zeigten, dass für die Installation, Konfiguration und Integration der Einzelkomponenten unterschiedlicher Hersteller ein drei bis vier mal höherer Aufschlag anzurechnen ist.

Das Technikteam der Tolly Group berücksichtigte insgesamt 13 Implementierungsschritte und notierte den Zeitaufwand, der bei der Installation der unterschiedlichen Produkte im Hauptsitz und in den drei Niederlassungen anfiel.

Der Zeitaufwand wurde vom Technikteam für folgende Aufgaben ermittelt:

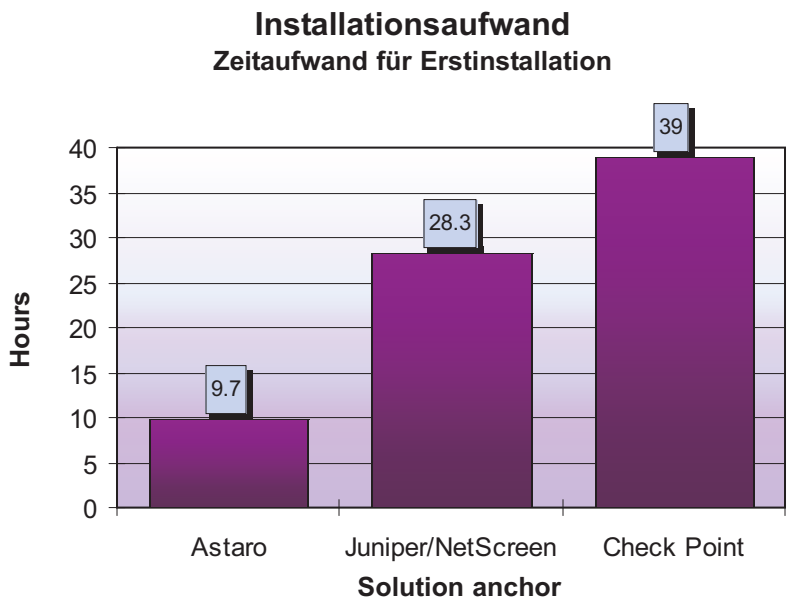
- Konfiguration des im internen Netzwerk eingesetzten DHCP-Servers und Zuweisung der IP-Adressen für die Workstations im privaten Netzwerk.
- Einrichten einer QoS-Policy (Quality of Service) für die Bereitstellung maximaler Bandbreite beim HTTP-Datenverkehr auf dem Webserver.
- Einrichten der Paketfilterregeln, um spezifischen Datenverkehr über bestimmte Ports oder Server im internen Netzwerk laufen zu lassen.

- Konfiguration eines Net-to-Net-VPNs zwischen zwei Firewalls.
- Backup der gesamten Konfiguration und Neuinstallation der Gesamtlösung und Einspielen der Backup-Konfiguration auf einem neuen System.

(Die vollständige Liste mit dem für alle drei Lösungen anfallenden Personalaufwand befindet sich in Anhang A: Installationsaufgaben, Ergebnisübersicht.)

Nach erfolgreicher Implementierung durch das Technikerteam der Tolly Group zeigte sich, dass die integrierte Sicherheitslösung Astaro Security Linux mit einem Installationsaufwand von zehn Stunden unter dem Aufwand von 28 Stunden des Softwarepakets "Juniper Networks/Trend Micro/Websense" (Firewall und VPN-Gateway befanden sich auf einer NetScreen-208, andere Komponenten liefen auf einem PC) und auch unterhalb des Wertes von 39 Stunden für die auf Check-Point-Software basierten Lösung (alle Komponenten liefen auf zwei PCs) lag. Weitere Informationen befinden sich auf Schaubild 2.

Schaubild 2. Installationsaufwand – Zeitaufwand für Erstinstallation



Der deutlichste Unterschied zwischen den Systemen aus Einzelkomponenten und der integrierten Komplettlösung zeigte sich bei der Datensicherung und der Neuinstallation des Gesamtsystems.

Im Fall von Astaro Security Linux waren das Backup und die Neuinstallation relativ problemlos mit einem durchschnittlichen Zeitaufwand von 20 Minuten pro Site, wenn man die Schritte in allen vier Netzwerken durchführte. Bei den Lösungspaketen von Juniper Networks und Check Point war die Prozedur nicht annähernd so einfach. Für Backup-Konfiguration, Neuinstallation der Software und Neustart aller Applikationen war bei diesen Systemen ein Zeitaufwand von 180 Minuten (also drei Stunden) erforderlich.

Die unterschiedlichen Ergebnisse resultierten zum Teil aus der Verschiedenartigkeit der Betriebssysteme Windows und Linux. Bei Astaro Security Linux wird das Betriebssystem zusammen mit den integrierten Applikationen installiert, ohne dass der User weitere Konfigurationsschritte oder separate Installationen durchführen muss.

Der Arbeitsaufwand für die Erstinstallation des Juniper-Networks-Pakets und der Check-Point-Lösung war zwar gleich groß, allerdings insgesamt neun mal zeitaufwändiger als die Astaro-Security-Linux-Installation. Der Hauptteil der Installationszeit entfiel auf die Installationsroutinen der Microsoft-Betriebssystemkomponenten.

Für die Einrichtung der Host-/Server-Einträge benötigte Astaro Security Linux nur zwei Minuten pro Gerät, wofür Juniper Networks/NetScreen fünf Minuten und Check Point zehn Minuten brauchten. Das reduziert die bei Astaro Security Linux anfallenden Kosten im Vergleich zu den anderen Pordukten um das Fünffache.

Host-/Server-Konfiguration

Die Einrichtung der Server- und Host-Einträge offenbarte bei der Installation ebenfalls die großen Komplexitätsunterschiede der Systeme aus Einzelkomponenten im Vergleich zum relativ einfach handhabbaren integrierten Produkt.

Dabei verwendeten die Techniker der Tolly Group die drei Produktpakete, um 30 Host-/Server-Einträge für den Hauptsitz und jeweils fünf für die drei Niederlassungen, insgesamt also 45 Einträge, einzurichten. Mit Astaro Security Linux waren für die Host-/Server-Eingabe lediglich je zwei Minuten erforderlich. Bei der Juniper-Networks-Lösung stieg dieser Wert auf fünf Minuten und bei der Check-Point-Lösung auf zehn Minuten.

Der gesamte Einrichtungsprozess der Server-/Host-Einträge dauerte bei Astaro Security Linux 90 Minuten für 45 Geräte. Die Juniper-Networks-Lösung verbrauchte für die gleiche Prozedur 225 Minuten, 2,5 mal mehr Zeit also als die integrierte Sicherheitslösung.

Bei der Check-Point-Lösung betrug der Zeitaufwand zehn Minuten pro Gerät, insgesamt also 450 Minuten (ein Konfigurationsaufwand von 7,5 Stunden). Im Vergleich zu Astaro Security Linux war der Arbeitsaufwand für die 45 Host/Server-Einträge damit fünf mal höher.

Herausforderungen bei der Integration

Mit jedem von der Tolly Group durchgeführten Implementierungsprozess wurde deutlich, dass die Unterschiede in puncto Arbeitsaufwand zwischen der integrierten Komplettlösung und den beiden anderen Produkten auf eine Ursache zurückzuführen ist: Fehlende Integration resultiert in steigender Komplexität.

Astaro Security Linux ist ein vorkonfiguriertes All-in-One-Paket, das Firewall, VPN-Gateway und URL-Filter mit Antivirus- und Antispam-Modulen verbindet.

Ein Techniker der Tolly Group investierte zehn Stunden Arbeitszeit, um die Check-Point-Software zu installieren und konfigurieren und sich durch die umfangreiche Dokumentation hindurchzukämpfen. Die Bedienungsoberfläche und Begleitliteratur der Lösung sind nicht benutzerfreundlich.

Die Juniper-Networks-/NetScreen-Software lief auf einer NetScreen-208-Appliance und wurde zusammen mit den Trend-Micro- und Websense-Produkten auf einem Windows-PC installiert. Allein für Websense war ein Installations- und Konfigurationsaufwand von über einer Stunde erforderlich. Beim Versuch, die Websense- und Juniper-Networks-Lösungen zu integrieren, stellte keines der beiden Unternehmen ausreichendes Dokumentationsmaterial für den Prozess zur Verfügung. Und beide Firmen verwiesen auf die jeweilige Gegenseite, wenn man nach Support-Unterstützung fragte. Nach ungefähr fünf Stunden Arbeit und ohne zufriedenstellende Unterlagen, erkundigten sich die Tolly-Group-Techniker bei der Websense-Support-Hotline nach Lösungsvorschlägen. Nach einer Stunde am Telefon schaffte das Technikerteam im Zusammenspiel mit insgesamt zwei Support-Leuten die erfolgreiche Integration der Lösungen von Websense und Juniper Networks.

Die Integration der Software von Trend Micro und Juniper Networks verlief erheblich einfacher, weil die Anbindung weniger umfassend war. Für die Antiviren-Software war etwas mehr als eine Stunde nötig, um die erforderlichen Komponenten zu installieren und zu konfigurieren. Auf der Client-Ebene kam OfficeScan v5.5 zum Einsatz. Auf der Server-Ebene wurde Server Protect v5.5 installiert. Die Software muss dabei auf jedem Client-Rechner einzeln heruntergeladen und installiert werden. Die Antispam-Software Trend Micro InterScan Messaging Security Suite v5.5 benötigte etwas mehr als eine Stunde für Installation und Konfiguration.

Erheblich mehr Aufwand war für die Check-Point-Lösung erforderlich.

Das von der Tolly Group verwendete Check-Point-Lösungspaket bestand aus einer Check Point NG mit Application Intelligence (R55) als Firewall und VPN-Gateway, Websense 5.1 als URL-Filter, Trend Micro OfficeScan 5.5 als Antivirenlösung auf Client-Ebene, Trend Micro Server Protect 5.56 als Antivirenlösung auf Server-Ebene und Trend Micro InterScan Messaging Security Suite 5.5 als Spamschutz. Die gesamte Softwarelösung wurde auf zwei Windows-Server-2000-PCs mit Service Pack 4 installiert.

Die Check-Point-Komponenten wurden auf einem PC installiert, die anderen Applikationen liefen auf dem zweiten Rechner. Über zwei Stunden wühlten wir uns durch die Installationsroutinen, um die Festplatte zu formatieren, das Server-Betriebssystem einzurichten, die Treiber zu installieren und Windows-Updates abzufragen und einzuspielen.

Danach verbrachten die Techniker der Tolly Group zehn Stunden damit, die Dokumentation durchzulesen und die Check-Point-Firewall mitsamt VPN-Gateway zu installieren und konfigurieren.

Schnell fand das Tolly-Group-Technikteam heraus, dass Check Point keinerlei technischen Support für die eingesetzte Testsoftware leistet, die bei diesem Projekt zum Einsatz kam. Um überhaupt technischen Support zu erhalten, muss man einen Supportvertrag abschließen - bei Check Point hieß es aber von offizieller Seite, dass das Unternehmen keine Supportverträge an Nutzer der eingesetzten Testsoftware verkauft. Allerdings erklärte sich die Firma dazu bereit, der Tolly Group Supportleistungen zu einem Preis von 445 US-Dollar pro Problemfall anzubieten.

Das Technikteam umging dieses Hindernis und arbeitete mit einem Check-Point-Berater bei Installation und Konfiguration zusammen. Die Tolly Group und der externe Dienstleister mussten 16 Stunden aufwenden (zwei Personen benötigten jeweils acht Stunden Arbeit), um allein die Check-Point-Software zum Laufen zu bringen. Die Installation der Trend-Micro- und Websense-Produkte mit anschließender Integration in die Check-Point-Software standen noch bevor.

Gegen Ende des Installationsprozesses musste der Dienstleister aufgrund einiger Integrationsprobleme bei Check Point Rat einholen.

Nachdem die Check-Point-Software fertig installiert war, stand den Technikern der Tolly Group eine ihrer Auffassung nach wenig intuitive Benutzeroberfläche zur Verfügung, die mehr einem Microsoft-Visio-Screen, als einer Software für Firewall- und VPN-Funktionen ähnelte.

Im Verlauf des Integrationsvorgangs benötigte Websense über eine Stunde für Installation und Erstkonfiguration. Während des Installationsprozesses konnte man wählen, welche Software integriert werden sollte und welche Appliance im Einsatz war. Unter anderem stand eine Option zur Integration in Check-Point-Software zur Verfügung, was die Arbeit der Techniker vereinfachte. Nachdem Websense installiert war und einige Regeln auf der Check-Point-Lösung erstellt worden waren, war der Integrationsprozess vollendet.

Zum Schluss befasste sich das Technikteam mit der Integration der Trend-Micro-Lösung. Dieser Prozess war wesentlich einfacher, weil die Anbindung weniger umfassend war. Im Fall der Antivirenkomponenten waren etwas mehr als eine Stunde erforderlich, um die benötigten Applikationen zu installieren und konfigurieren. Auf der Client-Ebene kam OfficeScan v5.5 als Antivirenlösung zum Einsatz. Auf der Server-Ebene wurde Server Protect v5.5 als Virenschutz installiert. Die Software muss dabei auf jedem Client-Rechner und auf jedem Server einzeln heruntergeladen und installiert werden. Die Antispam-Software Trend Micro InterScan Messaging Security Suite v5.5 benötigte etwas mehr als eine Stunde für Installation und Konfiguration.

Mit den Einzelkomponenten hatten die Techniker der Tolly Group erhebliche Schwierigkeiten. Bei der integrierten Komplettlösung gab es deutlich weniger Probleme.

Astaro Security Linux ließ sich in 15 Minuten von einer bootfähigen CD-ROM auf eine leere Festplatte spielen. Weitere 20 Minuten waren erforderlich, um die Software in Betrieb zu nehmen und Daten über die Clients laufen zu lassen. Die Bedienungsoberfläche, die Astaro WebAdmin nennt, ist sinnvoll geordnet und über einen HTTPS-verschlüsselten Webzugang erreichbar. Nach erfolgreichem Login stehen für jedes Menü und Untermenü verständliche Informationen zur Verfügung, die durch einfaches Anklicken abrufbar sind. Wer weiterführende Informationen zu bestimmten Funktionen benötigt, steuert ein mit einem Fragezeichen markiertes blaues Kästchen an, das als Popup-Fenster Zusatzinfos bereithält. Weitere Informationen befinden sich in der Online-Hilfe unter **http://docs.astaro.org** sowie in den User Groups unter **www.astaro.org**.

Regelmäßige Administrations- und Supportarbeiten

Im Vergleich von All-In-One Loesungen und Komponentenloesungen stellt der Zeitaufwand fuer die Erstinstallation nur ein Kriterium dar.

Im Testablauf zeigte sich während des gesamten Jahres, dass es in puncto Zeitaufwand bei der Bewältigung der anfallenden Support- und Administrationsaufgaben einen klaren Unterschied zwischen Astaro Security Linux und Juniper Networks bzw. Check Point gibt.

Schaubild 3 zeigt, dass der monatliche Administrationsaufwand bei der integrierten Komplettlösung um 50 Prozent bzw. 62 Prozent niedriger als bei den anderen Lösungspaketen ist.

Ein Blick auf die 16 monatlichen Administrationsarbeiten, die die Techniker der

Tolly Group durchgeführt haben (siehe Anhang B: Supportaufgaben, Ergebnisübersicht), dokumentiert den erhöhten Komplexitätsgrad, den der Einsatz separater Einzelkomponenten nach sich zieht.

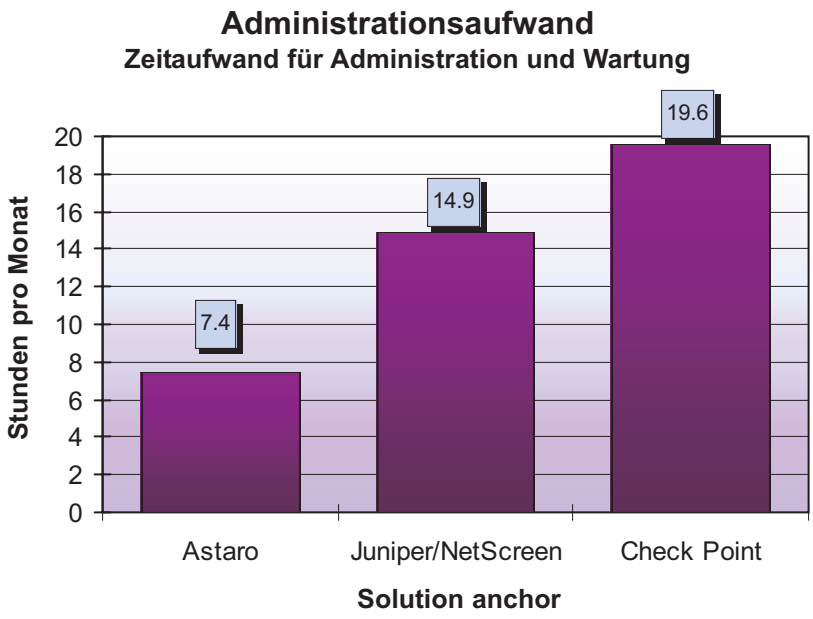
Beispielsweise benötigte die Check-Point-Lösung 33 Prozent mehr Zeitaufwand, um User-Accounts hinzuzufügen, zu verschieben und zu verändern. Das entspricht zwei Stunden Mehrarbeit im Monat oder 24 Stunden jährlich. Sowohl Juniper Networks als auch Astaro Security Linux benötigten 16 Stunden im Jahr zur Bewältigung der gestellten Aufgaben.

Eine der Hauptunterschiede zwischen einer integrierten Komplettlösung und anderen Systemen scheint der Arbeitsaufwand zu sein, der für ein monatliches Backup der gesamten Systemkonfiguration erforderlich ist. Die Datensicherung umfasste neben dem Speichern der Paketfilterregeln auch die Einstellungen des URL-Filters, des Spamschutzes und der Antivirenlösung.

Aufgrund der engen Verzahnung der einzelnen Applikationen in Astaro Security Linux dauerte die Konfiguration eines monatlichen Backups nur zwei Minuten. Die eigentliche Datensicherung lässt sich für alle vier Netze (Hauptsitz und drei Niederlassungen) gleichzeitig durchführen, so dass Astaro die Aufgabe in acht Minuten abgeschlossen hat, was einem Zeitaufwand von 96 Minuten jährlich entspricht.

Im Gegensatz dazu waren bei der Juniper-Networks-Lösung für die Konfiguration des monatlichen Backups 15 Minuten pro Site erforderlich, also 60 Minuten für alle vier Netze, was einem Zeitaufwand von jährlich 720 Minuten entspricht. Der Arbeitsaufwand für die Datensicherung liegt damit sieben mal höher als bei der integrierten Sicherheitslösung.

Schaubild 3. Administrationsaufwand– Zeitaufwand für Administration und



Die Schere geht noch weiter auseinander, wenn man die Ergebnisse der Check-Point-Lösung in Betracht zieht. Hier waren 30 Minuten pro Site erforderlich, also zwei Stunden für das monatliche Backup aller vier Netze. Auf das Jahr gerechnet ergibt sich ein Zeitaufwand von 960 Minuten, ein zehnfach höherer Administrationsaufwand als bei Astaro Security Linux.

Wiederholt zeigte sich, dass die Komplexität durch den Einsatz manuell zu integrierender Produkte deutlich steigt.

Auch vergleichsweise einfache Aufgaben dokumentierten die Unterschiede zwischen der integrierten Komplettlösung und den anderen Systemen, beispielsweise beim Überprüfen der benötigten Software-Patches und Updates. Bei der Astaro-Software war das ein Prozess, der nach fünf Minuten abgeschlossen war und auf alle vier Netze bezogen mit monatlich 20 Minuten zubuche schlug. Astaro-User erhalten automatische Benachrichtigungen für neue Software-Updates.

Bei den Juniper-Networks- und Check-Point-Lösungen verbrauchte diese Aufgabe 30 Minuten pro Site, also zwei Stunden für alle Netze, was einem sechs mal höheren Zeitaufwand im Vergleich zu Astaro entspricht.

Check Point ermöglicht keine automatischen Software-Updates oder automatischen Backups der Konfigurationsdateien. Astaro Security Linux schon. Daraus resultieren bedeutende Kostenunterschiede.

Ein wesentlicher Grund für die unterschiedlichen Ergebnisse bestand darin, dass Check Point keine automatischen Software-Updates oder automatischen Backups der Konfigurationsdateien ermöglicht. Auch Websense sieht die automatische Sicherung der Konfigurationsdaten nicht vor. Außerdem müssen Websense-User alle anderen Dienste einstellen, um ein Backup abzuspeichern oder einzuspielen. Trend Micro ermöglicht automatische Backups der Antispam-Konfiguration ebenfalls nicht.

Darüber hinaus würde es bei einem Serverausfall oder Hardwarefehler mindestens drei Stunden dauern, um Windows neu zu installieren, alle notwendigen Updates einzuspielen, die Einzelkomponenten zu integrieren und die Backupfiles herunterzuladen. Vorausgesetzt der betroffene Anwender hat die Datensicherung regelmäßig manuell durchgeführt.

Mit Astaro Security Linux müssen die Einstellungen des automatischen Backups einmal eingerichtet werden, danach läuft der Prozess von alleine und sichert alle Daten der integrierten Applikationen.

Der Wert der Integration

Das IT-Personal in mittelständischen, aber auch größeren Unternehmen steht der Herausforderung gegenüber, effektive Sicherheitssysteme effizient und harmonisch in das gesamte Unternehmensnetzwerk zu integrieren.

Eine Option besteht darin, die einzelnen Komponenten wie zum Beispiel Firewall, VPN-Gateway, URL-Filter, Antiviren- und Antispam-Lösung separat einzukaufen und zu integrieren.

Die Tolly Group versuchte diesen Ansatz in einem simulierten mittelständischen Unternehmen umzusetzen, setzte dabei auf etablierte Firewall-/VPN-Produkte von Juniper Networks/NetScreen bzw. Check Point und führte alle erforderlichen Integrationsmaßnahmen für das Zusammenspiel mit den Antiviren- und Antispam-Lösungen von Trend Micro Devices sowie dem URL-Filter von Websense durch.

Unser Test der Juniper-Networks- und Check-Point-Systeme zeigte, dass Anwender im ersten Jahr Lehrgeld dafür zahlen, wenn sie separate Produkte in einem Gesamtsystem für mittlere und größere Netze integrieren wollen. Für die Erstinstallation und weiterführende Administrationsarbeiten ist für die Juniper-Networks-Lösung ein doppelt so hoher Aufwand nötig wie für Astaro Security Linux. Die Check-Point-Lösung erfordert 2,5 mal mehr Arbeitsaufwand als Astaro Security Linux.

Lehrgeld ist vor allem fällig, weil sich die Komplexität mit jeder weiteren zu integrierenden Sicherheitslösung erhöht und darüber hinaus der Einsatz von Windows-Betriebssystemen Limitierungen mit sich bringt.

Einige Anwender werden sich fragen, warum die Integration so viel Zeit und Arbeit kostet. Die Antwort ist, dass die Herausforderungen in puncto Komplexität außerordentlich hoch sind, wenn User ihre eigene Sicherheitslösung implementieren wollen. Über einen einzigen Installationsprozess sparen sich Administratoren zum Beispiel die Zeit, die Applikationen einzeln zu installieren, mit allen dafür notwendigen Neustarts und System-Updates.

Eine einheitliche Benutzeroberfläche bedeutet auch, dass das Personal nur einmal angelernt werden muss, wodurch sich der Administrationsaufwand vereinfacht und beschleunigt. Ein einzelner Update-Automatismus einer integrierten Sicherheitslösung ermöglicht das automatische Einspielen von Softwareaktualisierungen ohne weitere Bindung von Mitarbeiterkapazitäten.

Die Tolly Group kommt zu dem Schluss, dass Astaro Security Linux als integrierte Softwarelösung extrem einfach zu installieren und verwalten ist. Das Komplettpaket besteht aus:

- Installations-CD, installierbar in 15 Minuten
- Einheitliche Benutzeroberfläche zur Administration
- Einheitliche Management- und Reporting-Tools
- Integrierter Update-Mechanismus

Die Astaro-Lösung ist extrem kostengünstig, weil sie als eine günstige Firewall-Plattform mit umfassenden Sicherheitsfunktionen und niedrigen Installations- und Administrationskosten ausgeliefert wird.

Aus Anwendersicht benötigt die integrierte Sicherheitslösung ein Drittel der Zeit, die für die Installation der zweitplatzierten Hybridlösung von Juniper Networks anfällt.

Die Testergebnisse fallen in puncto weiterführende Wartungskosten im ersten Jahr eindeutig zugunsten der integrierten Sicherheitslösung aus.

Für eine Auswahl von Administrationsaufgaben benötigte Astaro Security Linux lediglich 71 Stunden im Jahr, Implementierung und zwölf Monate Support eingerechnet.

Im Vergleich dazu waren bei der Juniper-Network-/NetScreen-Lösung 137 Stunden jährlich nötig, um die in zwölf Monaten anfallenden Supportarbeiten zu leisten. Monatlich sind das fast doppelt so hohe Administrationskosten gegenüber der Astaro-Lösung.

Für die untersuchten Aufgaben benötigte die Check-Point-Lösung 184 Stunden pro Jahr (Implementierung und zwölf Monate Support), um alle Aufgaben durchzuführen. Verglichen mit Astaro Security Linux ist also ein 160 Prozent höherer Administrationsaufwand erforderlich.

Abgesehen von den Unterschieden beim Datenmanagement stieß das Technikerteam der Tolly Group bei Juniper Networks/NetScreen und Check Point immer wieder auf Schwierigkeiten, wenn es darum ging, diese Produkte mit den Lösungen von Websense und Trend Micro zu kombinieren.

Besonders störend empfanden die Tolly-Group-Techniker, dass es immer wieder nötig war, die einzelnen Bedienungsoberflächen zu erlernen, Nuancen bei der Software-Integration zu verstehen und mit dem verwirrenden oder fehlenden Dokumentationsmaterial umzugehen.

Systemadministratoren und IT-Manager sollten bei der Umsetzung einer eigenen Sicherheitslösung vorsichtig vorgehen. Selbst wenn sie die separaten Komponenten bei aller Komplexität erfolgreich installieren und integrieren, scheint der dafür erforderliche Arbeitsaufwand angesichts der zwangsläufig entstehenden Kosten deutlich die vermeintlichen Vorteile negativ einzufärben.

Das Technikteam der Tolly Group begegnete keinen Problemen bei der Installation von Astaro Security Linux und den untersuchten Administrationsarbeiten. Das Produkt scheint speziell auf die Bedürfnisse mittelständischer Unternehmen und anderer Organisationen mit engem Personalbudget zurechtgeschnitten zu sein. Astaro hat die Integrationsarbeit komplett übernommen; Anwender installieren die Lösung innerhalb von Minuten und vermeiden die Schwierigkeiten, denen sie bei der Integration separater Komponenten wahrscheinlich begegnen würden.

# # #

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 crested 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 concurently 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 concurently 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 7.37		**3,639** **61 hours**

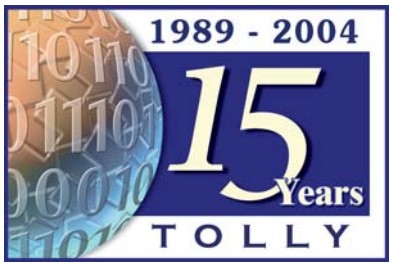
Juniper/Net Screen Solution — Annual Recurring Admin Effort

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 19.58		**8,735** **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

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. sab 22 July 04