

## Security Management

Im Test: Pineapp Mail-Secure 3.60

### Mail-Missbrauch verhüten durch Origin-basierte Anti-Spam-Maßnahmen

15.08.2008 | Autor: Ulrich Roderer

Mit der Mail-Secure bringt Pineapp eine Security-Appliance auf den Markt, die dazu in der Lage ist, den Mail-Verkehr zu überwachen, unliebsame Inhalte auszufiltern, Viren und Malware zu blocken sowie Spam-Übertragungen zu unterbinden. SearchDataCenter.de hat sich angesehen, was das Produkt im praktischen Einsatz leistet.



Die Informationsseite der Pineapp Mail-Secure-Appliance

Die Pineapp Mail-Secure ist eine 19-Zoll-Appliance in einfacher Bauhöhe und verfügt insgesamt über vier Netzwerkschnittstellen. Diese können beim Einsatz im LAN, beim Anschluss an die DMZ und bei WAN-Verbindungen Verwendung finden. Das Produkt kann als Mail-Relay im Unternehmen arbeiten. Im Test richteten wir die Lösung so ein, dass sie als eine Art Mail-Proxy in unserem Netz zum Einsatz kam. Dazu richteten wir ein Port-Forwarding des externen Ports 25 unserer Firewall auf die Appliance ein, damit eingehende Mails bei ihr landeten. Dann teilten wir der Appliance mit, an welchen Mailserver im Netz sie die

geprüften und gefilterten Mails weiterleiten sollte.

Um auch ausgehende Mails zu überwachen, trugen wir die Appliance als SMTP-Server auf unseren Test-Clients ein. Anschließend konnten wir sowohl lokal als auch im Internet Mails senden und empfangen, die alle von der Lösung überprüft wurden.

#### Inbetriebnahme

Nach dem Anschluss der Appliance ans Netz und dem Hochfahren der Lösung müssen die Administratoren einen Konfigurationsclient in das C-Klasse-Subnetz 192.168.24.0 verschieben. Danach sind sie dazu in der Lage, via Browser das Managementinterface der Lösung aufzurufen, das über die URL <https://192.168.24.24:7443> zur Verfügung steht. Der Login erfolgt mit dem Administratorkonto „pineapp“ und dem Passwort „password“. Die Appliance zwingt den IT-Verantwortlichen nicht, nach dem ersten Login das Default-Passwort zu ändern, es findet sich lediglich ein Hinweis im Quick-Start-Guide, dass dieser Schritt sinnvoll wäre.

#### Erstkonfiguration

Zur Erstkonfiguration reicht es, wenn die zuständigen Mitarbeiter unter „Networking/Interfaces“ die Netzwerkkonfiguration mit IP-Adresse, Netzmaske und Gateway an ihre Umgebung anpassen und sich danach über die neue LAN-IP-Adresse der Lösung erneut mit dem Produkt verbinden. Jetzt kommen die Angabe der DNS-Server (unter „Networking/General“) und der Postmaster-Mail-Adresse (in „Mail System/General“) an die Reihe. Anschließend geht es ans Einrichten der ersten Mail-Domäne (über „Mail System/Local Domains“). Im Test entschieden wir uns, eine SMTP-Domäne zu erstellen und als Delivery Server den Mail-Server in unserem LAN zu verwenden. Alternativ besteht auch die Möglichkeit, POP-Domänen zu generieren, in diesem Fall geben die Verantwortlichen noch eine Mailbox und einen Login-Namen an.

Nach dem Einrichten der Domäne ist ein Zugriff auf „Mail System/Relay Networks“ erforderlich, um der Appliance mitzuteilen, welche Netzwerkadressen im lokalen Netz Mails verschicken dürfen und wie die IP-Adresse des lokalen Mailservers lautet. Eine

manuelle Aktualisierung der Antivirus-Patterns im „Antivirus“-Menü schließt die Mail-Konfiguration ab. Standardmäßig arbeitet die Lösung danach mit zwei Mail-Regeln, die die Übertragungen ausführbarer Dateien via Mail verhindern und die Spam-Mails mit einem Score von sechs blockieren.

Zur Anti-Spam-Einstellungen empfiehlt der Hersteller im Betrieb nicht nur die content-basierten Antispam-Module zu aktivieren, sondern auch die Commtouch-RPD-Technologie. Diese verwendet eine „Recurrent-Pattern-Detection“ (RPD), die eingehende Mails mit einer Datenbank abgleicht, die das Commtouch Detection Center durch eine Echtzeitüberwachung des Internetverkehrs auf dem neuesten Stand hält.

RPD arbeitet unabhängig von der Sprache der Mails. Ebenfalls empfohlen: Die Zero-Hour-Virus-Protection, die Heuristic Engine und Pineapps ZDS. Die heuristische Engine verwendet auch einen Bayes-Filter und das ZDS (Zombie Detection System) überprüft die Senderadressen in Echtzeit dahingehend, ob es sich um bekannte Zombieadressen handelt, die bereits eine Reputation als Spam-Schleuder haben. Dazu gleicht es die Senderinformationen mit einer Datenbank des Herstellers ab.

Damit die Appliance richtig arbeitet, müssen zudem noch folgende Ports in der Firewall offen stehen: 25 (SMTP) ein- und ausgehend, 53 (DNS) und 80 (HTTP) ausgehend und optional für Servicezugriffe durch den Hersteller eingehend 7022 (via SSH) und 7443 (via SSL). Damit ist die Initialkonfiguration abgeschlossen und das Produkt nimmt seine Arbeit auf.

#### **Konfiguration**

Wenn sich ein Administrator im laufenden Betrieb beim Konfigurationsinterface anmeldet, so landet er in einem Administrationswerkzeug, das auf den ersten Blick etwas gewöhnungsbedürftig ist. Üblicherweise arbeiten solche Tools heutzutage mit einer Menüstruktur auf der linken Seite, die eine explorer-ähnliche Baumstruktur verwendet oder in Untermenüs verzweigt. Eine Menüleiste gibt es bei der Pineapp-Appliance auch, die Untermenüpunkte befinden sich aber jeweils am oberen Fensterrand.

Das erscheint zunächst etwas gewöhnungsbedürftig, stört aber nach einiger Zeit nicht mehr. Abgesehen davon befinden sich oben, außerhalb des Menüs noch zwei Konfigurationsoptionen die man nicht übersehen sollte. Diese dienen zum Einstellen der Sprache (Chinesisch, Englisch, Französisch, Portugiesisch, Russisch, Spanisch) und zum Festlegen der Zahl der Einträge, die das Werkzeug auf einer Seite präsentieren soll (beispielsweise bei Log-Listen).

Standardmäßig zeigt das Produkt nach der Anmeldung eine Übersichtsseite, die Informationen über die Lizenz, die Software-Version, die Seriennummer, die Version der Antivirus-Datenbank und ähnliches präsentiert. Außerdem liefert sie Details zur Netzwerklast (mit empfangenden und gesendeten Daten in MByte), Daten zu Uptime und Systemlast sowie den Hostnamen, die aktuelle CPU-Temperatur, die Disk-Auslastung, die Größen der Mail-Warteschlangen und den Status der Mail-beziehungsweise Antispam-Dienste.

Die nächsten Bereiche wurden relativ übersichtlich gehalten: Das „Licensing“ zeigt an, wie lang die aktuelle Lizenz noch Gültigkeit besitzt. Außerdem lässt es das Eintragen einer neuen Lizenz zu. Das Benutzermanagement ermöglicht nicht nur das Ändern des Passworts des Administrationskontos, sondern dient auch zum Anlegen neuer Benutzer,

die ihrerseits auf die Appliance zugreifen können (dazu später mehr).

Es ist sogar möglich festzulegen, ob die User einen Daily-E-Mail-Report erhalten sollen und die Benutzerkonten mit einem LDAP-Server zu synchronisieren. Letzteres stellte im Test kein Problem dar. Die LDAP-Konnektoren arbeiten mit CommuniGate 5, Exchange 5.5, Iplanet, Lotus Notes, Novell, OpenLDAP, Windows 2000 und Windows Server 2003 zusammen.

Ansonsten umfasst die Systemkonfiguration noch eine Option zum Generieren eines SSL-Zertifikats, die Zeitonenkonfiguration mit NTP-Servern und einen Dialog zum Durchführen von Software-Updates. Dazu kommen Befehle zum Konfigurationsmanagement, eine Funktion zum Sichern der Konfiguration und der Mailboxes über einen Scheduler und eine Monitoring-Seite, die auch Alerts enthält.

Auf der genannten Seite überwachen die zuständigen Mitarbeiter den Prozessorlüfter, die CPU-Temperatur, die Systemtemperatur und die Temperatur des Boards. Außerdem aktivieren sie SNMP, laden die MIB der Appliance auf ihren Client herunter und richten eine Syslog-Funktion auf einen zentralen Server ein. Einstellungen zum remote Access mit zur Verwaltung zugelassenen Management-IP-Adressen, über SSH oder via externes Modem schließen die Systemkonfiguration gemeinsam mit einer Syslog-Ansicht und Befehlen zum Neustart und zum Herunterfahren ab.

#### **Netzwerk konfigurieren**

Im Netzwerkbereich konfigurieren die zuständigen Mitarbeiter nicht nur die Netzwerkeinstellungen der vier Interfaces, sondern legen auch die Ports für die Dienste HTTP, HTTPS, SSH sowie für einen HTTP-Proxy fest. Darüber hinaus definieren sie bei Bedarf statische Routen und geben die Parameter für statische NAT, Portforwarding und Masquerading an.

Das ist beispielsweise sinnvoll, wenn das Produkt in einer Gateway-Konfiguration zum Einsatz kommt. Eine Übersichtsseite zeigt stets die Routing- und ARP-Tabellen sowie den aktuellen Status der einzelnen Netzwerkinterfaces. Zum Prüfen der Verbindung zu bestimmten Sites steht eine Ping-Funktion bereit. Da sich das Mail-Relay auch in Hochverfügbarkeitskonfigurationen nutzen lässt, findet sich bei den Netzwerkeinstellungen ein Cluster-Management-Dialog, der zudem das Setzen von Load-Balancing-Einstellungen ermöglicht.

Da die Mail-Secure OPSEC-zertifiziert wurde, kann sie außerdem mit der Checkpoint Firewall-1 kommunizieren und dieser IP-Reputationsdienste zur Verfügung stellen.

Von größerem Interesse ist die Konfiguration des Mail-Systems. Hier gibt es zunächst die Option, SMTP-Authentifizierung und SMTP über TLS zu aktivieren sowie den Nachrichteneingang zu sperren, wenn in der Scanning-Mail-Queue mehr als 1000 Nachrichten hängen. Ansonsten gehören noch folgende Punkte zu den allgemeinen Settings des Mail-Systems: Einstellungen zu Benachrichtigungen (für den Sender oder den Empfänger verdächtiger Mails beziehungsweise den Administrator), der Umgang mit Bounces, die Mail-Adresse des Postmasters, die Service-Banner, ein Forwarding-Host und Größenbeschränkungen für Nachrichten.

Mit der Domain-to-Host- beziehungsweise der Address-to-Host-Conversion haben die Administratoren die Option, das System so zu konfigurieren, dass es verschiedene Mails abhängig von ihren Domänen oder Adressen an unterschiedliche Server weiterleitet. Abgesehen davon existiert auch die Möglichkeit, Mail-Retriever einzurichten, die Mails in bestimmten Intervallen von POP-Servern abholen und an definierte Zieladressen

weiterleiten.

Das so genannte POP-Scanning kommt zum Einsatz, wenn Administratoren die Appliance als transparenten POP-Proxy nutzen möchten. Diese Feature steht nur zur Verfügung, wenn die Lösung im Gateway-Modus arbeitet. Eine Backscatter-Protection bekämpft illegitime Bounce-Back-Nachrichten, hier sind die zuständigen Mitarbeiter dazu in der Lage, vertrauenswürdige SMTP-IP-Adressen anzugeben. Die POP3-Access-List realisiert schließlich eine Zugriffsbeschränkung auf den POP-Dienst des Produkts.

Die restlichen Bereiche der Mailkonfiguration sind schnell beschrieben: Eine Queue-Information mit Suchfunktion, sorgt dafür, dass die Administratoren über die Aktionen des Systems auf dem Laufenden bleiben. Diverse Logs geben Aufschluss über Mailauslieferungen sowie den SMTP-, den POP- und den IMAP-Verkehr. Eine Masquerading-Funktion sorgt im Gegensatz dazu bei Bedarf dafür, dass die Mail-Adresse eines Benutzers für diesen anders präsentiert wird, als es in Wirklichkeit der Fall ist.

Auf diese Weise lassen sich unter anderem Mails die an {testuser@firma.com} adressiert wurden so darstellen, als seien sie an {testuser@firma.de} gerichtet gewesen. Über die erweiterten Einstellungen legen die Administratoren schließlich die maximale Zahl der gleichzeitigen Verbindungen, den Timeout, die Lebensdauer der Nachrichten, die Zahl der erlaubten SMTP-Authentifizierungsversuche pro Benutzer und ähnliches fest.

#### **Regeln**

Der Umgang der Appliance mit den Mails wird über Regeln festgelegt. Die diesbezügliche Policy-Konfiguration stellt demzufolge das Herzstück der Lösung dar. Standardmäßig arbeitet das Produkt mit den beiden bereits erwähnten Regeln, die ausführbare Dateien in Mails und Spam ab der Scoring-Stufe sechs unterdrücken. Die IT-Mitarbeiter können aber noch eine Vielzahl anderer Regeln angeben, unter anderem auch Content-Regeln, die den Mailinhalt auf unerwünschte Inhalte untersuchen.

Diverse allgemeine Einstellungen in diesem Bereich sorgen auf Wunsch dafür, dass die Appliance Viren direkt löscht, statt die infizierten Mails in Quarantäne zu verschieben. Außerdem geben die Administratoren hier an, wie die Lösung Mails behandeln soll, die an nicht existierende Benutzerkonten gerichtet sind (Auto-Quarantäne, Auto-Delete etc.). „Default Permissions“ regelt, welche Rechte neue Benutzer auf dem System bekommen (Personal Spam Manager, Network Manager, Read Only und so weiter - damit haben die Verantwortlichen die Option, die Permissions der einzelnen Accounts genau an ihre jeweiligen Anforderungen anzupassen).

Von besonderem Interesse ist in diesem Zusammenhang eine Funktion namens „Maximum non-existing recipients allowed within a message before blocking it entirely“. Diese blockiert alle Nachrichten, bei denen mehrere Empfängerkonten (beispielsweise 50 Prozent), im Unternehmen nicht existieren. Damit bekämpft die Appliance Spammer, die blind nach irgendwelchen Mail-Konten in der Unternehmensdomäne suchen. Bei denen ist es höchstwahrscheinlich, dass mehr als 50 Prozent der von ihnen angegebenen Empfänger nicht existieren, während legitime Versender wohl niemals so viele Fehler machen werden.

Die Policy-Definition selbst funktioniert über die Richtung, der Absenderadresse oder Maske, bei Spam-Regeln dem maximalen und minimalen Spam-Score, den zu blockenden Kategorien, der Weiterleitung und der Benachrichtigung, die das System bei Bedarf an den Sender, den Empfänger oder den Administrator schickt, wenn die Regel

greift. Dazu kommt dann noch die auszuführende Aktion: Delete, Block, Park oder Allow. Alle Regeln lassen sich global, auf Gruppenbasis oder für spezifische Anwender definieren. Damit hat der Administrator ein sehr mächtiges Werkzeug in der Hand, mit dem er von Weiterleitungen, über Attachment-Regeln bis hin zur Spam-Bekämpfung alle Mail-Transaktionen in seinem Umfeld granular beeinflussen kann. Im Test konnte diese Funktionalität voll überzeugen.

#### **Mail-Traffic-Management**

Das Mail-Traffic-Management bietet den Verantwortlichen die Option, Mails geordnet nach Richtung, Sender etc. anzuzeigen und Details über Source-IP-Adressen, gefundene Viren, den Spam-Score und ähnliches einzusehen. Das Zone Management übernimmt im Gegensatz dazu die Definition von Park-Zonen und der Quarantäne. Hier legen die Administratoren beispielsweise fest, wie viele Tage eine Mail in der Quarantäne vorzuhalten ist.

Zum Verwenden von Dateitypen in Regeln, beispielsweise zum Ausfiltern bestimmter Mail-Anlagen, lassen sich die einzelnen File-Types in Gruppen zusammenfassen, wie „Graphic“, „Music and Sound“, „Executables“ und so weiter. Das verbessert die Übersicht deutlich. An gleicher Stelle ist es auch möglich, Dateitypen zu definieren.

Das Content Filtering, das wir bereits angesprochen haben, lässt sich ebenfalls flexibel konfigurieren. Dabei haben die Administratoren die Option, bestimmte Wörter zu Kategorien hinzuzufügen, neue Regel anzulegen und so weiter. Alle Kategorien müssen innerhalb der Content-Filter-Definition aktiviert werden, sonst stehen sie bei der Regeldefinition nicht zur Verfügung.

Im Test fiel auf, dass es zwar Kategorien wie Badwords für Dutch, French und Italian sowie einen Eintrag für russische Pornographie gibt, mit deutschen Inhalten geizt der Hersteller bedauerlicherweise aber.

Die weiteren Punkte der Policy-Definition helfen den zuständigen Mitarbeitern beim Anlegen von Footnotes, die das System den ein- und ausgehenden Nachrichten automatisch anhängt, beim Einsehen der Scanning-Warteschlange und beim Einrichten der Vorlagen für Benachrichtigungen für Sender, Empfänger und Administratoren.

Bei der Template-Definition stehen den Verantwortlichen auch Schlüsselwörter wie `_REASON_` und `_ACTION_` zur Verfügung, die genau wie Variablen zum Einsatz kommen. Eine Definition könnte also so aussehen:

**Der Grund für das Abblocken Ihrer Mail lautet: `_REASON_`**

Zum Bekämpfen von Viren setzt die Pineapp-Appliance auf die Antivirussysteme von F-Secure und Kaspersky. Die Update-Frequenz liegt standardmäßig bei 30 Minuten, das lässt sich aber über das Konfigurationswerkzeug genauso ändern wie das Scan-Zeitlimit pro Datei.

Was die Konfiguration der Anti-Spam-Funktionen angeht, so lassen sich für diese Aufgabe diverse Methoden nutzen. Dazu gehören neben dem Spam-Scoring-Feature, auf das wir bereits im Rahmen der Policy-Definition eingegangen sind, und den im Rahmen der Initialkonfiguration beschriebenen Vorgehensweisen eine Spoofing-Protection, eine Überprüfung der Absenderdomäne, die Treat Commtouch RPD Bulk Classification und das Pineapp Nextgen Greylisting.

Letzteres weist Mails von einer unbekanntenen IP-Adresse mit einer „Try Again“-Meldung

zurück. Spammer werden in so einem Fall kaum versuchen, ihre Nachricht nochmal zu schicken, die meisten „normalen“ Mailserver schon. Dazu kommt noch das Commtouch IP Reputation System, das Spam von Zombies bereits auf SMTP-Ebene blockt.

Eine weitere interessante Anti-Spam-Maßnahme ist das Anti-Zombie-Fake-SMTP-Banner-Delay. Dieses Feature macht sich zu Nutze, dass die meisten Spammer nur dann Verbindungen zu Mail-Hosts aufbauen, wenn diese innerhalb kürzester Zeit antworten. Das SMTP-Banner-Delay verzögert die Host-Antworten so, dass ein Großteil der Spam-Versender abspringen, während normale Mail-Übertragungen erhalten bleiben.

Es ist optional sogar möglich, auch bei trusted IP-Adressen IP-Checks durchzuführen, alle externen Empfänger automatisch zur White-List des jeweiligen Absenders hinzuzufügen, identifizierten Spam als Attachment weiterzuleiten und ankommende Mail auch dann durch die Spam-Filter laufen zu lassen, wenn der transparente POP3-Proxy Verwendung findet. Darüber hinaus richten die Administratoren in der Anti-Spam-Konfiguration den Tagging-String ein, mit dem das System spam-verdächtige Nachrichten im Betreff kennzeichnen kann und aktivieren einen bei Bedarf einen Report für jede Spam-Mail.

Außerdem arbeitet die Appliance auf Wunsch auch mit Realtime Blackhole Lists (RBLs) und Back- sowie White-Lists. Bei den RBLs wurden standardmäßig bl.spamcop.net und sbl-xbl.spamhaus.org aktiviert. Ein täglicher Report ist schließlich dazu in der Lage, die Anwender über die von der Appliance durchgeführten Aktionen zu informieren, den Verkehr anzuzeigen und den Nutzern zu ermöglichen, Mails aus der Quarantäne zu entlassen. Der Report steht auf Chinesisch, Englisch, Französisch, Hebräisch, Italienisch, Portugiesisch, Russisch und Spanisch bereit. Es ist sogar möglich, ein eigenes Logo auf die Appliance hochzuladen und in den Report einzubinden.

## Statistiken und Reports

Der letzte Funktionsbereich, den wir bisher noch nicht erwähnt haben, umfasst die Statistiken und Reports. Hier stehen Übersichten in Form von diversen Grafiken für den gesamten Mail-Verkehr, für die SMTP-Verbindungen, für die Content Analyse und für aus- und eingehende Daten bereit. Spezielle Reports lassen sich für weitergeleitete, zurückgewiesene und ähnliche Mails sowie für SMTP-Connections und Mails im Allgemeinen erzeugen.

Abgesehen davon bietet das Produkt noch Benutzerreports und Domänenreports, die Aufschluss über saubere und virenverseuchte Mails beziehungsweise Spam und Vergleichbares auf User- und Domänebene geben. Diese Reports sind auch ins CSV-Format exportierbar, die zuständigen Mitarbeiter können sie folglich jederzeit in anderen Anwendungen weiterbenutzen. Statistiken in Listenform gehören ebenfalls zum Funktionsumfang der Appliance. Sie informieren in numerischer Form über die aus- und eingehenden Verbindungen, die blockierten Mails, die gefundenen Viren und ähnliches.

Die Statistik liefert zudem Durchschnittswerte wie Verkehr pro Minute, Stunde oder Tag. Eine Top-Liste mit den Top-Sendern sowie den Top-Empfängern von Viren, Spam und ähnlichem auf Benutzer- und Domänenebene rundet den Leistungsumfang der Appliance ab.

## Benutzerzugriffe

Wenn sich ein Benutzer mit Default-Rechten bei der Appliance anmeldet, so kann er ebenfalls mit dem Web-Interface arbeiten. In diesem Fall hat er Gelegenheit, seine

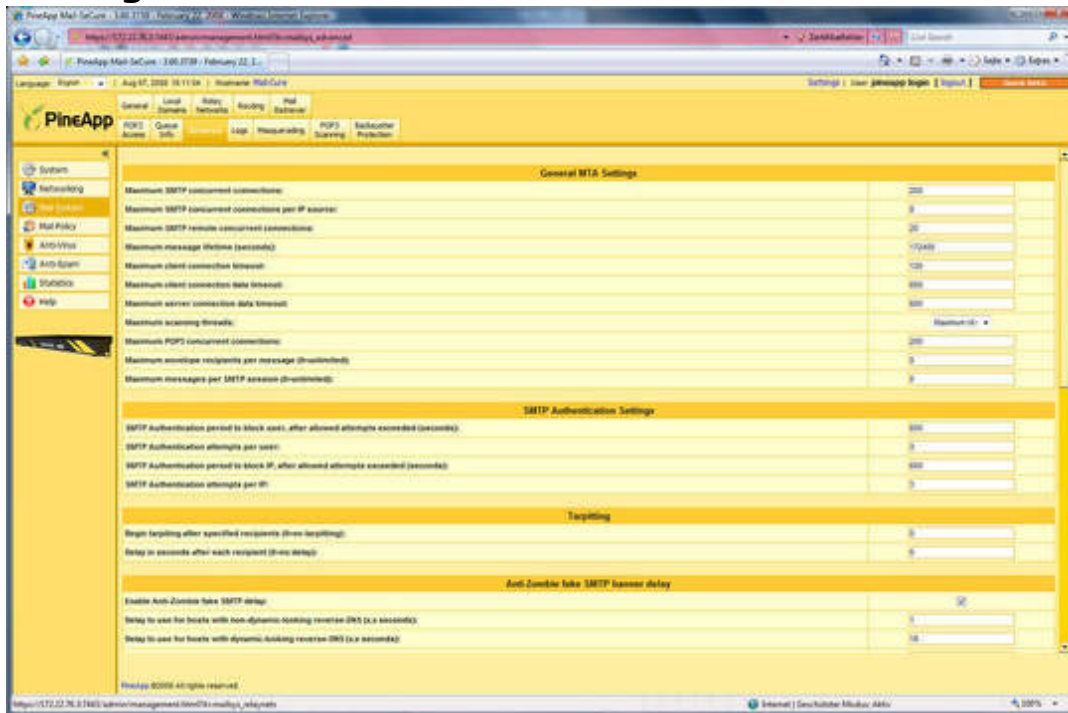
user-spezifischen Regeln zu modifizieren und eigene Black- und White-Lists zu verwalten.

#### **Der Test**

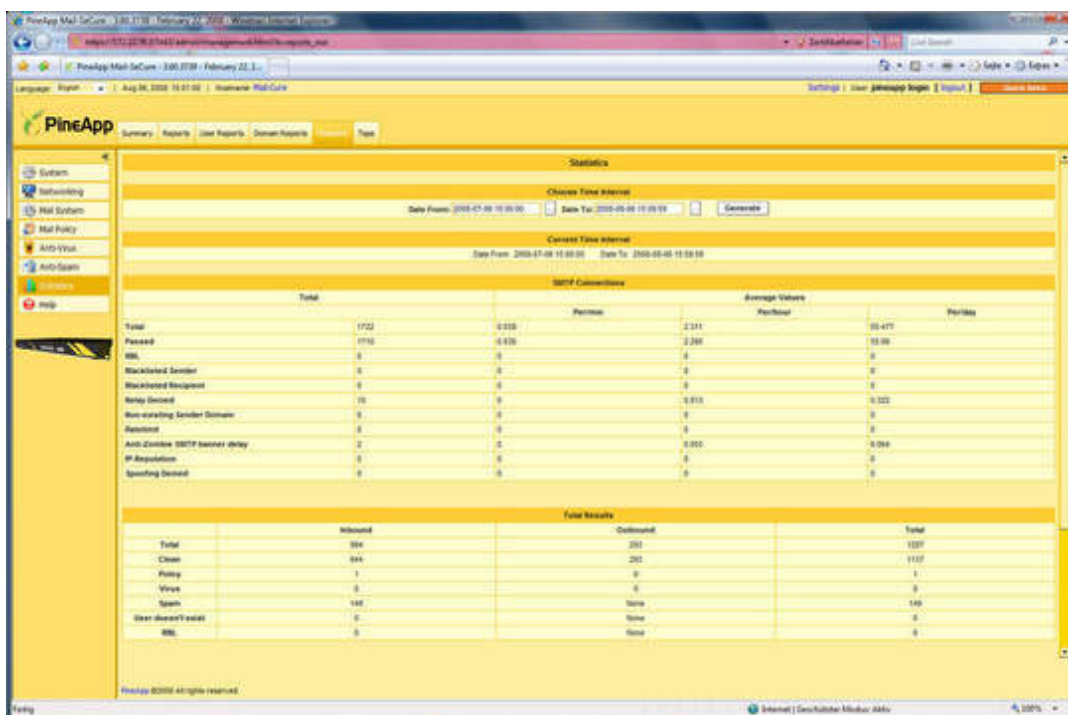
Das Spam-Filtering mit der Mail-Secure erfolgt nach Angaben des Herstellers zu 80 bis 90 Prozent durch die Analyse der Absenderadressen, also nur zum Teil über Content-Scans. Folglich erhält man im Test kein objektives Ergebnis, wenn man im Testlabor eine definierte Menge an Ham- und Spam-Nachrichten durch die Appliance schickt. Da alle Mails in diesem Fall vom gleichen Absender kommen, bleibt die wichtigste Anti-Spam-Maßnahme der Pineapp-Lösung im Laborumfeld außen vor. In einem solchen Szenario erreichten wir eine Erkennungsrate von lediglich 60 Prozent. Deswegen ist es nur sinnvoll, die Lösung in Umgebungen einzusetzen, in denen die Spam-Mails - wie in der wirklichen Welt - von unterschiedlichen Absendern stammen. Dabei kamen wir zu folgendem Ergebnis: Im Testzeitraum erhielt unser Test-Account etwas mehr als 3000 Mails, davon waren knapp 2500 Spam-Nachrichten. Von diesen Spam-Mails erkannte die Appliance mehr als 98 Prozent bei Null False Positives, was sich auch mit den Aussagen des Herstellers deckt, der 98 bis 99 Prozent Erkennungsquote bewirbt. Damit wird klar, dass Origin-basierte Anti-Spam-Maßnahmen in der Praxis wirklich sinnvolle Ergebnisse bringen. Auch die restlichen Funktionen des Produkts, mit den Content-Filtering-Rules, der Anti-Virus-Engine und den Reports konnte im Test durchaus überzeugen. Das gleiche gilt für die Online-Hilfe. Damit handelt es sich bei Pineapps Mail-Secure um eine durchaus empfehlenswerte Lösung mit guten Leistungswerten. Das zu Anfang ungewohnte Aussehen des Administrationswerkzeugs sollte also niemanden abschrecken.

Die Beiträge auf dieser Website sind urheberrechtlich geschützt. Bei Fragen zu den Nutzungsrechten wenden Sie sich bitte an manuela\_maurer@vogel-medien.de oder Tel.: 0931-418-2888.

## Bildergalerie

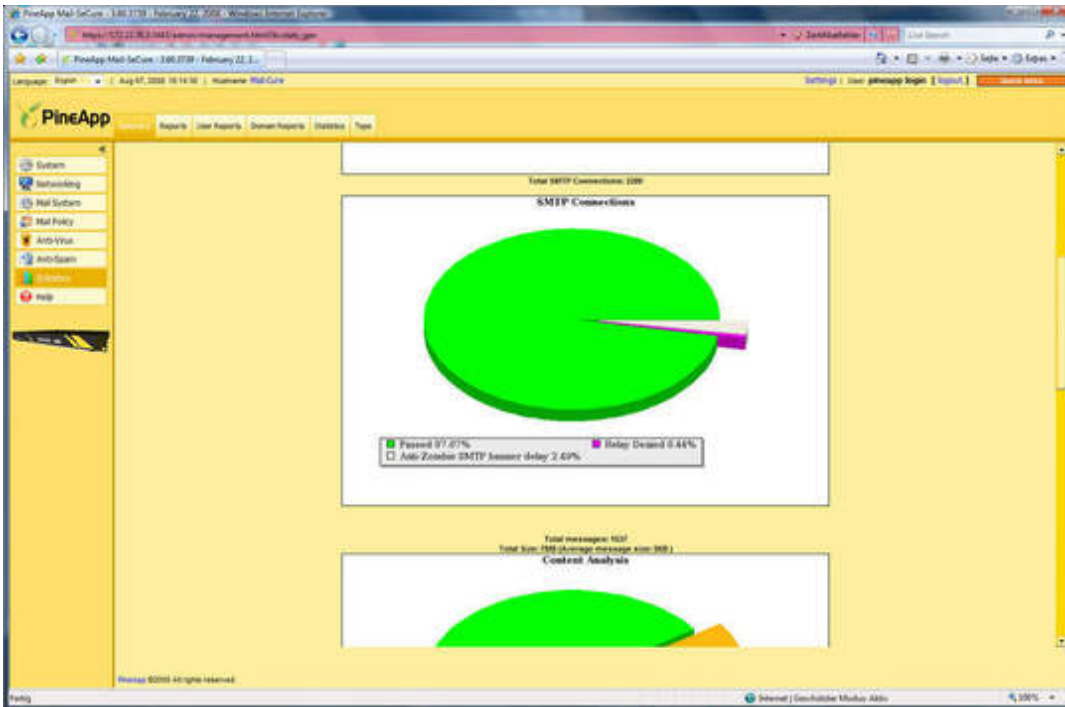


In den erweiterten Einstellungen zum Mail-System haben die Verantwortlichen Gelegenheit, den SMTP-Verkehr genau zu beeinflussen



Umfassende Statistiken geben Aufschluss darüber, welcher Verkehr über die Appliance gelaufen ist





Übersichtliche Grafiken geben Aufschluss über die Aktionen des Systems

Dieses PDF wurde Ihnen bereitgestellt von <http://www.searchdatacenter.de>