Secure Messaging: Fortimail gegen Spam

Technopark – Amrein Engineering

8. April 2005

Die Einflüsse von Spam

- Produktivität
  - Mitarbeiter verbringen Zeit mit dem Lesen und Löschen von Spam
  - Die Häufung von Spam bringt längere Verzögerungen
- Unnötiger Resourcenverbrauch
  - Email Serverresourcen werden von Spam verbraucht
    - Diskspace, Email-Transfer Zeiten,..
- Spam verbraucht Bandbreite
  - Beeinflussung von Business kritischen Applikationen wie VoIP oder Video conferencing
- Nutzung als Threat Delivery System
  - Viruses, Würmer, Trojaner und vermehrt Spyware/Adware
  - Neu: Social Engineering wie Phishing (CityBank,…)

Spam ist nicht mehr nur ein Ärgernis, es ist ein gefährlicher Mechanismus mit vermehrt finanziellen Hintergründen

Wachstum und Kosten von Spam

- Spam beeinflusst den Unternehmensgewinn
  - Verlorene Produktivität pro Mitarbeiter 3000 SFr. pro Jahr
    - Source: Nucleus Research
- Spamverkehr wächst
  - Über 17 Milliarden Spam werden jeden Tag versendet
  - Erwartetes Wachstum: bis zu 23 Milliarden bis 2007
    - Source IDC
- Veränderung der Absichten
  - Bis zu 30% aller Spam Nachrichten enthalten eine Form von Viren oder Spyware
  - Attacken müssen neu bewertet werden. Waren sie zuvor einfach lästig, bekommen Sie heute eine klare finanzielle Komponente

Spam Detection Methoden

Inhaltsanalyse (Content Level Detection)

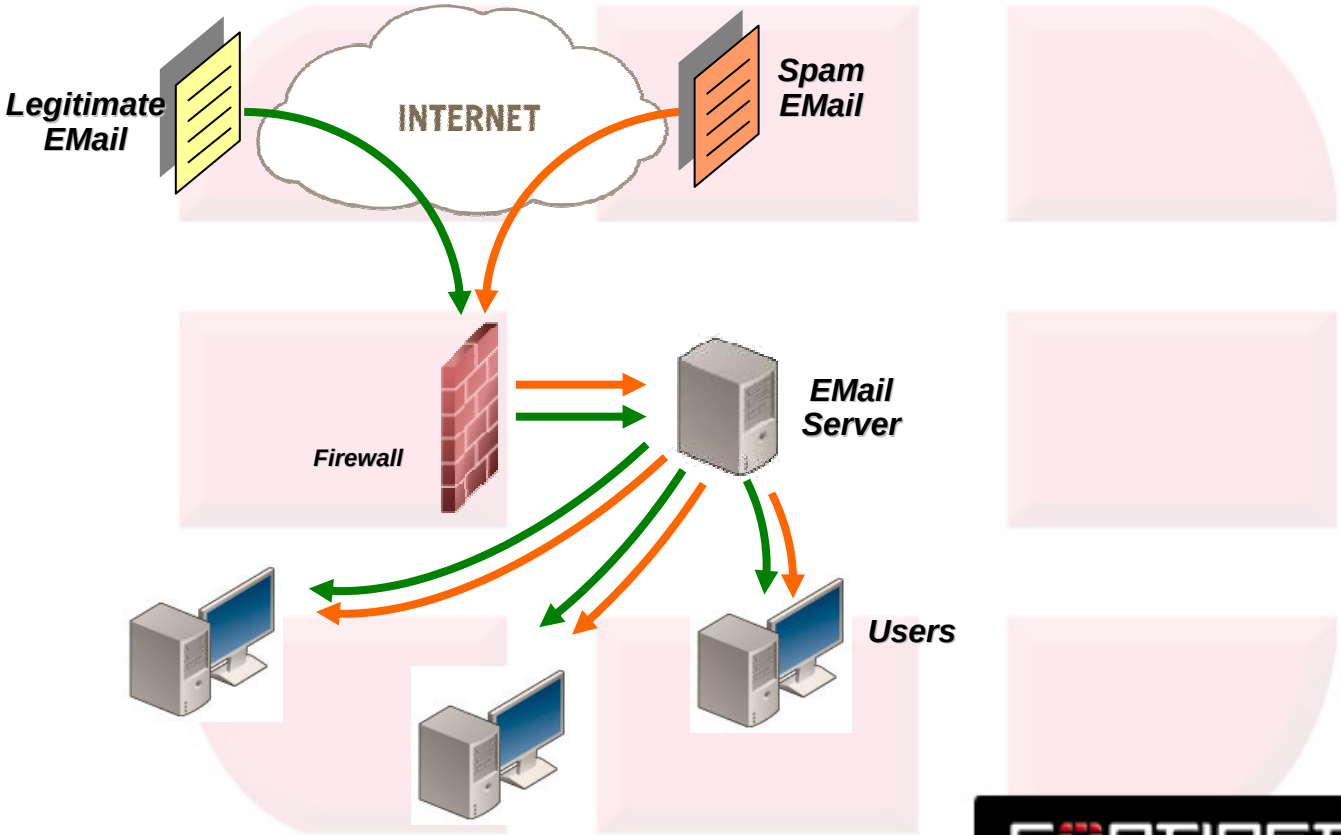
- Black/White Listen, Schlüsselwort Erkennung
- Bayesische Filter
  - Verwenden von Wörtern und Mustern zur Erkennung von Spam, Hier die Mitarbeit der Benutzer von zentraler Bedeutung
- Distributed Checksum Clearinghouse (DCC)

Verbindungsanalyse (Connection Level Detection)

- Black/White Listen, Automatische White Listen, Reverse DNS Lookup
- Real-time Blackhole Lists/Open Relay Database (RBL/ORDB)
- Sender Verifizierung
  - Hierbei wird beim Mailserver das Vorhandensein des Senders verifiziert
- Gray Listing
  - Das erste Mail wird verzögert und erst mit den nachfolgenden Emails nachgereicht
- Spam Probe
  - Sammeln aller relevanten Informationen, die der Spammer mitgibt

PC basierende AntiSpam Lösungen

- AntiSpam Tool wird auf dem PC mit dem Email Client installiert
- Benutzer erhält komplete Kontrolle über die Klassifizierung der Spam
- Erweiterungen sind nur schwerlich möglich. Hoher Wartungsaufwand
- Hoher Resourcenaufwand seitens Bandbreiten, Emailresourcen (CPU, storage,..)
- Geeignet nur im persönlichen oder kleinen Umfeld



Email Server basierende AntiSpam Lösungen

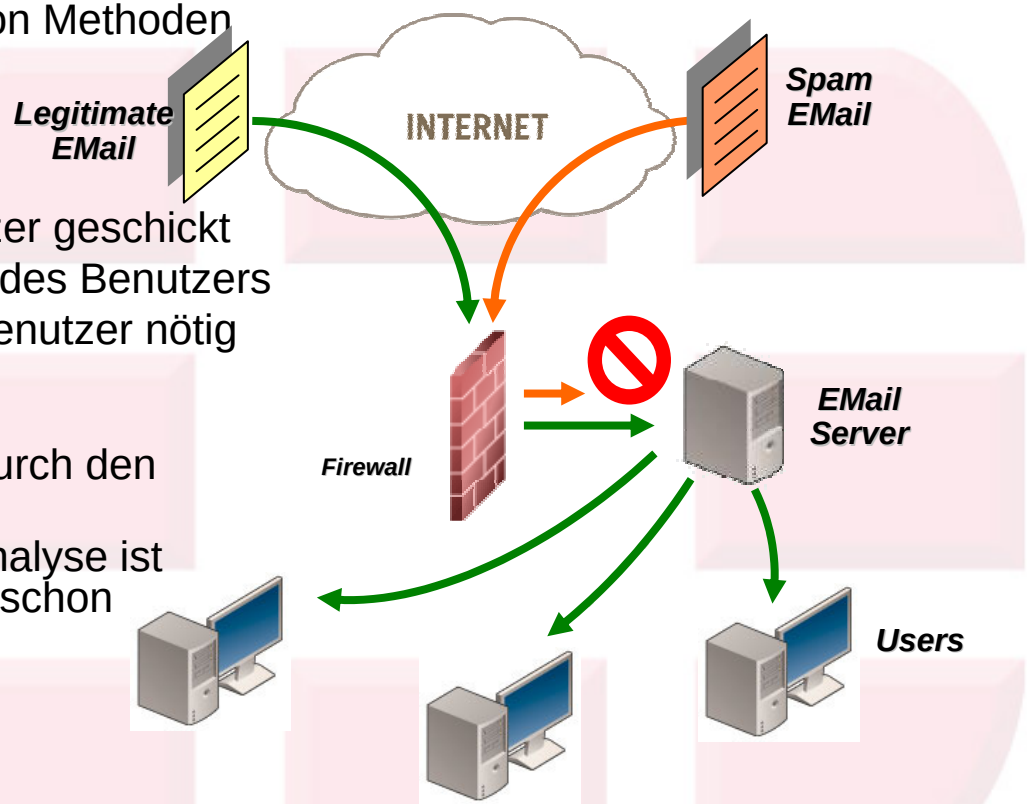
- Werden auf den Email Servern installiert und analysieren die Email sobald diese ankommen.
- Benötigt erheblichen Rechenaufwand auf dem Email Server
- Üblicherweise Content Detection Methoden

Vorteile:

- Spam wird nicht an den Benutzer geschickt
- Spart Bandbreite auf der Seite des Benutzers
- Es ist keine Installation beim Benutzer nötig

Nachteile:

- Internet link wird immer noch durch den Transfer der Spam verstopft
- Verbindungsorientierte Spamanalyse ist nicht mehr möglich, weil Spam schon angekommen ist



Gateway basierende AntiSpam Lösung

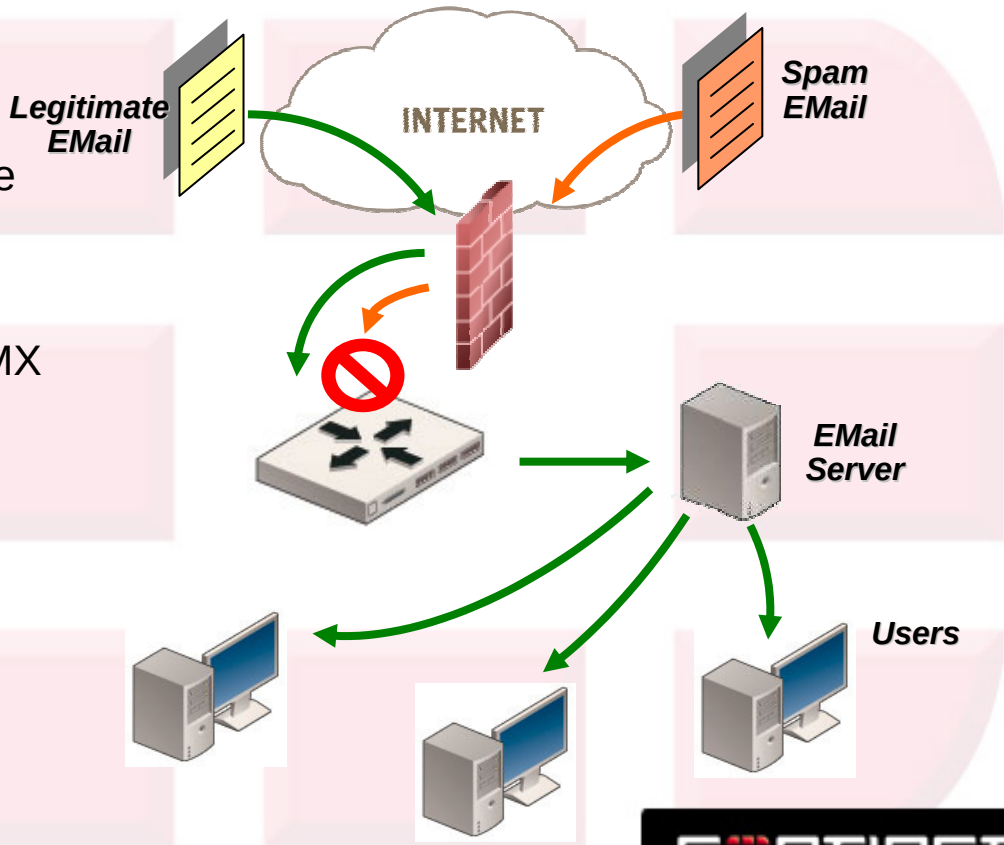
- Die Installation geschieht im Internet Gateway Bereich und agiert als Mail Proxy
- Spam wird am Eintrittspunkt ins Firmennetzwerk identifiziert und entfernt Spam. Nur “gute” Emails werden weitergereicht.
- Antivirenschutz möglich, dies erhöht den Sicherheitslevel
- Es können alle bekannten Methoden der Spam Erkennung eingesetzt werden.

Vorteile:

- Entfernen von Spam optimiert die Bandbreite intern
- Schützt Emailserver Resourcen, Serverupgrades sind nicht nötig
- Einfache Konfiguration: DNS & MX record Modifikationen

Nachteile:

- AntiSpam Gerät kann zu einem Flaschenhals werden (SPOF)
- Kosten können die anderer Lösungen übertreffen



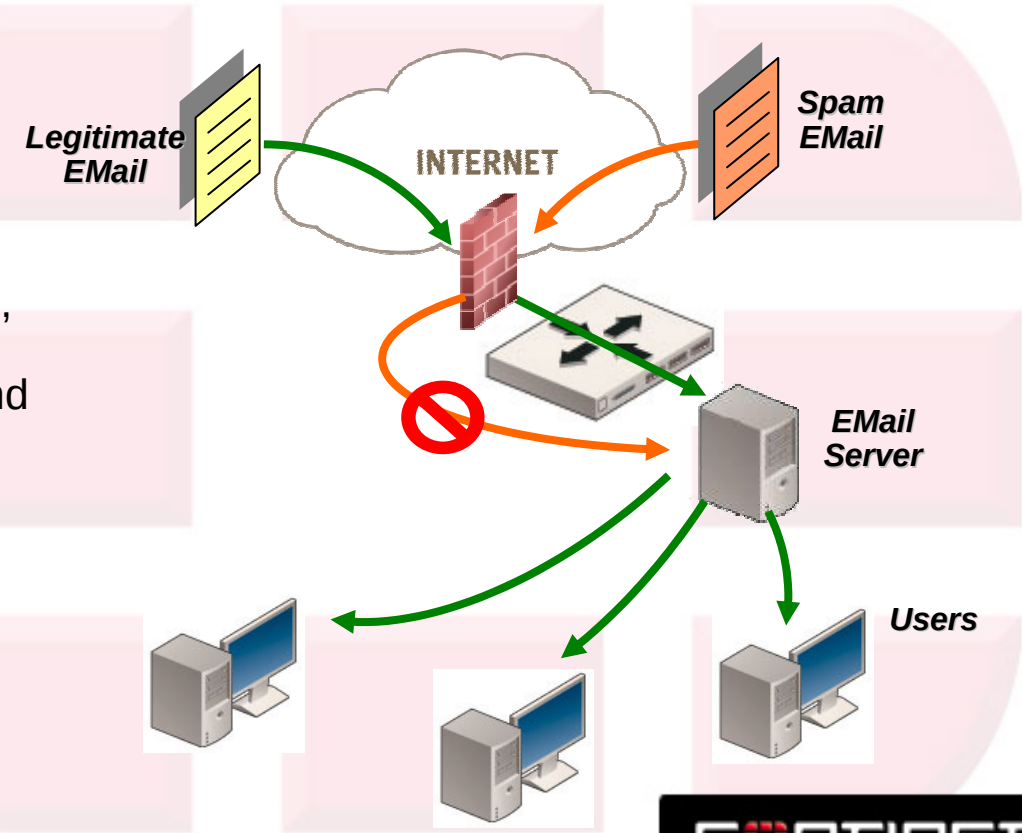
Einzigartig : Transparente AntiSpam Lösung

- Die Installation geschieht vor dem Mailserver
- Der Administrator muss keine IP Adressranges oder MX&DNS Einträge verändern
- Spam wird vor dem Mailserver identifiziert und entfernt. Nur “gute” Emails werden weitergereicht.
- Antivirenschutz zusammen mit Spam Erkennung erhöht den Sicherheitslevel
- Es können alle bekannten Methoden der Spam Erkennung eingesetzt werden.

Vorteile:

- Das IP Konzept wird in keiner Weise tangiert.
- Schützt Emailserver Resourcen, Serverupgrades sind nicht nötig
- Einfachste Konfiguration: Es sind keinerlei Modifikationen am bestehenden Netzwerk nötig

Nachteile:



MSSP basierende AntiSpam Lösung

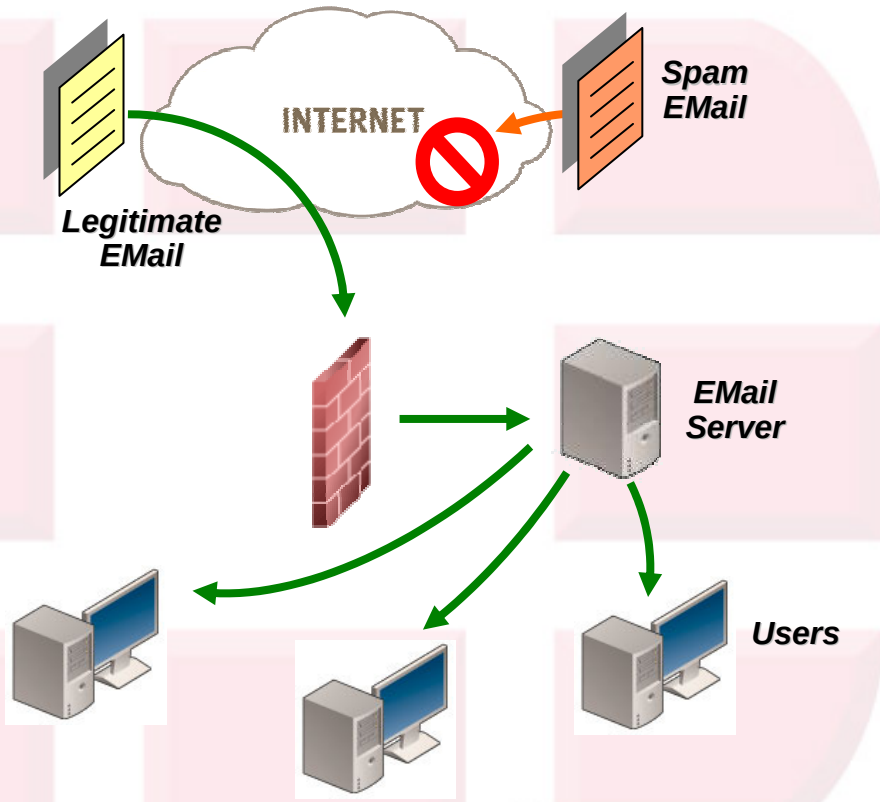
- AntiSpam Lösung als Service beziehen
- Spam wird durch den MSSP erkannt und entfernt, kommt nie bis zum Kunden durch
- Einfache Konfiguration: Einfache Änderung der DNS Einträge
- Es können alle bekannten Methoden der Spam Erkennung eingesetzt werden

Vorteile:

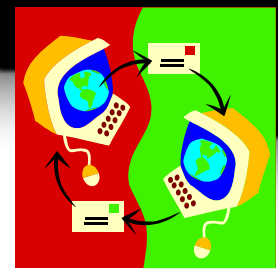
- Hohe Verfügbarkeit und redundante Architektur sind möglich
- Reduziert die Bandbreite des Kunden
- Unterstützt mehrere Emailserver und Internetverbindungen
- Minimiert den Administrationsaufwand
- Keine Investitions-, sondern nur zusätzliche Wartungskosten p.a.

Nachteile:

- Fine tuning kann langsam sein
- Granularität kann verloren gehen
- Spam Erkennungsrate kann tiefer sein als bei einer eigen-installierten Lösung



AntiSpam – Effektivität gefordert



- Transparent, MSSP und Gateway
  - Bringen die besten Gesamtresulte
  - Stoppt Spam bevor es die internen Resourcen oder gar Benutzer erreicht
- Die Kostenersparnis sinkt, je näher der Spamfilter beim Benutzer ist
  - Mehr Speicheraufwand Bandbreite, Rechenpower
  - Reduziert den administrativen Aufwand, benötigt Benutzerkonfiguration
- Schutz auf mehreren Ebenen
  - Verschiedene Filter Mechanismen erhöhen die Erfolgsrate
  - Granulare benutzerbasierende Filter optimieren näher zum Benutzer
- Der stufenweise Schutz zwischen dem Internet und dem Emailserver ergibt eine bessere Kontrolle und verbessert die Erkennung

FortiMail unterstützt die Installation als Gateway, als Server, als MSSP-Lösung sowie im TRANSPARENT Mode.

FortiMail Secure Messaging Platform

Fortinet's aktuelle Sicherheits-Plattform für den Bereich des Email Messaging

Fortinet’s FortiMail AntiSpam Lösung

- Gehärtete AntiSpam Security Plattform
  - Dediziertes Appliance mit gehärtetem OS
  - Keine bekannten Schwachstellen oder erfolgreiche Attacken
- Zwei Modelle
  - FortiMail-400 (mittlere Kapazitäty)
  - FortiMail-3000 (hohe Kapazität)
- Drei Modi der Implementation
  - Transparent, Gateway, Server
- Flexible Installationsoptionen (mehrere Schnittstellen)
- Standard FortiNet Web management interface (wie bei Fortigate)
- Content- und Netzwerk basierende AntiSpam Technologien sorgen für höchste Erfolgsraten

FortiMail-400

FortiMail-400

- **Spezifikation**
  - 1U 19” rack mount
  - 2 x 10/100/1000 Ethernet Ports
  - 4 x 10/100 Ethernet ports
  - 120G HDD (RAID 0/1)

- Kundensegment: Mittelgrosse bis grosse Unternehmen
- Unterstützt bis zu 2000 Email Konten
- Performanz (1K-3K sample Grösse)
  - 70k pro Stunde 1.68m pro Tag (antispam)
  - 140k pro Stunde 3.36m pro Tag (antivirus)
  - 130k pro Stunde 3.12m pro Tag (logging)
  - 85k pro Stunde 2.04m pro Tag (archiving)
  - 54k pro Stunde 1.30m pro Tag (all features)

Ausgereifte AntiSpam Optionen

- Kompletes Email Scanning
  - Header, body, raw body, URI, und Meta Information
- Advanced spam detection und Filter Methoden:
  - Access Policy filtering
  - Content filtering
  - Global und User Black/White List filtering
  - Real-Time Blackhole List (RBL) filtering
  - Spam URI RBL (SURBL)*
  - FortiGuard-Antispam (BL & URI) filtering
  - Per User Bayesian filtering
  - Heuristic filtering (900+ rules)
  - Distributed Checksum Clearinghouse (DCC)
- Globale bayesische Trainingsdatenbank für ein effizientes Finetuning

Erweiterter AntiVirus und DoS Schutz

AntiVirus

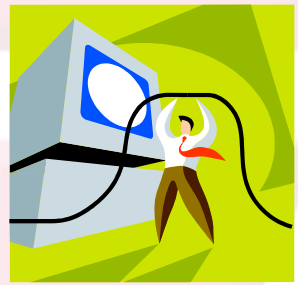
- Antivirusengine für Viren und Spyware Erkennung mit automatischen Update durch FortiProtect's Global Network
- FortiMail scant SMTP Mitteilungen
- Komprimierte und archivierte Anhänge
- Setzt infizierte Dateien in Quarantäne
- Replacement Messages
- Blockieren der Dateien aufgrund der Dateigrösse
- Anhang Filter

Denial-of-Service

- Denial of Service (Mailbomben)
- Empfänger Address Attack
- Email Rate Limiting
  - Anzahl der erlaubten Emails pro Sender
  - Anzahl gleichzeitiger SMTP Sessions pro Sender
  - Ausnahmelisten
- Sender Reverse DNS Check (anti-spoofing)

Transparent & Gateway Mode Optionen

- Multiple email domain support
- Acts as SMTP mail gateway for existing mail servers
- Fast and simple deployment through a simple DNS MX record change (Gateway Mode)
- Integrated policy-based mail routing and queue management
- Functions as an Outbound Mail Relay for improved mail security
- Granular layered detection policies for spam and antivirus
- Antivirus replacement messages for notification
- Spam quarantining and spam tagging
- Accept, Relay, Reject or Discard spam based on email address, IP address, or domain
- Quarantined email access with WebMail, POP3, and IMAP
- Daily quarantine summaries
- Policy-based email archiving of inbound and outbound messages
- Comprehensive email monitoring, logging, and reporting
- Mail Queue support for failed, deferred, and undeliverable mail
- SMTP Authentication support through LDAP, RADIUS, POP3 or IMAP
- Per User Automatic White List
- DNS acceleration
- Per user AV and AntiSpam configuration via LDAP query



Server Mode Features

Alle Optionen aus dem Transparent und Gateway Mode plus:

- POP3, SMTP, und IMAP Email services
- SMTP over SSL Support
- Disk quota Regeln für Benutzer
- Secure WebMail Benutzerzugang
- Benutzer, Gruppen und Aliaslisten
- Local Account und LDAP Authentisierung
- Bulk Folder Support für Spammail

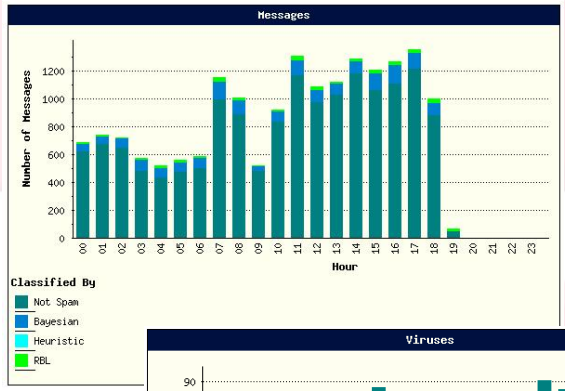
FortiMail Logging & Reporting

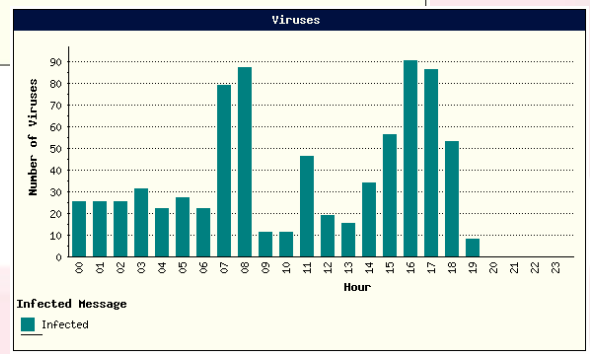
- Change-Management und Event-Management loggen
- Antivirus loggen
- Antispam Aktivitäten loggen
- Externer und lokaler Syslog Server Support
- Erweitertes, zentrales Reporting mit dem FortiReporter möglich
- Alarmierung bei Virenvorfällen oder auch bei System-kritischen Vorfällen
- Ausgereiftes Reporting mit über 140 Reporte aus 7 Kategorien
- Mehrere Reportformate wie MS Word, PDF, HTML
- Reporte können nach Wunsch zeitlich geplant und dann automatisiert per Email verschickt werden.

Absolute Transparenz - FortiMail Reporting

- Reporte, geplant oder nach Bedarf
- Sieben Report Kategorien:
  - High Level Breakdown (22 Reporte)
  - Mail pro Sender (15 Reporte)
  - Mail pro Empfänger(15 Reporte)
  - Spam pro Sender (30 Reporte)
  - Spam pro Empfänger(15 Reporte)
  - Virus pro Sender (30 Reporte)
  - Virus pro Empfänger (15 Reporte)

Messages		Today	This Hour
Not Spam		15742	51
Spams Classified By	Bayesian	1659	6
	Heuristic	27	0
	RBL	351	15
	Spam Subtotal	2037	21
Virus Infected		772	8
Total		17779	72





FortiMail Archivierung

- Archivirungsregeln erlauben die Selektion nach folgenden Kriterien:
  - Sender Adresse
  - Empfänger Adresse
  - Schlüsselwörter im Betreff
  - Schlüsselwörter im Text
  - Anhänge nach Namen
- Ausnahmelisten
  - Basierend auf der Sender und Empfänger Adresse
- Support für externen Speicher

FortiMail Quarantäne & Spam Optionen

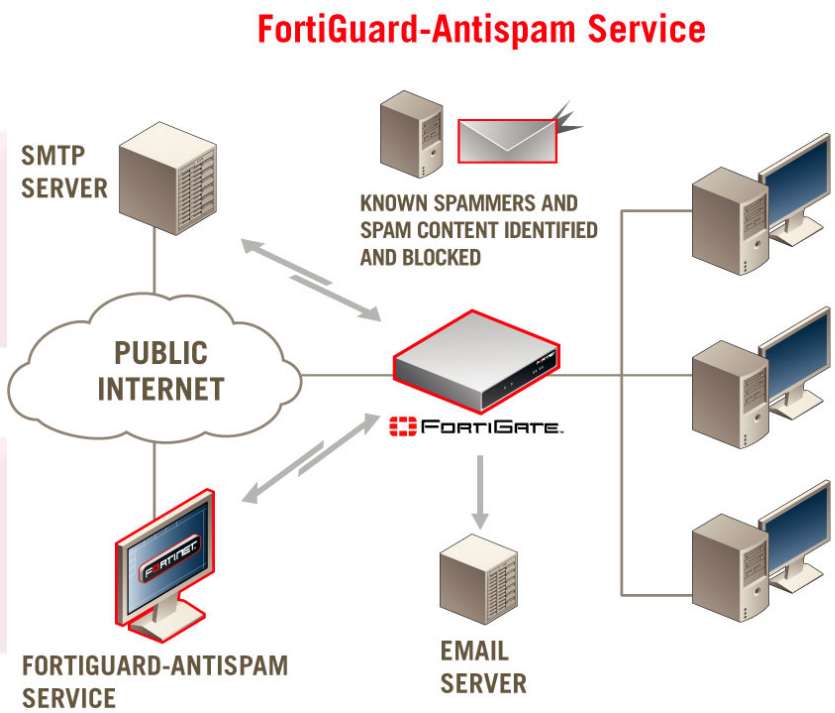
- Zugriffskontrolle
  - Accept, Relay, Reject, Discard email basierend auf der Email Adresse, IP Adresse, oder auch Domaine
- Mail Queues
  - Failed Queue: Speichert nicht gesandte Messages älter als 5 Tage. Erlaubt dem Administrator diese zu verwerfen oder nochmals zu senden.
  - Deferred Queue: Speichert nicht gesandte Messages weniger als 5 Tage alt. Sie werden automatisch nochmals versandt.
  - Dead Mail Queue: Speichert Emails die eine falsche Sender oder Empfänger Adresse hat.
- In Quarantäne befindliche Emails können über folgende Zugriffe verarbeitet werden:
  - Automatic Release
  - WebMail
  - POP3

FortiGuard-Antispam Service

Fortinet’s Service für AntiSpam

FortiGuard-Antispam Service

- Abgerundeter Service zur Reduzierung von Spam
- Fortinet's Spamsonden sammeln globale Spammer Informationen
- AntiSpam Datenbank wird täglich unterhalten und erweitert.
- Verfügbar für FortiGate wie auch FortiMail Plattformen
- Dual pass scanning Technology verbessert die Erkennungsrate mit den RBL Services
  - 1ter Pass sucht nach IP Adressen bekannter Spammer
  - 2ter Pass benutzt bekannten URI Inhalt zur Identifikaton von Spam



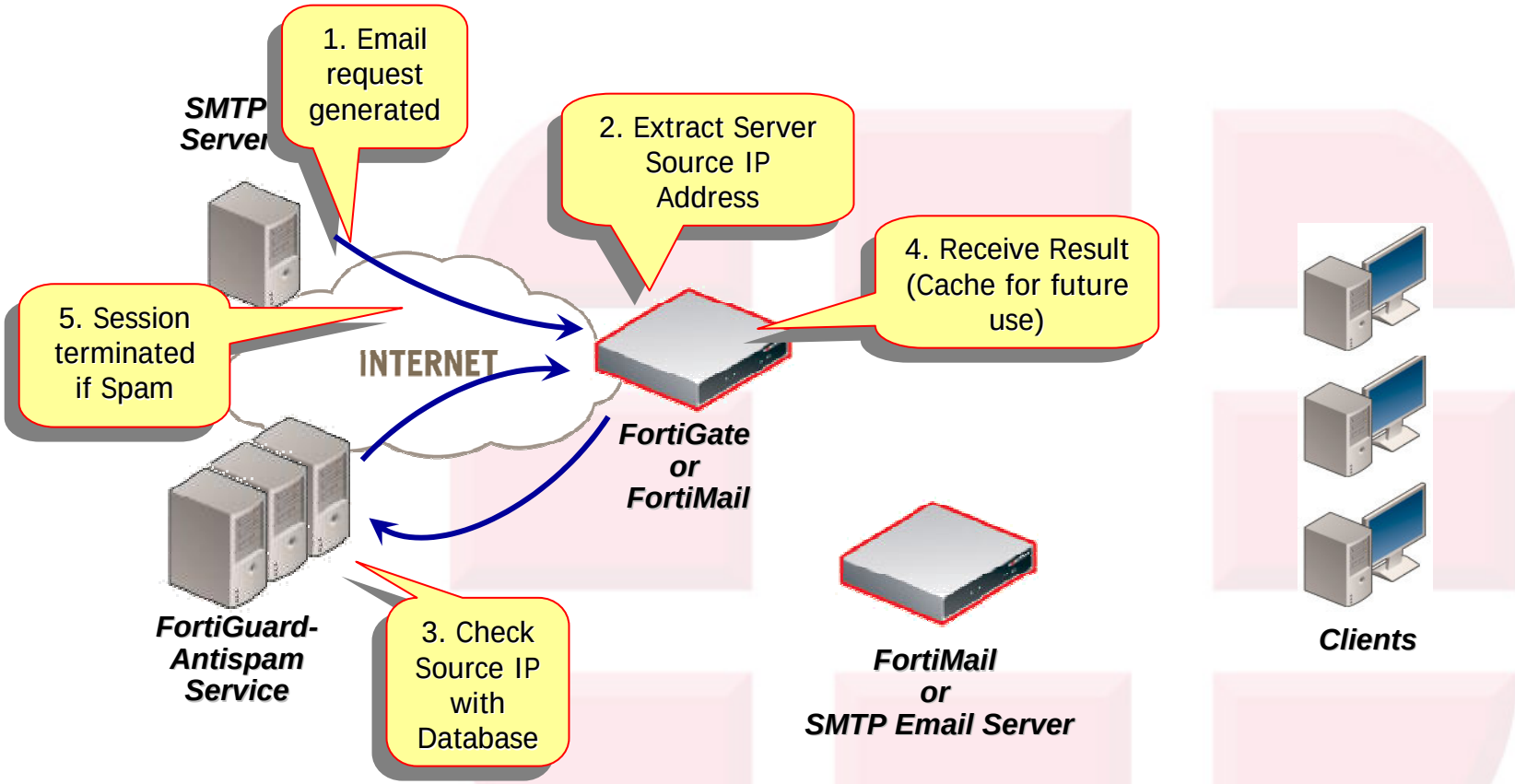
Was bietet FortiGuard-Antispam mehr

- Realtime Blackhole Listen (RBL) sind Datenbanken ,die wir für unsere Kunden pflegen. Damit erhöhen wir die Qualität, Aktualität und natürlich Erreichbarkeit.
- Bayesische Filter suchen Spam nach Wörtern oder auch Pattern ab. Zum einen müssen diese Filter durch den Benutzer trainiert werden, zum anderen verfeinern wir die Filter laufend.
- Wir unterhalten eigene DCC Server im Verbund mit anderen Servern (Distributed Checksum Clearinghouse). Über jedes Mail wird eine oder mehrere Checksumme gelegt und mit anderen aus der grossen Datenbank verglichen. Damit garantieren wir die bestmögliche Erkennung von Massenmails.

Der Administrator braucht eine Lösung, die sich selbst optimiert und den „spammerischen“ Veränderungen kontinuierlich anpasst, auf allen Ebenen der Kommunikation.

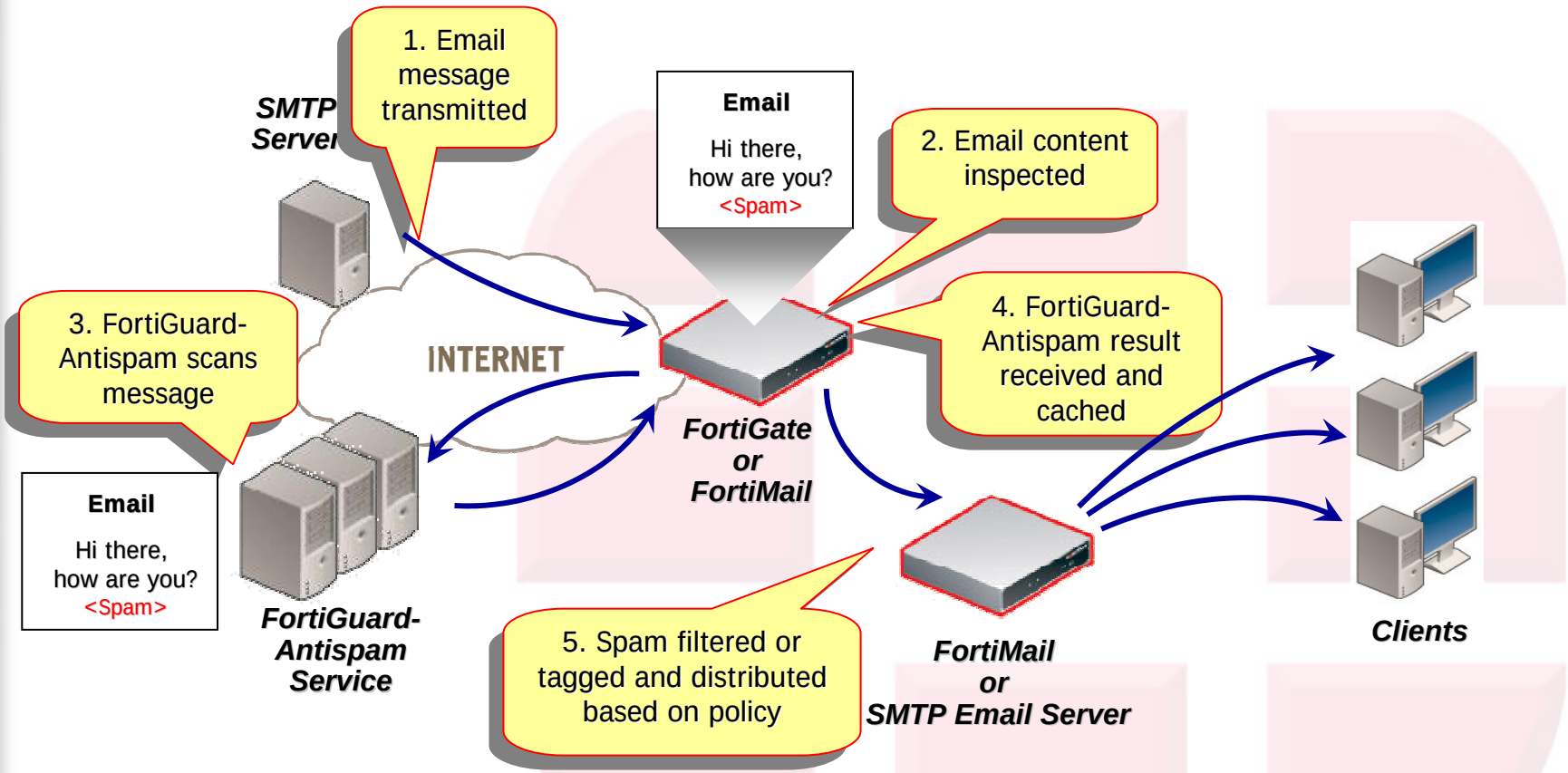
FortiGuard-Antispam Übersicht – Erster Scan

- Connection Check



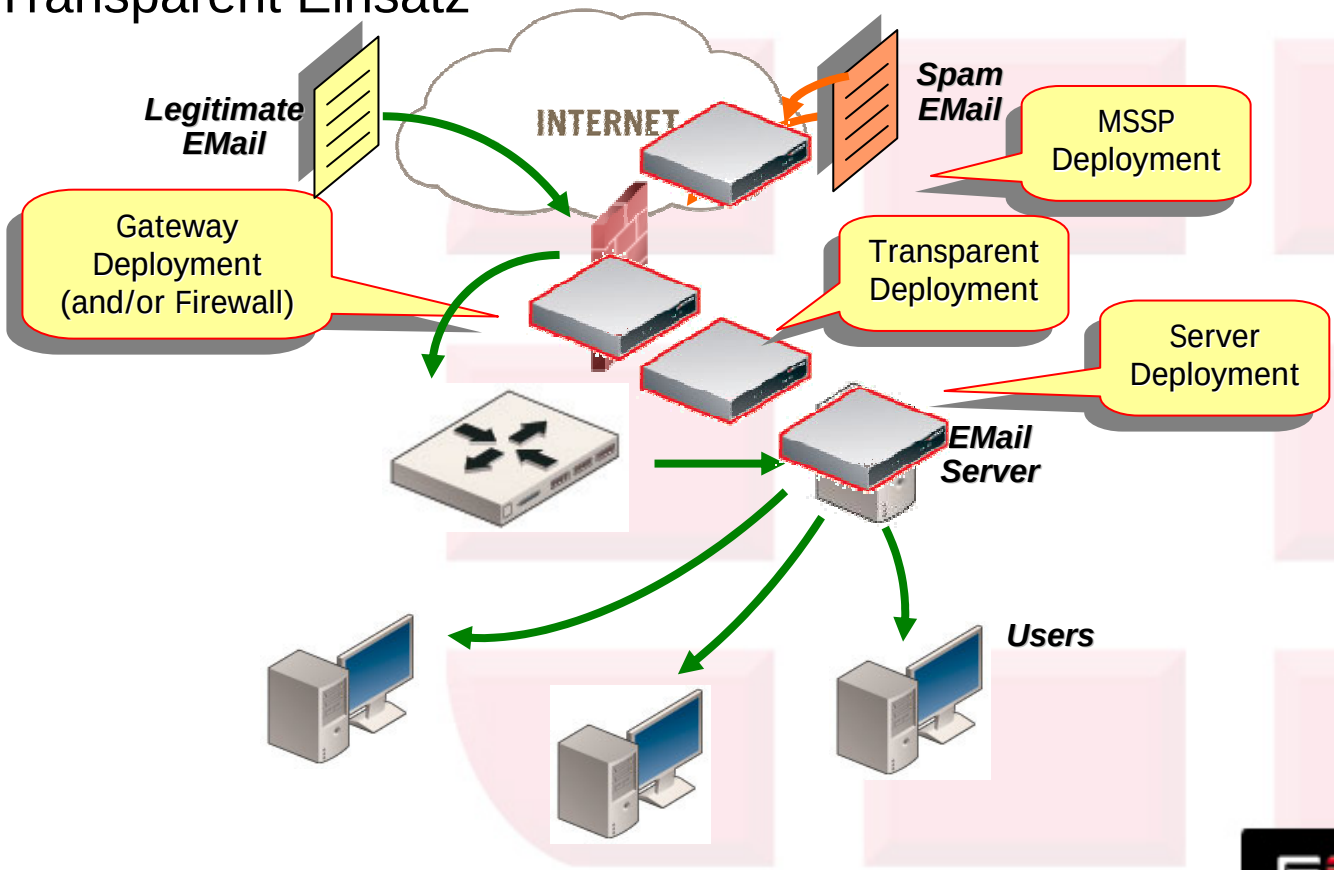
FortiGuard-Antispam Übersicht – Zweiter Scan

- Content Screening



FortiMail - der Einsatz Ihrer Wahl

- MSSP Einsatz
- Gateway Einsatz
- Server Einsatz
- Transparent Einsatz



Fortinet: der anerkannte Leader bei UTM

- Gegründet im Oktober 2000, heute 600 Mitarbeiter
  - Gründer Ken Xie, Gründer/CEO/President von NetScreen (jetzt Juniper)
- Headquarter in Sunnyvale, CA
  - Entwicklungscrews in Amerika, Kanada, Süd-Frankreich und Japan
  - Schweiz: Vertriebsbüro in Zürich mit Franz Kaiser und Urs Blum (SE)
  - Vertrieb über >120 Reseller bzw. über unseren Distributor Cetus
- Entwickler des einzigen ASIC-powered “Content Analyse Systems”
  - Fortinet Produkte sind optimiert um UTM (Unified threat management) in realtime auszuführen, sind von Anfang an dafür konzipiert worden
- 100Mio$ Venture Capital, IPO geplant Ende 2005
  - Dow Jones und Light Reading ernannten Fortinet zu TOP 10 IPO Firmen für das Jahr 2005.


FORTINET
THE POWER IN NETWORK PROTECTION
Danke für Ihre Aufmerksamkeit !