Cisco Expo 2008

Secure Messaging Solutions

Daniel Wolf, Sales Manager / Austria
Achim Kraus, Systems Engineer / Central Europe

Agenda

Aktuelle Bedrohungen

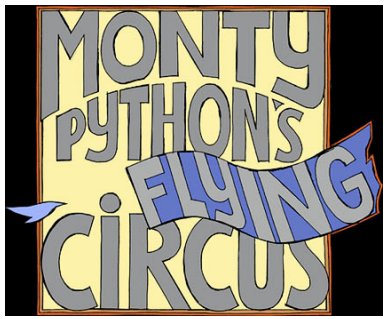
Technische Aspekte und Bedrohungen anhand von aktuellen Beispielen aus der Praxis.

Lösungsansätze

Wege der Gefahrenabwehr durch mehrschichtige und reputationsbasierte Gateway-Lösungen.

Aktuelle Herausforderungen

"Spicy Pork And Meat"
Hormel Foods Corporation



Erste Spam-Emails?

- April 1994

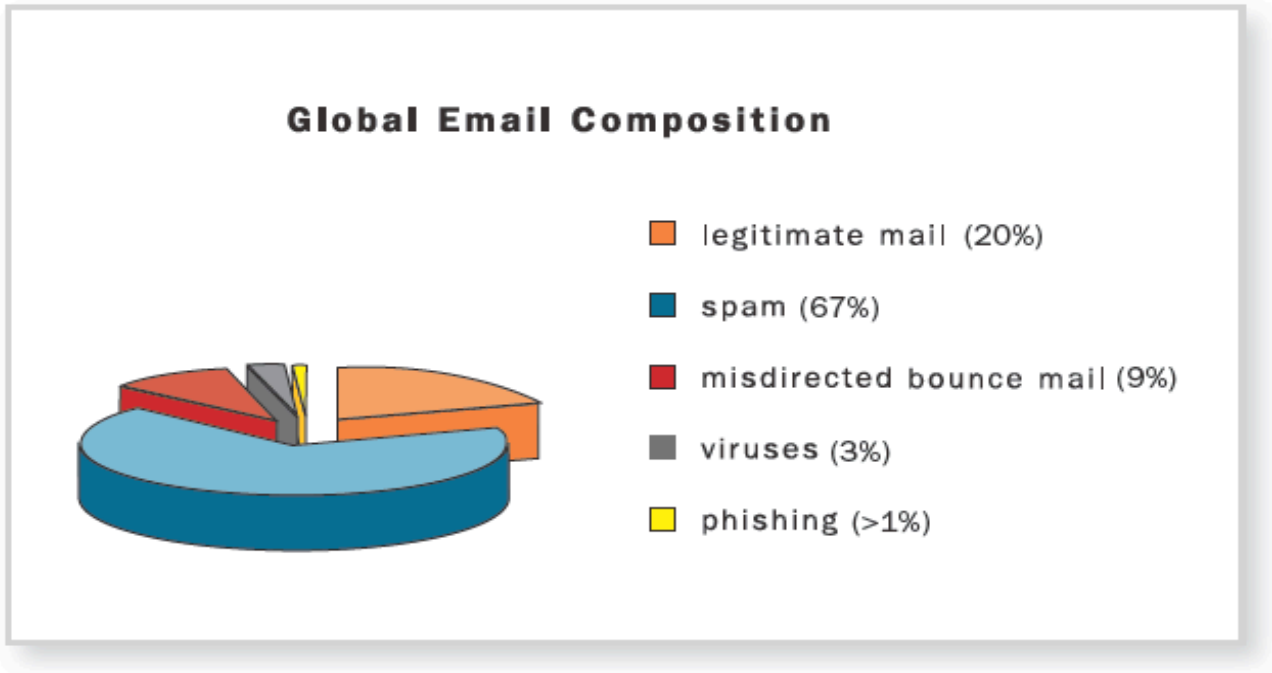
Neues Bot-Netz an einem Tag?

- 23. Mai: 892.565

Infektion um Spam zu versenden?

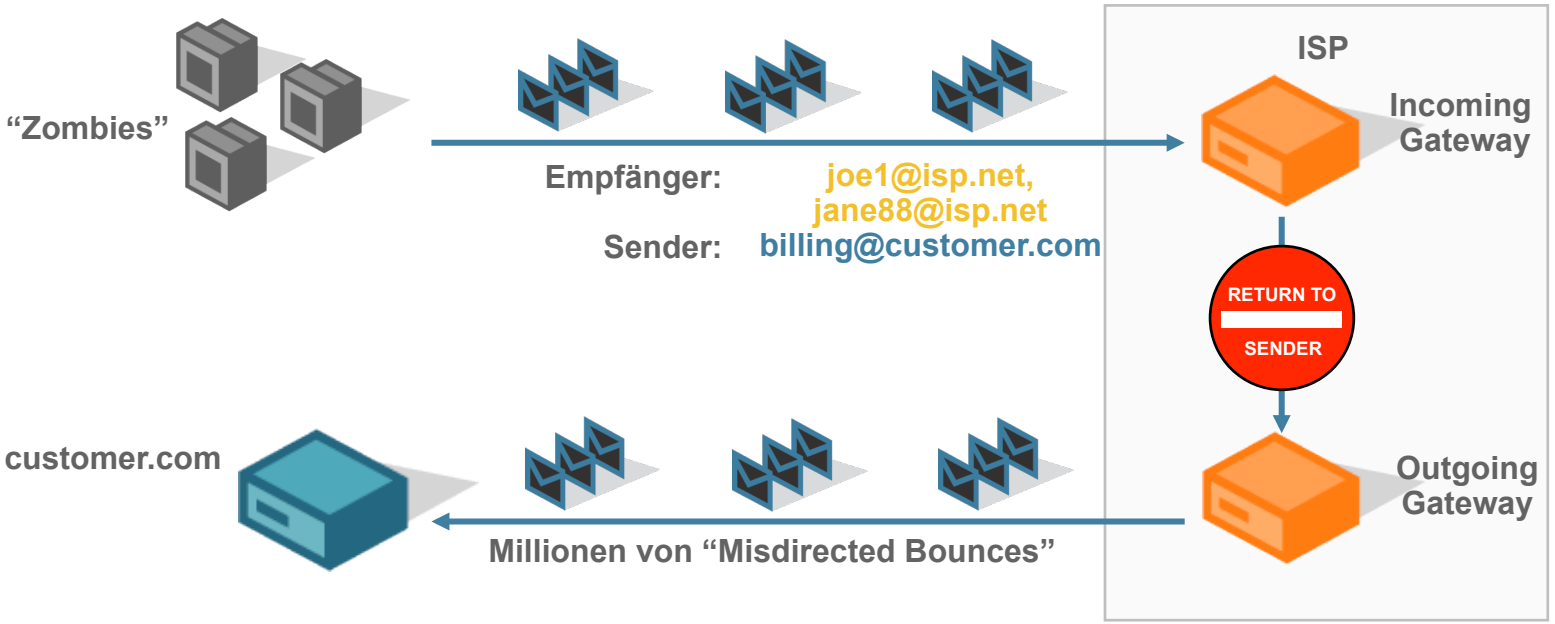
- 36 Sekunden

Unerwünschte Email-Kommunikation



Quelle: IronPort Threat Operations Center (25 – 30% weltweiter Email-Kommunikation)

Misdirected Bounces (4.5 Mrd. täglich)

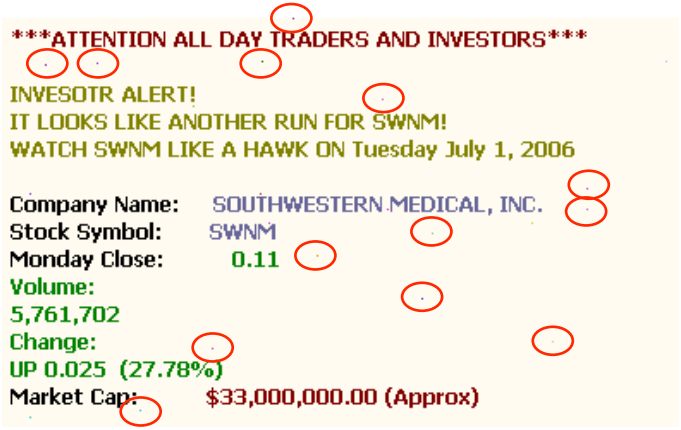


> 55% der Fortune 500 Unternehmen berichten Ausfälle durch "Misdirected Bounce" Attacken !

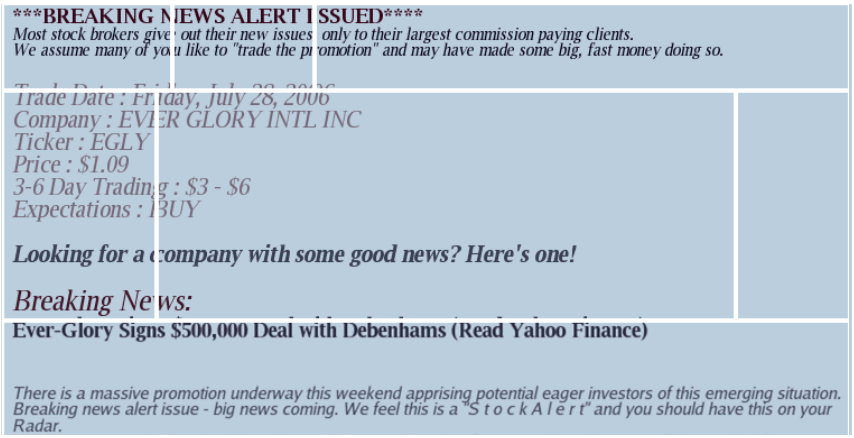
Quelle: IronPort Threat Operations Center (25 – 30% weltweiter Email-Kommunikation)

Spam-Varianten
Image-basierend

“Polka-Dots”



“Slice & Dice”



Profil dieser Spam Attacke

Spam-Attacke von 20 Milliarden Emails innerhalb von zwei Wochen im Mai 2006

- Zeitweise mehr als 1.5 Milliarden Emails täglich

Vorgehensweise

- Ständig modifizierter Spam-Inhalt einschliesslich URL

Spam Infrastruktur

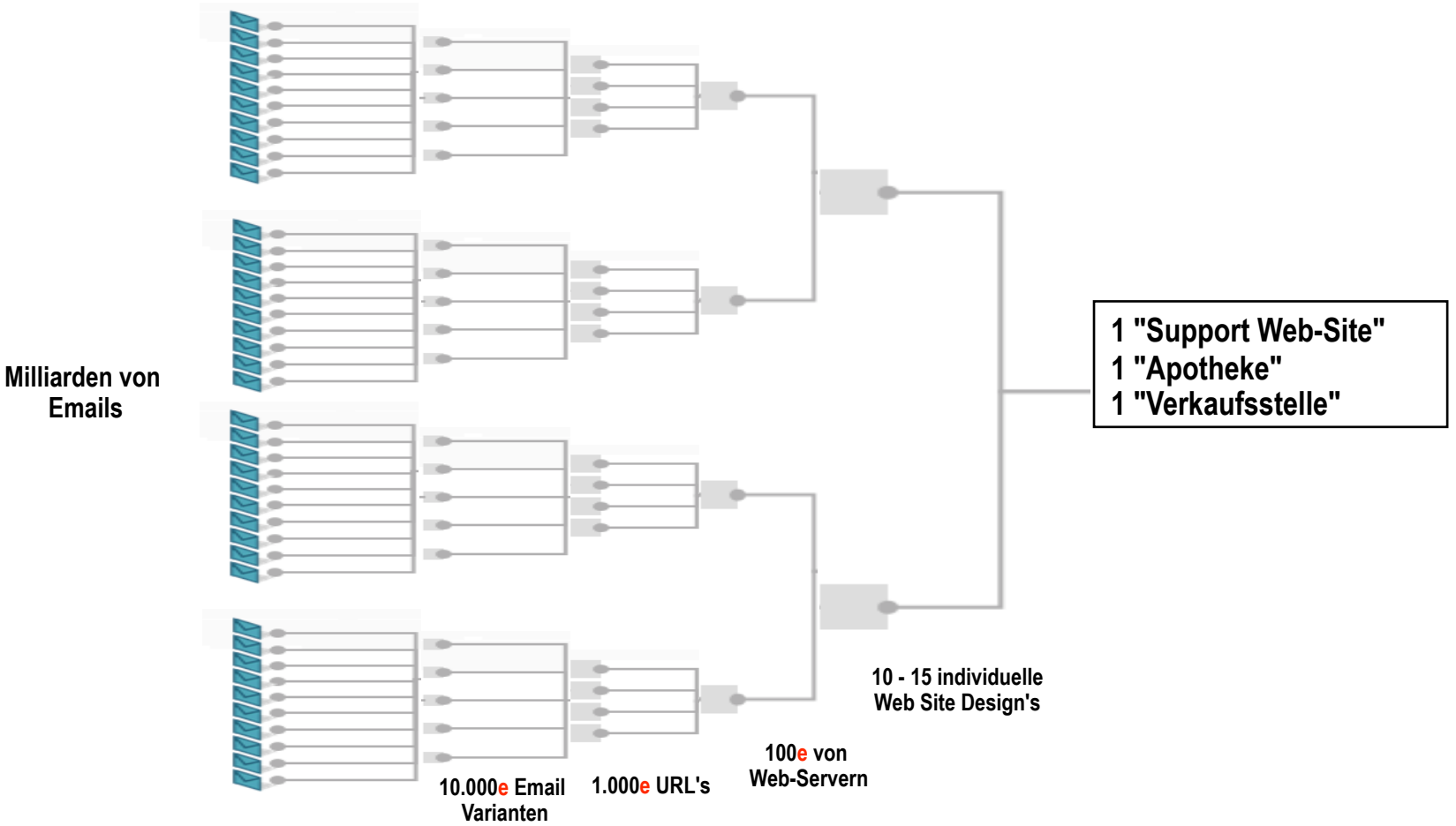
- 100.000 infizierte PC's (Zombies)

"Botnet Command and Control" (C&C) Infrastruktur

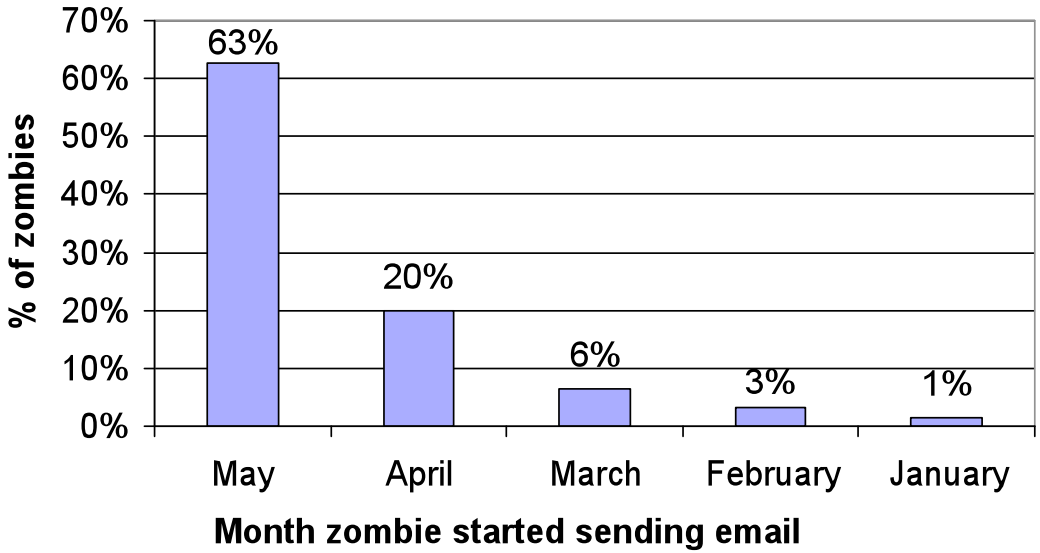
- 1500 Domänen und 100 Web Server

Ein "Geschäftsmodell”.

Analyse einer Spam-Attacke



Spam Quelle: 100.000 Zombies

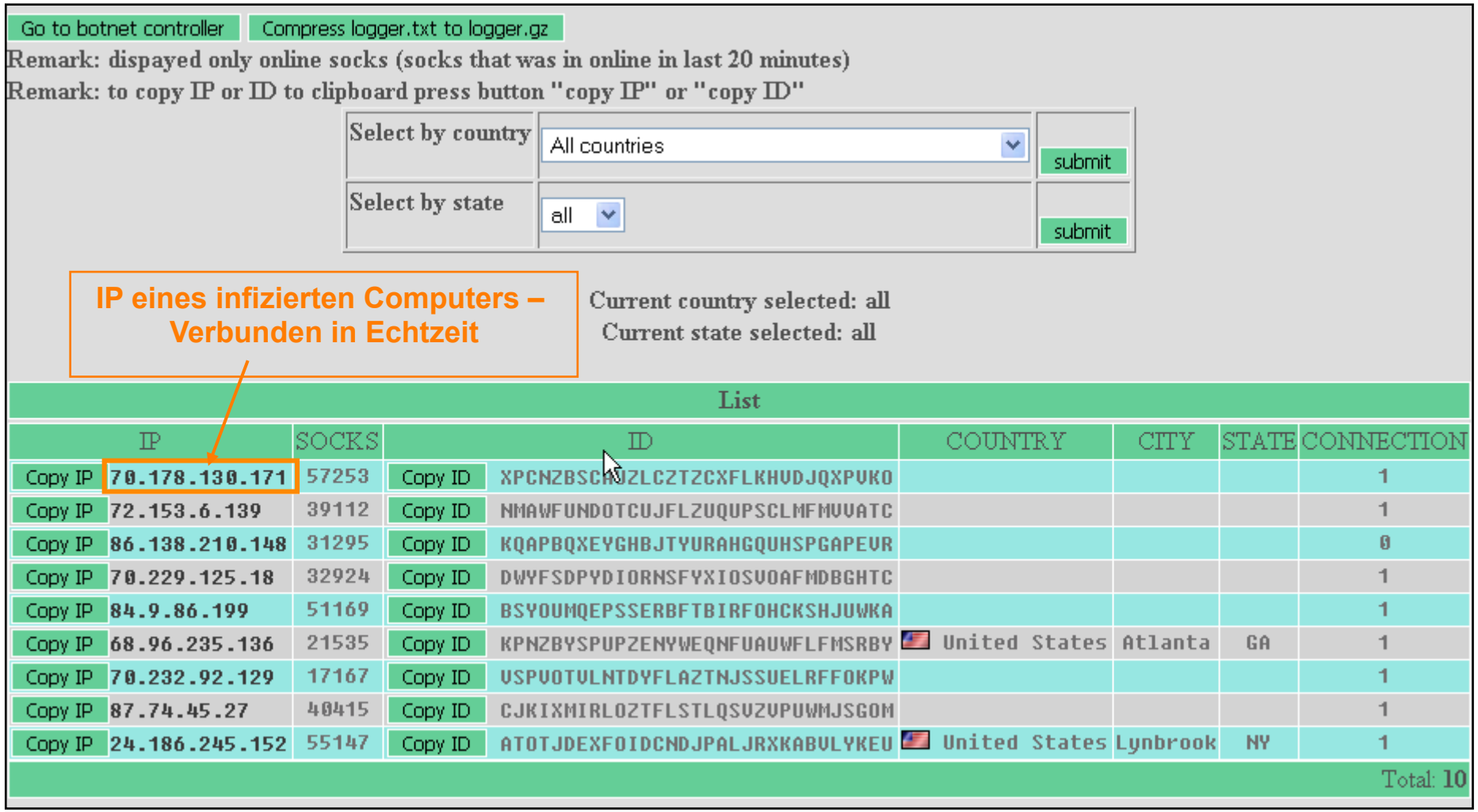


80% Spam von Zombies < 30Tage 'alt'

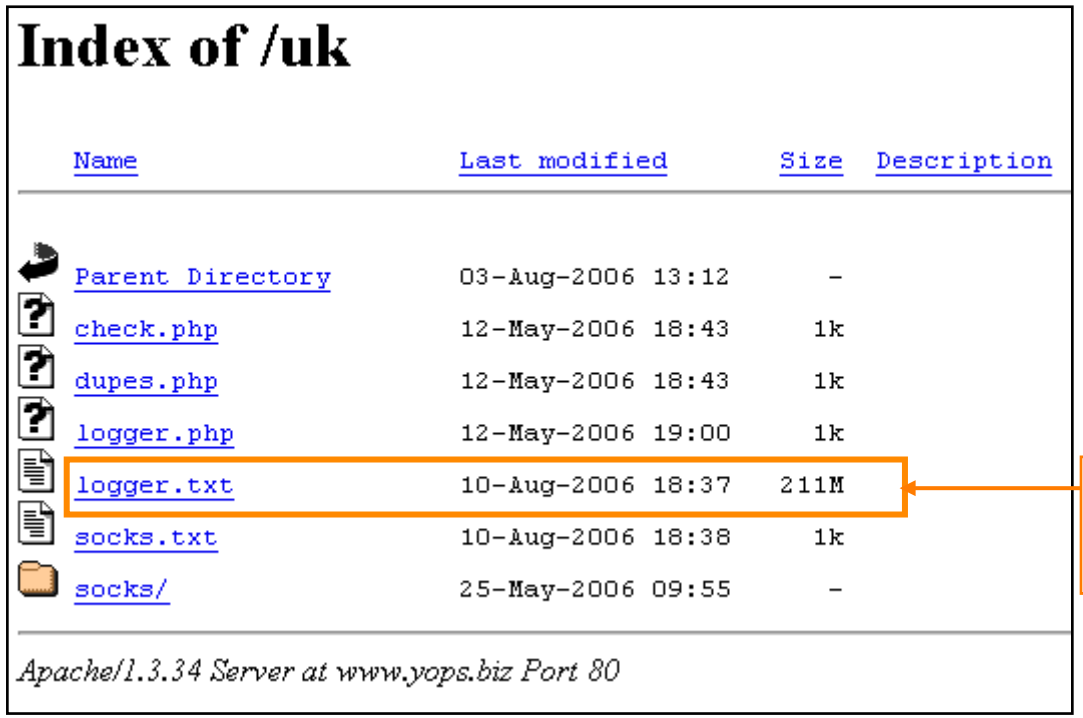
Top 10 Netzwerke senden 28% weltweiten Spam Aufkommens

Rank	Network Owner	Country	%
1	Telefonica de Espana	Spain	6.7%
2	France Telecom	France	4.3%
3	Proxad	France	3.4%
4	Telecom Italia	Italy	2.6%
5	Deutsche Telekom AG	Germany	2.2%
6	Cableuropa - ONO	Spain	2.2%
7	Telemar Norte Leste S.A.	Brazil	1.8%
8	Wanadoo France	France	1.7%
9	Telefonica de Espana SAU	Spain	1.7%
10	TELECOMUNICACOES DE SA	Brazil	1.7%

Botnet “Command & Control Center”



Botnet “Command & Control Node”

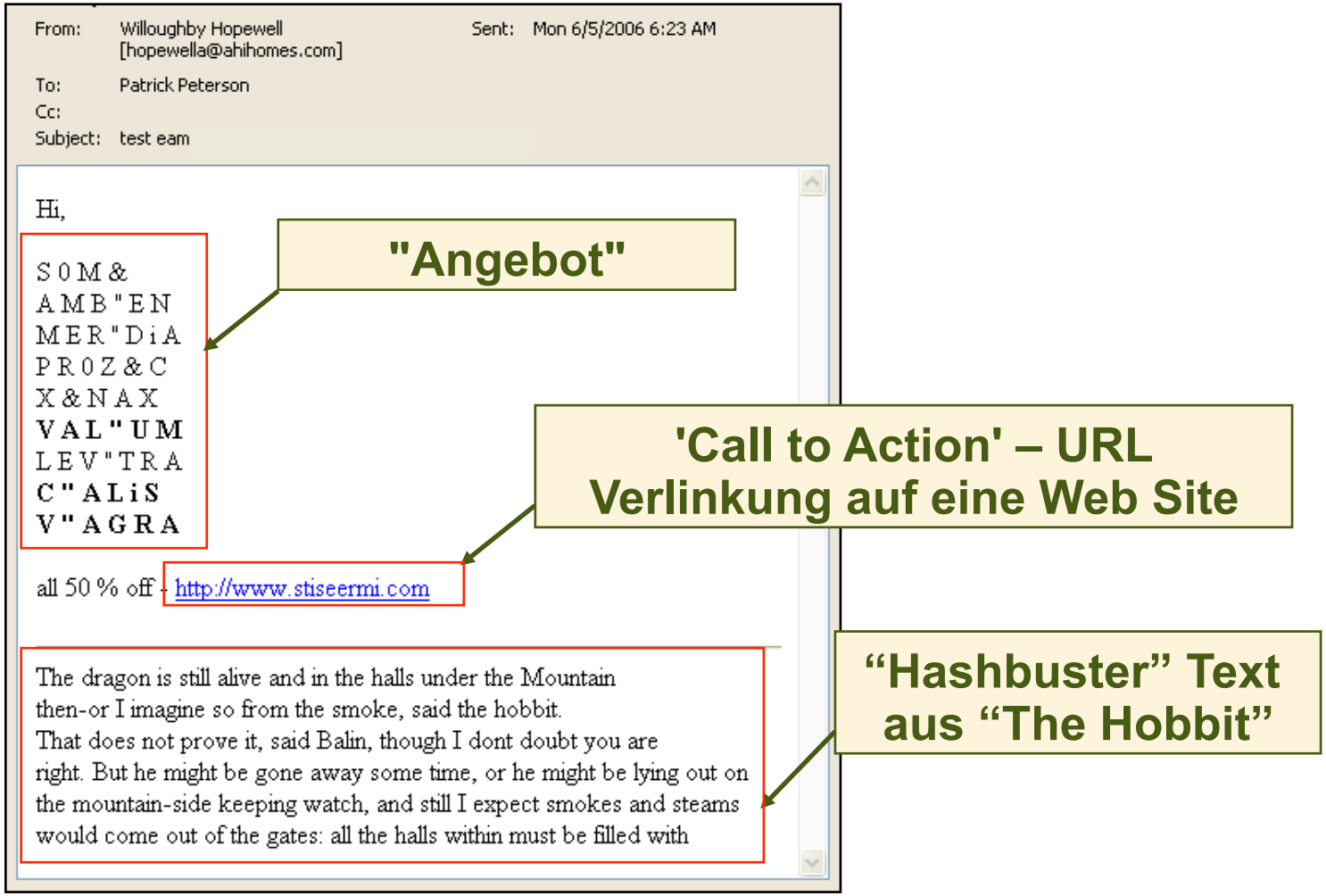


Index of /uk

Name	Last modified	Size	Description
Parent Directory	03-Aug-2006 13:12	-	
check.php	12-May-2006 18:43	1k	
dupes.php	12-May-2006 18:43	1k	
logger.php	12-May-2006 19:00	1k	
logger.txt	10-Aug-2006 18:37	211M	
socks.txt	10-Aug-2006 18:38	1k	
socks/	25-May-2006 09:55	-	

Apache/1.3.34 Server at www.yops.biz Port 80

Das 'Angebot' – 1 Spam Email



Irreführung - 6 unterschiedliche Inhalte

15 individuell gestaltete Web-Sites

Pharma Sites (9)

- My Canadian Pharmacy
- International Legal RX
- US Drugs
- Super Viagra
- Viagra Pro
- Generic Viagra
- Cialis Soft Tabs
- Viagra Soft Tabs
- Maxaman

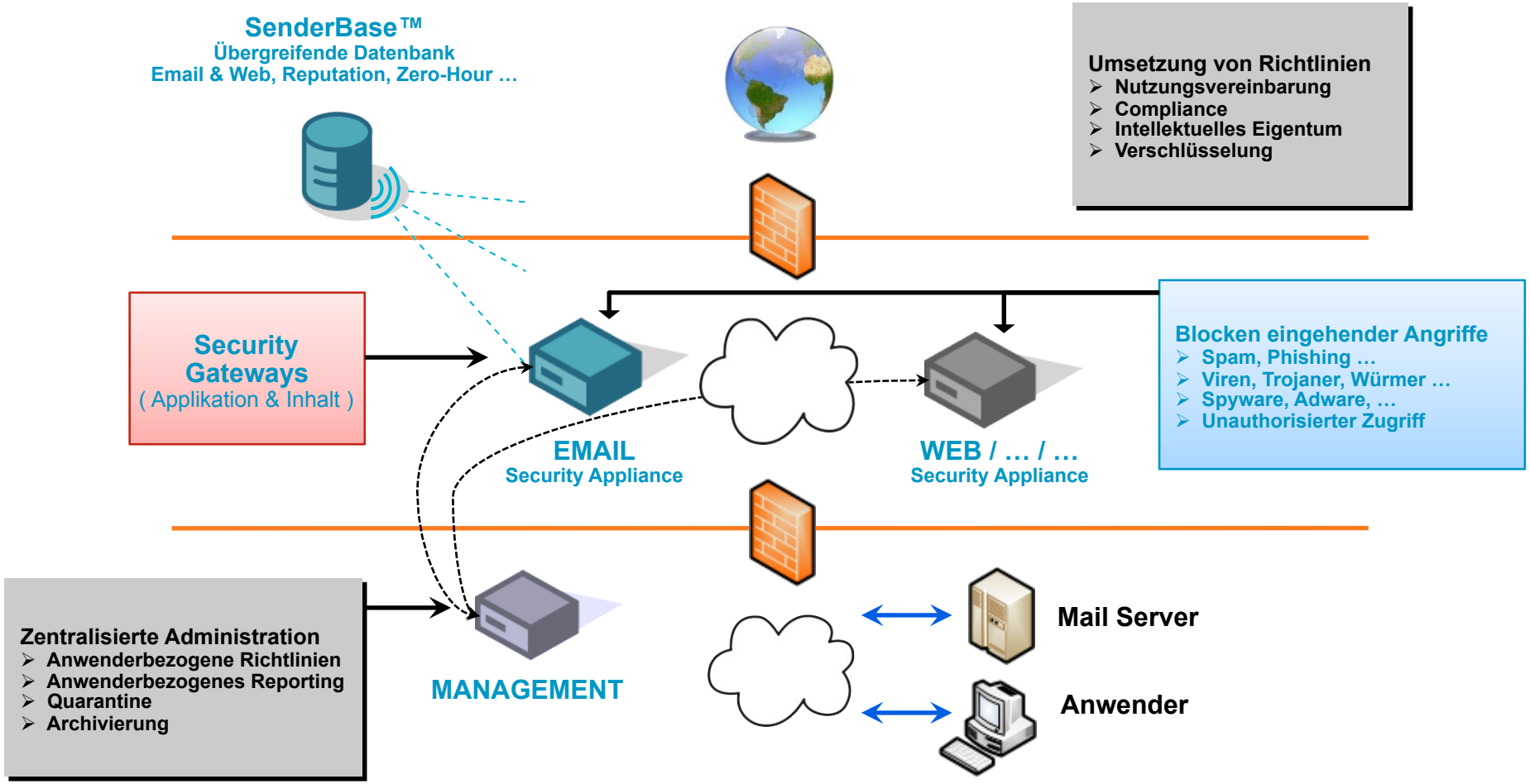
Andere Sites (6)

- Virility Patch
- Super HGH (flash)
- SpermaMax
- My Replica Rolex
- Exclusive Caviar Online
- Double Your Dating

Unterschiedliche Web Auftritte

Lösungsansatz:
- Globale Konsolidierung
- Anwendungsoptimierte Security Appliances

Lösungsansatz:
Konsolidierte Applikations Sicherheit



Produktfamilien Security Gateways

E-MAIL-SICHERHEIT

IronPort Systems bietet mit der C-Serie eine führende E-Mail-Sicherheitslösung zum Schutz von Unternehmen jeglicher Größenordnung. IronPorts innovative Technologien kommen in den anspruchvollsten Netzwerken der Welt zum Einsatz und liegen allen E-Mail-Security-Appliances gleichermaßen zugrunde. Die leistungsstarken Plattformen schützen auf Grund der stetigen Weiterentwicklung nicht nur vor aktuellen, sondern auch vor zukünftigen Gefahren.

WEB-SICHERHEIT

Mit dem branchenweit ersten Web-Reputationsfilter bietet IronPorts S-Serie eine leistungsstarke, mehrschichtige sowie herstellerunabhängige Lösung zur Abwehr von sämtlichen webbasierten Bedrohungen, wie beispielsweise Spyware.

SICHERHEITS-MANAGEMENT

Die IronPort M-Serie™ ermöglicht eine zentrale und konsolidierte Verwaltung Ihrer Daten und stellt Administratoren und Endbenutzern eine integrierte Schnittstelle für das Sicherheitsmanagement zur Verfügung.

IRONPORT C100

Technologien der Enterprise-Klasse in einer leistungsstarken und zugleich preiswerten Appliance für die Sicherheit von kleineren Unternehmen und Filialen mit bis zu 1.000 E-Mail-Nutzern.

IRONPORT C300

Höchste Sicherheit für die E-Mail-Kommunikation in mittelständischen Unternehmen und Organisationen mit einer Größenordnung von 1.000 bis 5.000 E-Mail-Nutzern.

IRONPORT C600

E-Mail-Sicherheit auf höchstem Niveau – die C600 kommt bei Netzwerken mit sehr hohen Leistungsanforderungen und mehr als 5.000 E-Mail-Nutzern zum Einsatz.

IRONPORT X1000

Acht der weltweit zehn größten Internet-Service-Provider (ISPs) haben sie bereits im Einsatz: die X1000 bietet eine hochperformante E-Mail-Sicherheitslösung für die anspruchsvollsten Netzwerke.

IRONPORT S300

Mit den gleichen Funktionen wie die IronPort S600 bestückt, entspricht diese preiswerte Web-Security-Appliance den Sicherheitsanforderungen von Unternehmen mit bis zu 5.000 Benutzern.

IRONPORT S600

Applikations-Proxies für HTTP, HTTPS und FTP, ein Layer-4-Traffic-Monitor sowie eine ausgeklügelte Scanning- und Vectoring-Engine gewährleisten ein Höchstmaß an Leistung und Effektivität.

IRONPORT M600

Die perfekte Ergänzung der E-Mail- und Web-Security-Appliances von IronPort für das zentrale Management von Sicherheitslösungen mit bis zu 5.000 Benutzern.

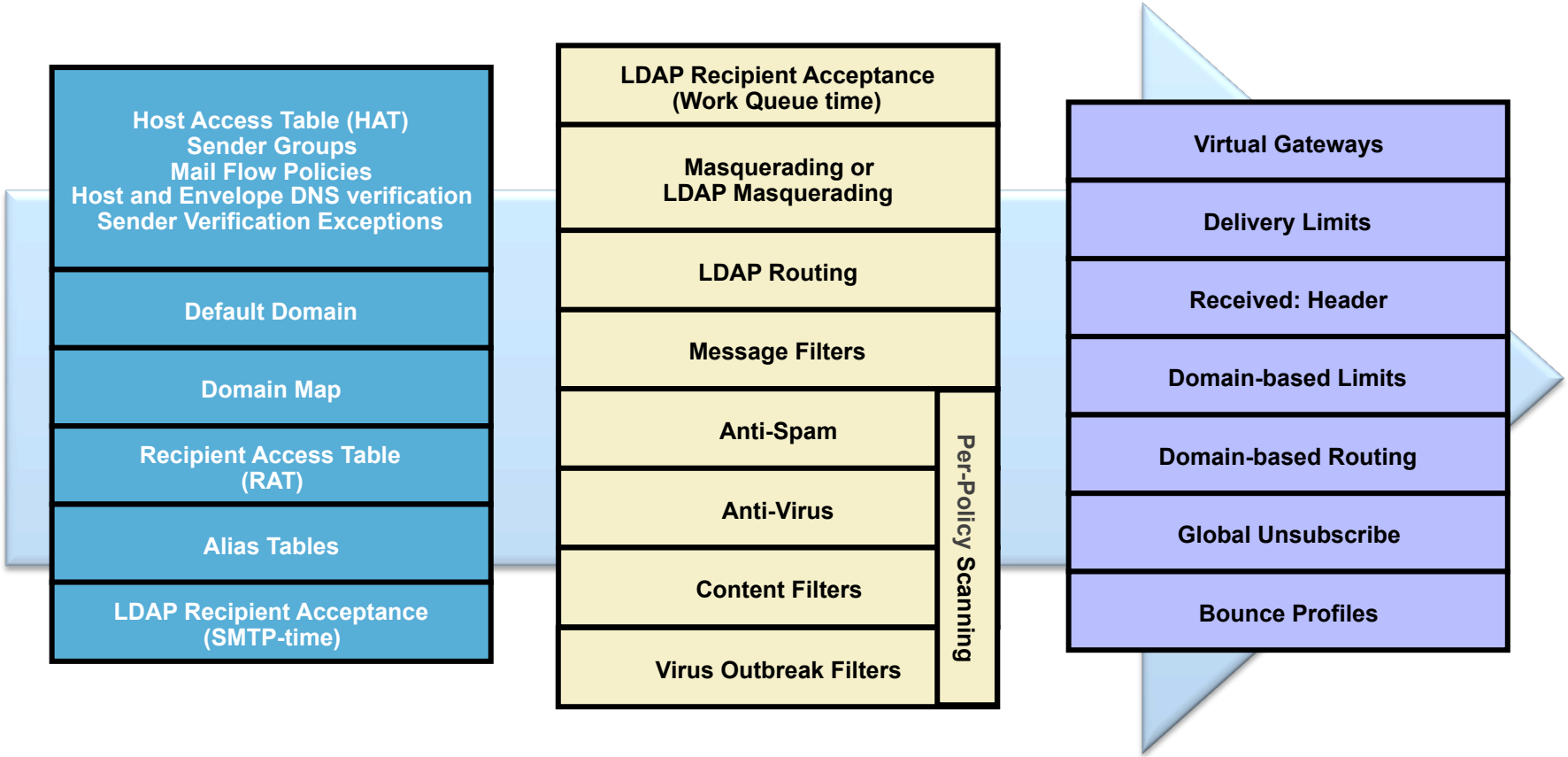
IRONPORT M1000

Die zentrale Quarantäne- und Reporting-Appliance mit dem Extra an Speicher und Leistung für Unternehmen mit mehr als 5.000 Benutzern.

IronPort Architektur
Mehrstufige E-Mail Sicherheit

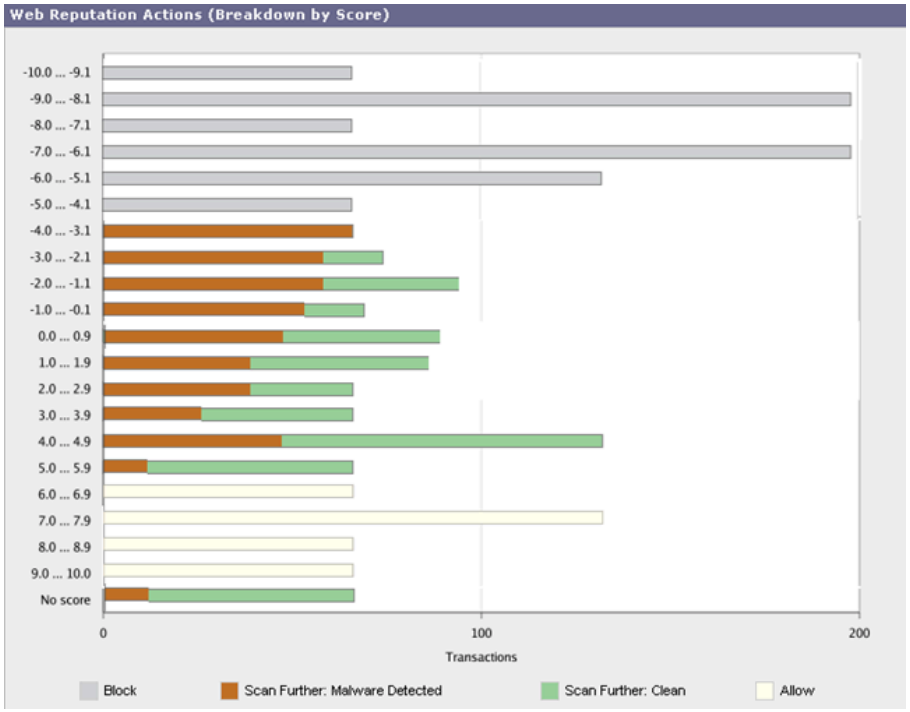
Die IronPort AsyncOS Email Pipeline

[Vereinfacht dargestellt]



IronPort SenderBase Netzwerk - Reputationsdatenbank

Datenbank zur Analyse von E-Mail- und Web-Kommunikation

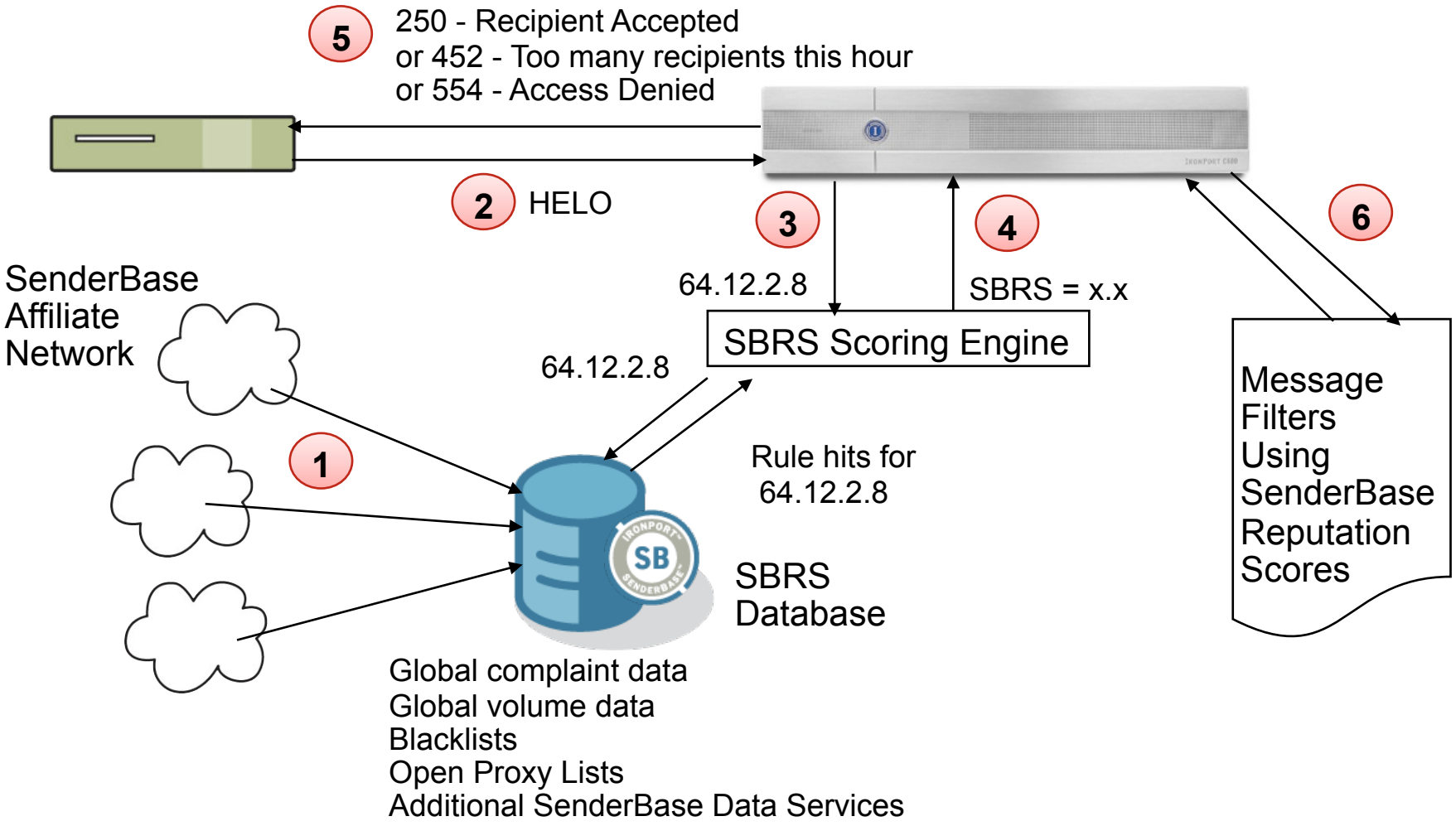


25% des weltweiten E-Mail-Verkehrs

150+ Parameter zur Bewertung von Email- & Web-Resourcen

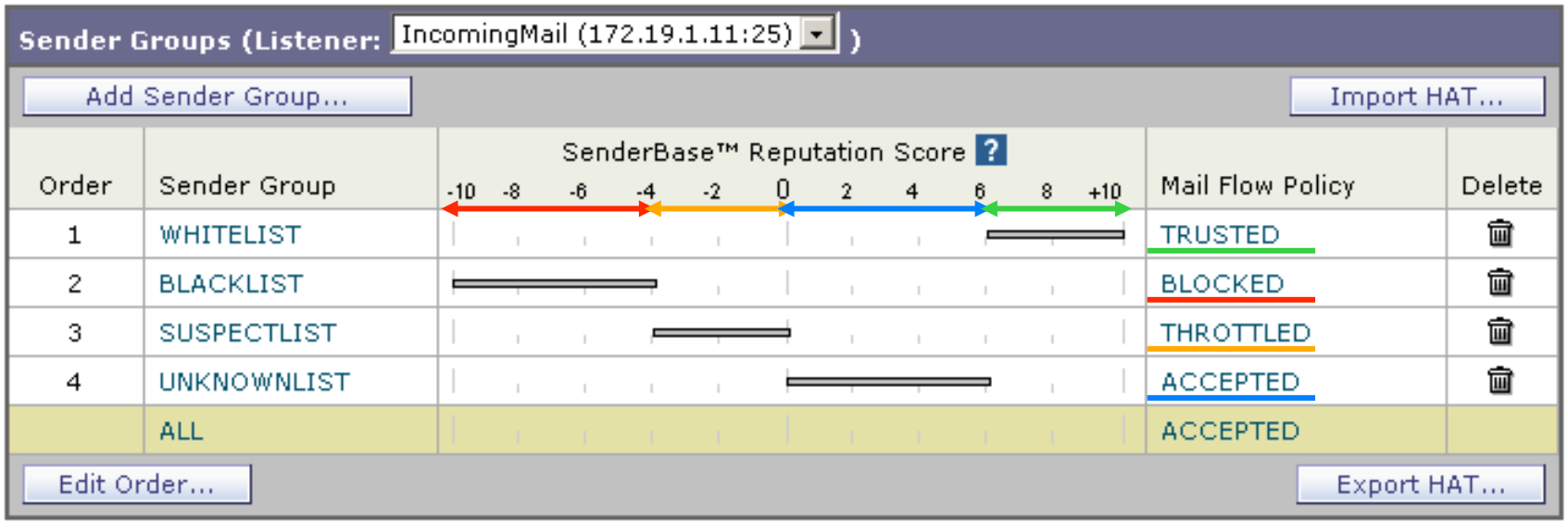
5 Milliarden Anfragen täglich (20 Mrd. Emails)

Ermittlung & Anwendung SenderBase Reputation Score (SBRS)



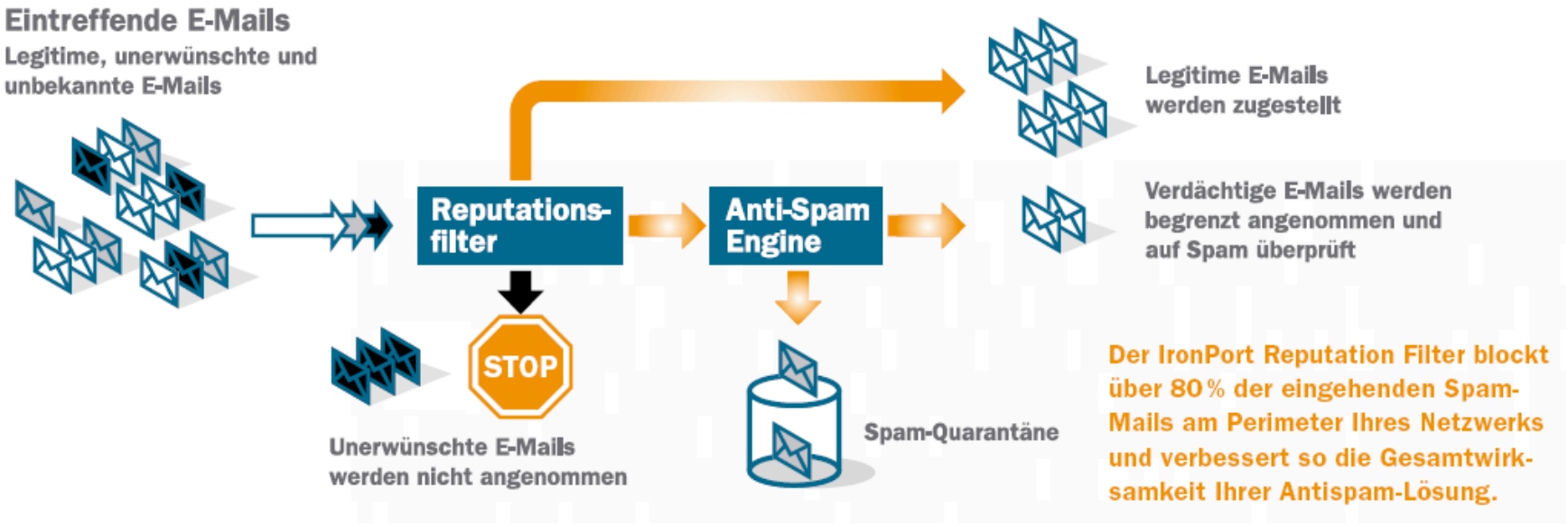
IronPort Reputations-Filter

Mail Flow Monitor & Rate Limiting



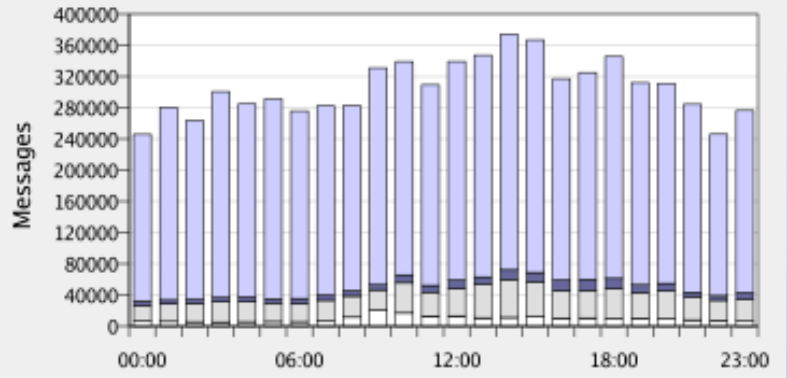
IronPort Reputationsfilter

Stoppt ~ 80% des Spams bereits vor der Annahme



Live Kennzahlen ISP Umfeld

Europa, 24 Stunden, 1 Appliance



Incoming Mail Category	%	# Messages
Total Attempted Messages		**7,330,484**
Stopped by Reputation Filtering	83.94	6,153,125
Invalid Recipients	2.78	204,137
Spam Messages Detected	10.18	746,233
Virus Messages Detected*	0.0	0
Total Threat Messages	**96.9**	**7,103,495**
Clean Messages Accepted	**3.1**	**226,989**

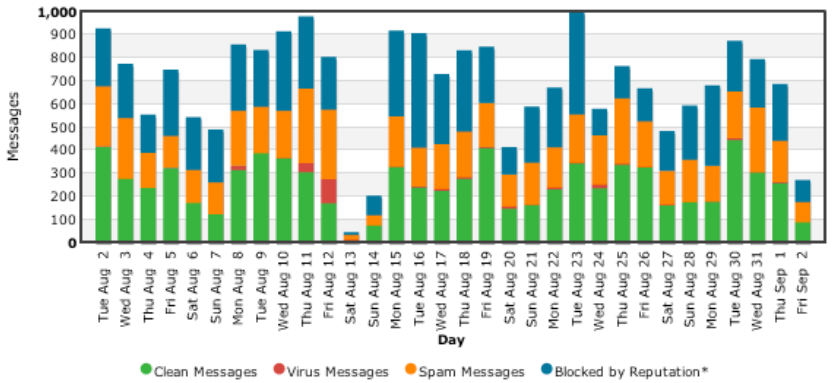
IRONPORT™

IronPort Mail Traffic Report

For data collected from: Aug 2, 2005 through Sep 2, 2005

Your IronPort Email Security Appliance is designed to meet the needs of a wide range of customer demands. The IronPort appliance's exclusive **preventative filters** and highly accurate **reactive filters** eliminate spam, enforce corporate policy, secure the network perimeter, and reduce the total cost of ownership (TCO) of your enterprise email infrastructure.

Incoming Message Volume By Day



Consolidated

This graph represents the message volume received by your IronPort appliance – including:

- **Messages blocked by Reputation Filtering:** These messages are blocked at the SMTP connection level based on the history of the sending IP address. Reputation Filtering prevents Denial of Service attacks, lowers bandwidth utilization, and reduces computing costs on your IronPort appliance.
- **Messages blocked as Invalid Recipients:** These messages are blocked because they match no valid recipients in your network (determined by querying your directory or the Recipient Access Table configured on the appliance). Blocking invalid recipients at the gateway protects you from directory harvest attacks and reduces the load on your groupware servers.
- **Messages identified to contain spam and/or viruses:** These are messages that are positively identified by IronPort's reactive spam and virus scanning engines. Through policies in the Email Security Manager you determine which messages get scanned. Remember that in many cases, messages containing security threats have already been blocked by the preventive reputation filters above.
- **Clean messages:** These messages have been determined not to contain any security threats, and are then delivered to your internal groupware servers.

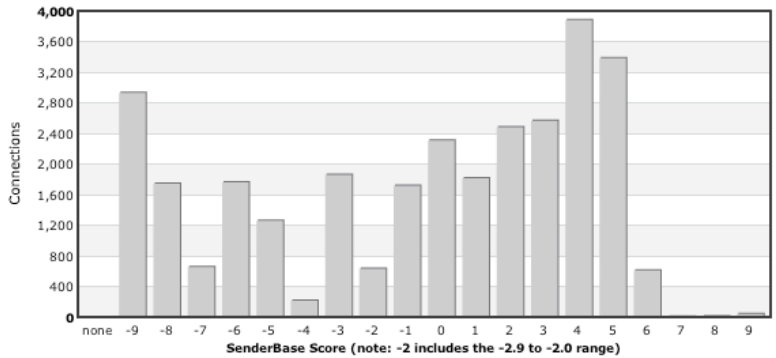
Messages

Blocked by Reputation	7,692
Spam Messages	6,017
Virus Messages	272
Clean Messages	7,938

Reputation Filtering

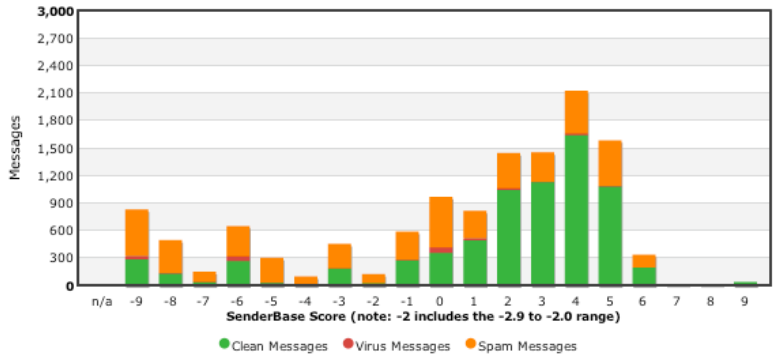
IronPort Reputation Filters provide the outer layer of defense for your email infrastructure. As the IronPort appliance receives inbound mail, it performs a threat assessment of the sender and assigns a proprietary SenderBase Reputation Score (SBRS). Suspicious senders are throttled or blocked while recognized senders, such as customers or business partners, are allowed access. Your IronPort appliance's response is determined by mail flow policies configured in the Host Access Table.

Connections by SenderBase Score



The 'Connections by SenderBase Reputation Score' graph provides a view of the total connections made to your IronPort appliance associated with each senders' SBRS scores. The 'Messages by SenderBase Reputation Score' provides a view into messages actually processed by the appliance, via mail policies and filters.

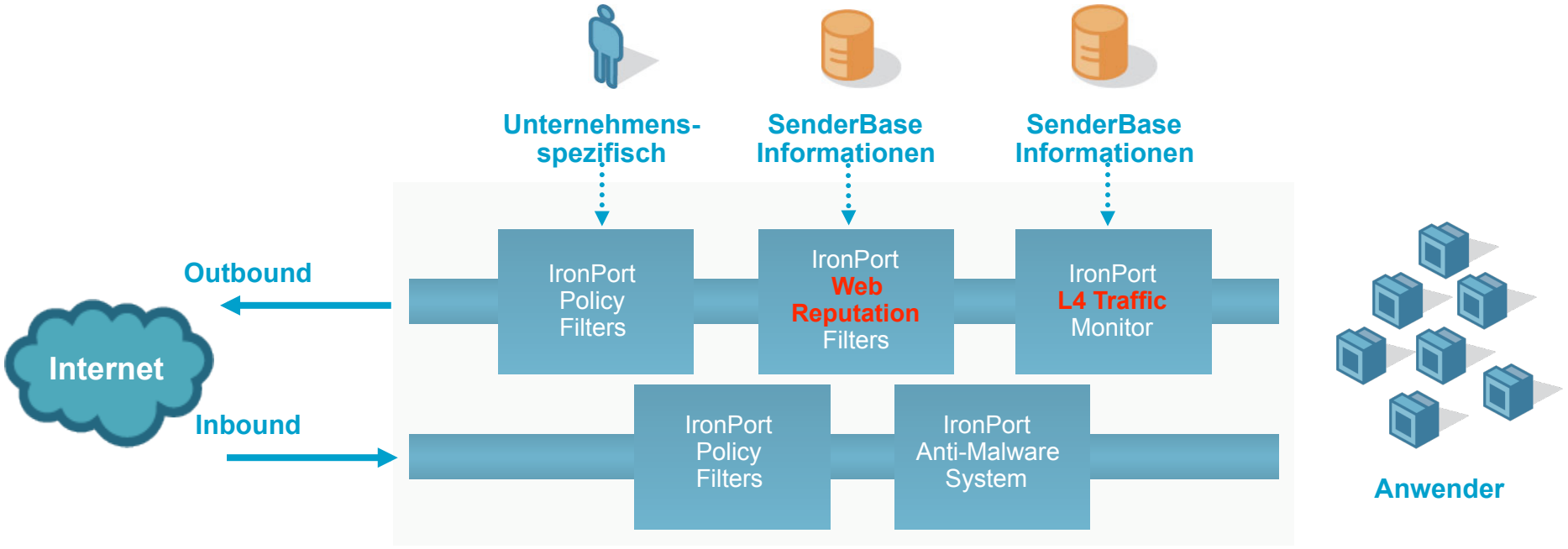
Messages by SenderBase Score



By contrasting the two graphs, you can see that:

- The portions of the 'Messages by SenderBase Reputation Score' graph where blocking is used and no messages are displayed demonstrates the effectiveness of the IronPort appliances's preventative reputation filters. These filters reduce the traffic load on the appliance by blocking connections to the appliance by disreputable senders - enhancing the availability of your email, even during heavy virus or spam outbreaks.
- The majority of email sent by senders with a lower SBRS (less than 0) but not blocked on connection, is identified as spam. As you become comfortable with the veracity of SenderBase Reputation scoring, you can fine-tune your mail policies to block more email at the SMTP connection.
- Generally, a SBRS of 'None' is assigned to newer IP addresses where no information exists from the SenderBase Reputation Service to make an accurate assessment of the sender's reputation.

HTTP-Transaktionen
Multi-Layer & Multi-Vendor



Web Security Manager™
Umsetzung von Unternehmens-Richtlinien

Web Filtering Policies

Policies

Add Group...

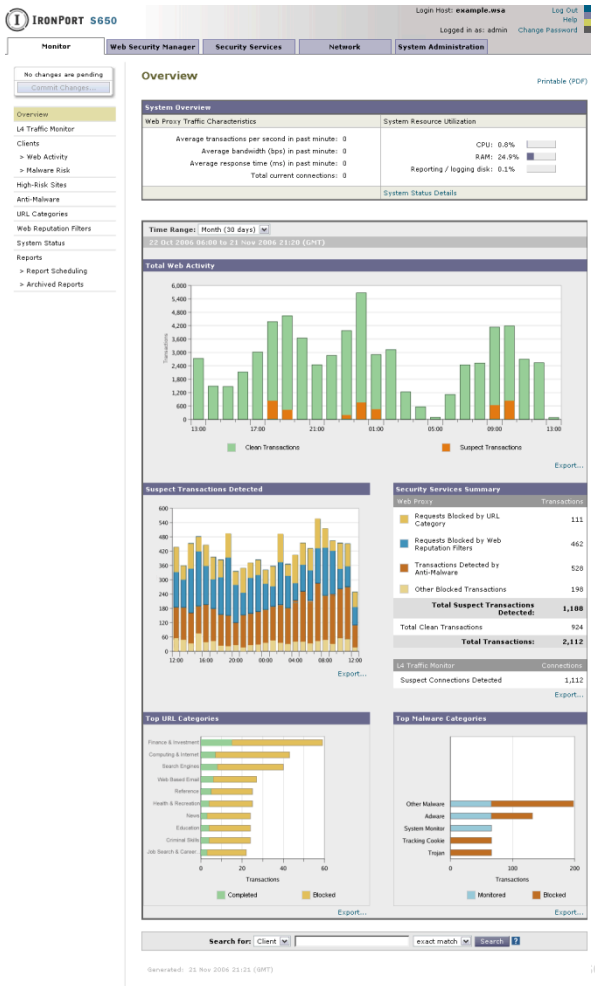
Order	Group	Applications	URL Categories	Objects	Anti-Malware	Delete
1	**QA**	Block: FTP Block: User Agents	Block: 52 Monitor: 2 Allow: 0	Block: 256 Mb	(global policy)	
2	**Engineering**	Block: User Agents	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(disabled)	
3	**Marketing**	(disabled)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 11 Monitor: 2	
4	**Dev**	(global policy)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size	(global policy)	
	Global Policy	Block: FTP, HTTPS Allow: HTTP Block: User Agents Allow: Ports 443, 21	Block: 46 Monitor: 8 Allow: 0	Block: 256 Mb Block: Object Types Block: File Types	Block: 13 Monitor: 0	

Key: Global Disabled
Authentication

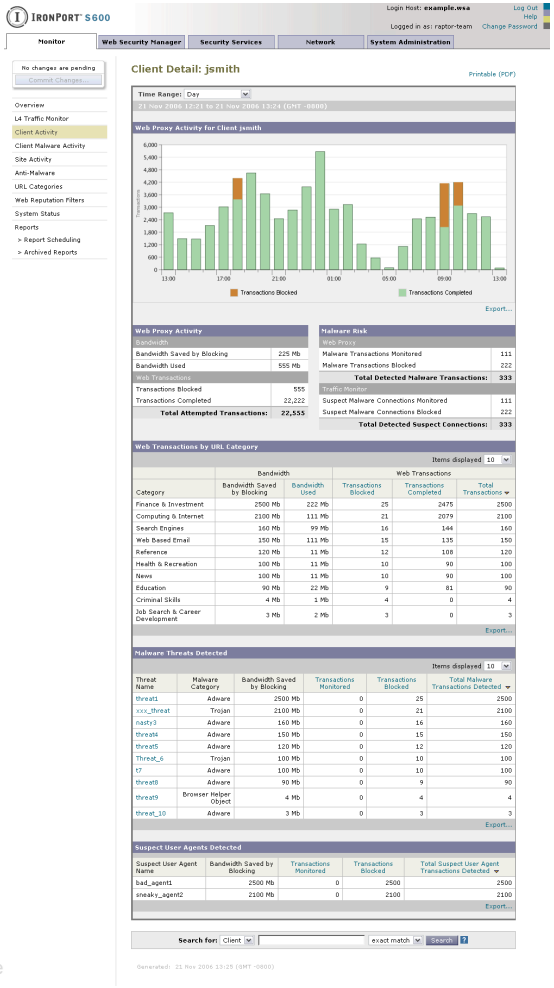
Web Security Monitor™

Überwachung von Unternehmens-Richtlinien

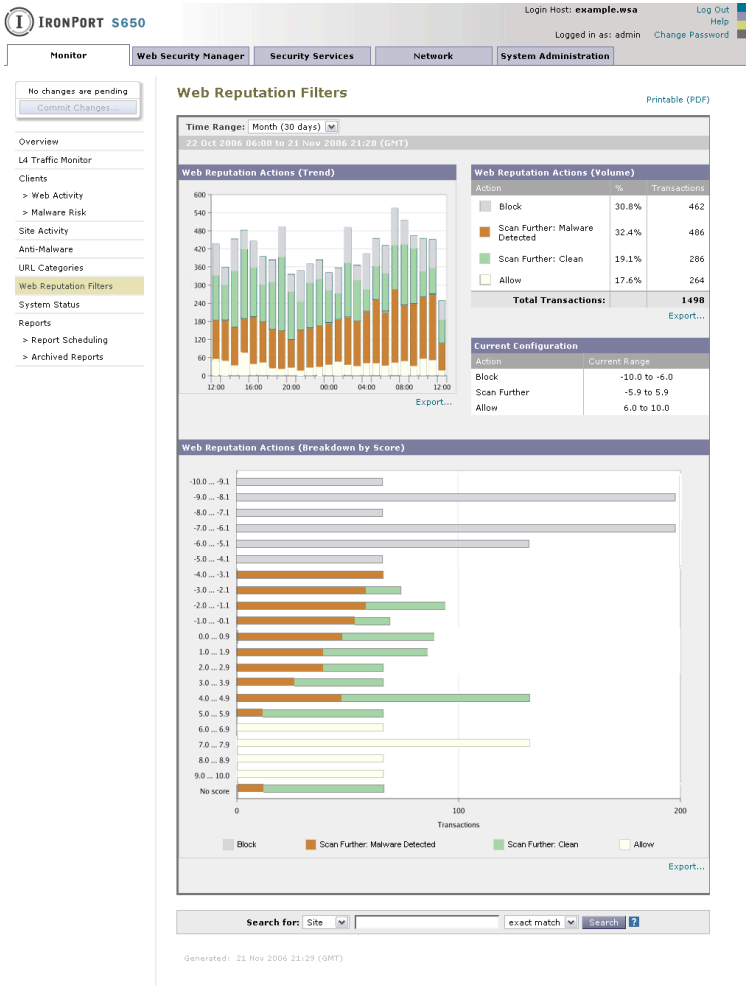
System Overview



Client Detail



Web Reputation



Q & A