



Astaro Internet Security  
Simplifying Email, Web & Network Protection

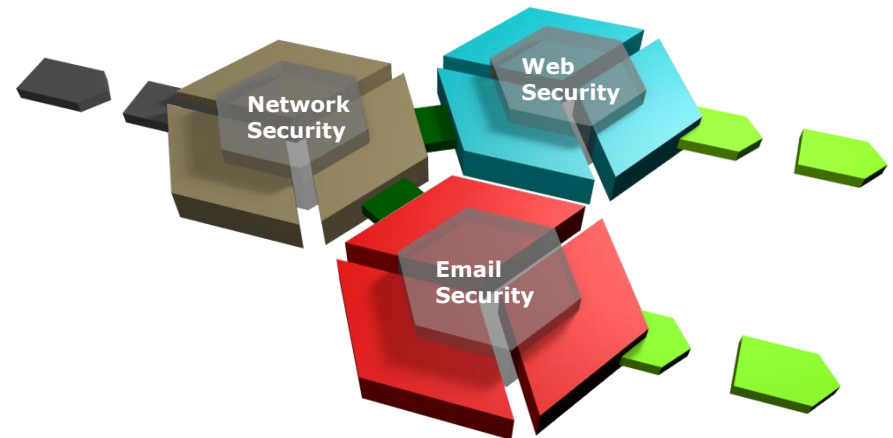
## Astaro Internet Security Atlanta Data Connectors



Bill Prout  
Application Engineer  
Astaro Internet Security  
Phone: 781-345-5000  
Fax: 781-345-5100  
Email: [bprout@astaro.com](mailto:bprout@astaro.com)  
Website: [www.astaro.com](http://www.astaro.com)

# Topics

Astaro Company Profile  
The Security Challenge  
Vulnerability Points  
Network Security Technologies  
Additional Resources



# Astaro Company Profile

## #1 Supplier of Open Source Based Security Software

- Protecting 30,000+ networks in over 60 countries



## Global Presence

- Established in 2000
- Headquarters in Boston, MA and Karlsruhe, Germany
- 400+ solutions partners worldwide

## Award-Winning Software

- Astaro Security Gateway - Nine integrated network security applications and management platform
- Robust for Today, Scalable for Tomorrow!
- Extensive features
- Excellent quality
- Easy to deploy and manage
- Available on appliances or as software



# Recognition



Common Criteria Arrangement



**SC Magazine “Best of 2006”**

**Common Criteria Certified - 2006**

**Firewall ICSA Labs Certified**



**Product of the Year 2005**  
- CRN

**Best of the Year 2004 / 2005**  
- PC Magazine



**Best of 2005**  
**5 star rating & SC Magazine**  
**“Best Buy”**  
- SC Magazine

**Up-to-Spec Certified**  
- The Tolly Group

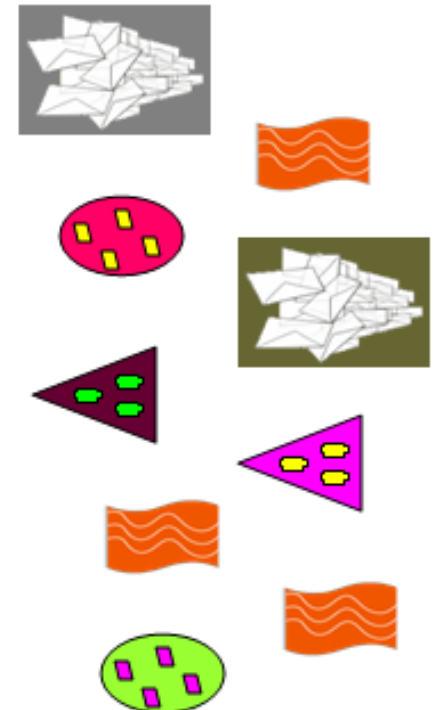
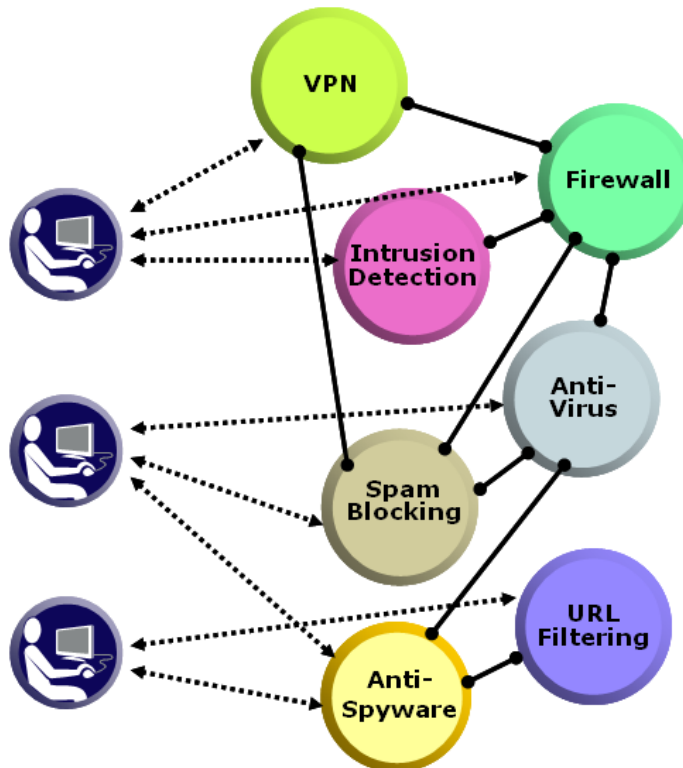
# The Network Security Challenge

Difficult to Deploy and Manage

Expense to Maintain (People and System)

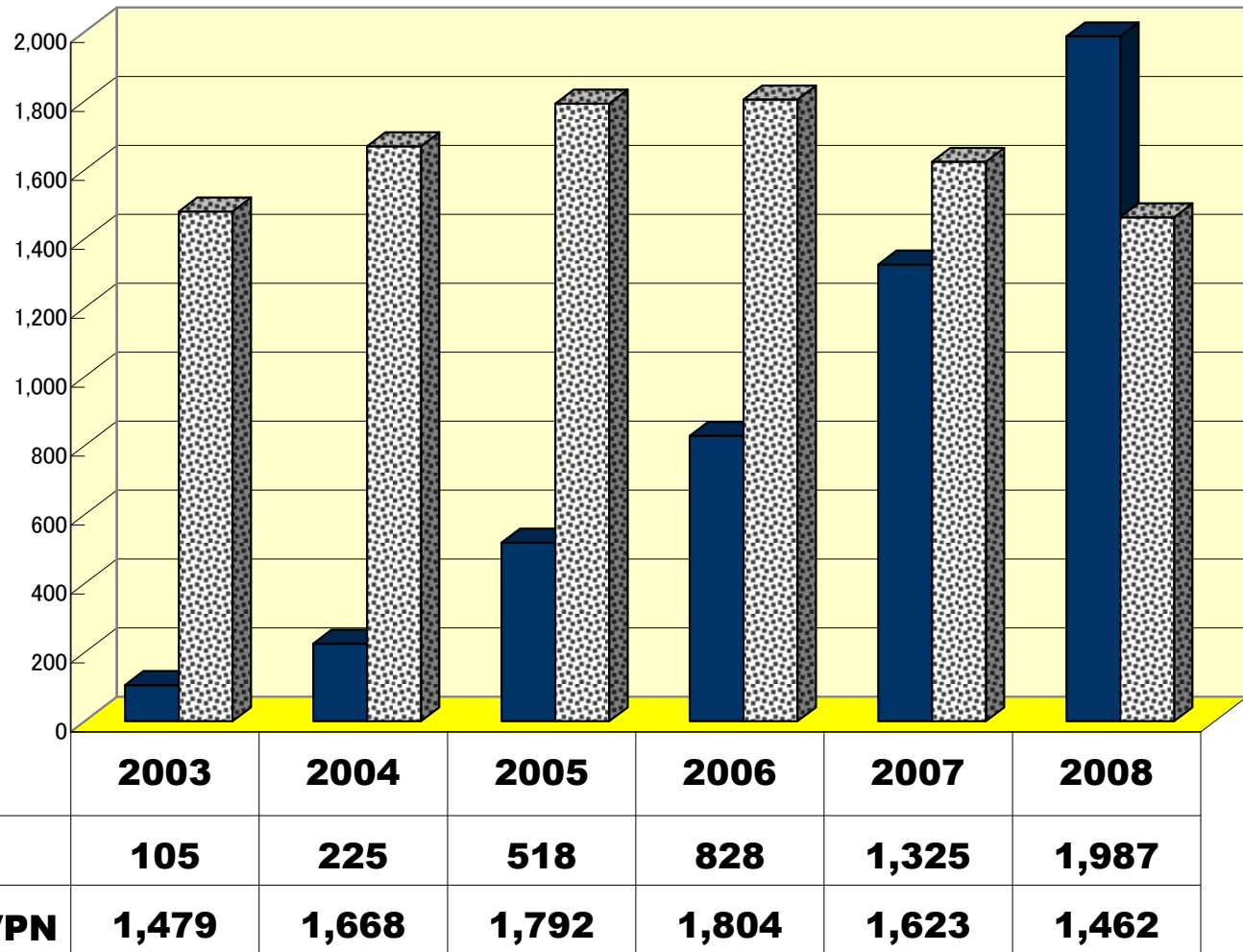
Ongoing and Emerging Threats

- ∞ Evaluate
- ∞ Purchase
- ∞ Train
- ∞ Install
- ∞ Integrate
- ∞ Configure
- ∞ Manage
- ∞ Update



# Worldwide UTM Appliances vs. FW/VPN Forecast 2003-2008 (IDC)

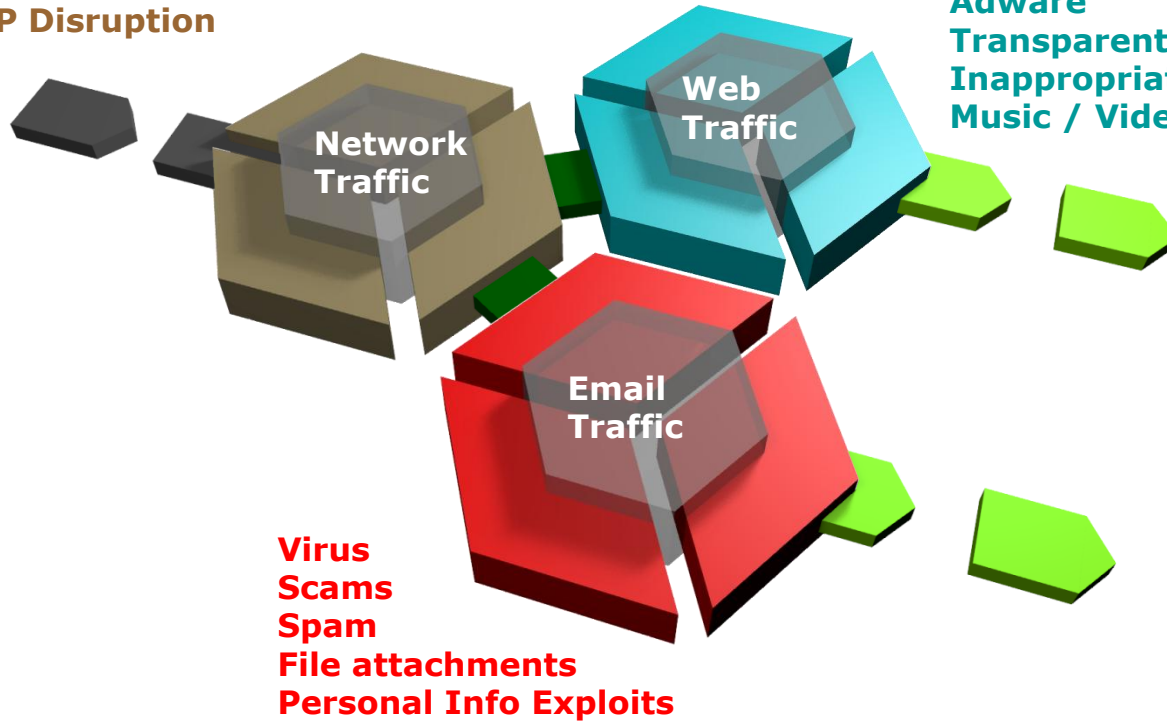
UTM (Unified Threat Management) Shipments are on the rise. Single function security devices have reached a peak. Security stance can be improved and budget savings achieved by centralizing network protection mechanisms by deploying multi function solutions such as the Astaro Security Gateway.



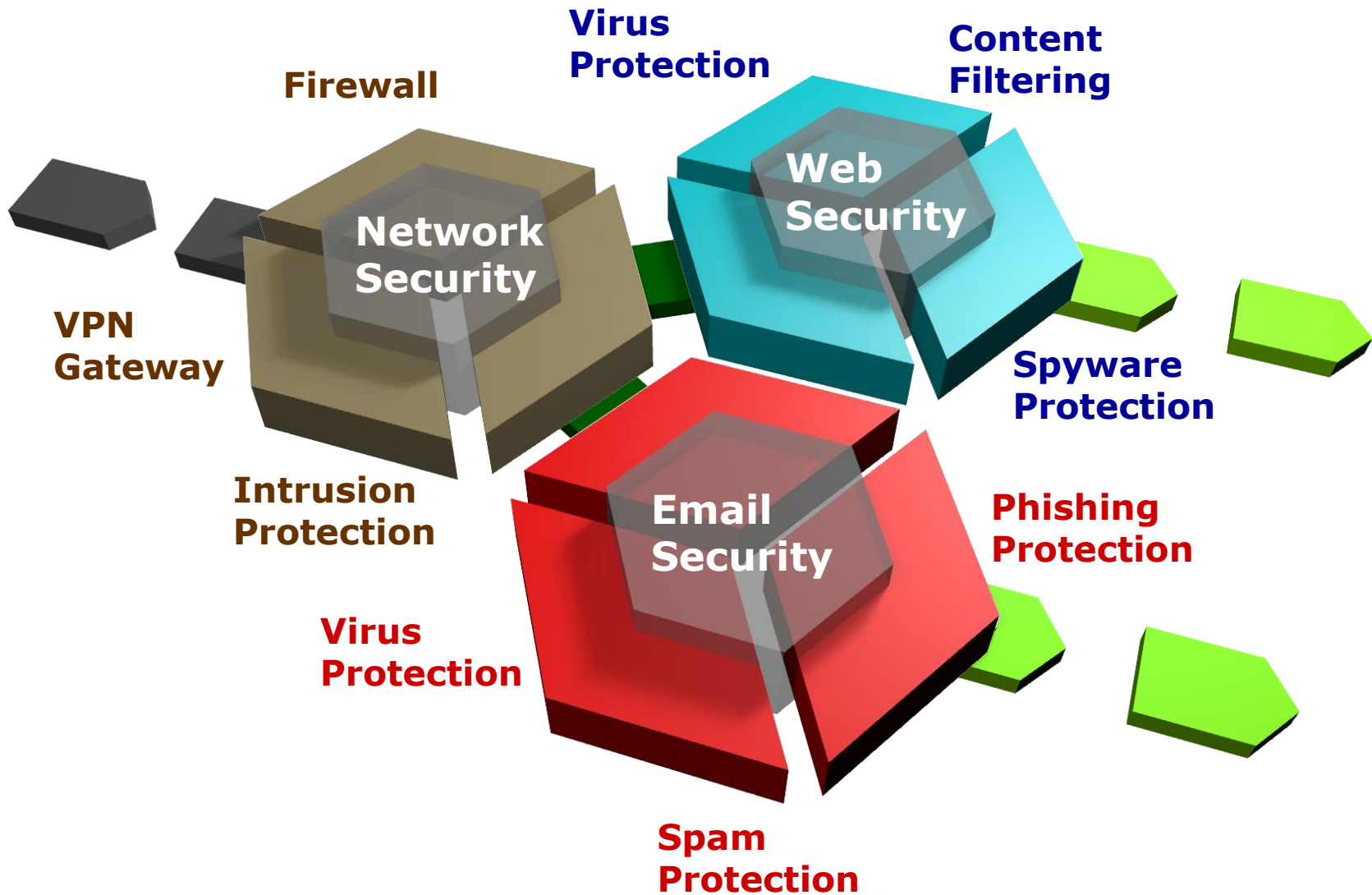
# Major Vulnerability Points

**Hack Attacks**  
**Attack traffic**  
**Connection Hijacking**  
**Denial of Service**  
**Probes**  
**VOIP Disruption**

**Virus**  
**Spyware**  
**Adware**  
**Transparent proxies**  
**Inappropriate Web Surfing**  
**Music / Video downloads**



# Network Perimeter Technologies



# Network Security Technologies

**Firewall** with stateful packet inspection and application-level proxies, guards Internet communications traffic in and out of the organization.

**Intrusion Protection** detects and blocks probes and application-based attacks using heuristics, anomaly detection, and pattern-based techniques.

**Virtual Private Network Gateway** assures secure communications with remote offices and “road Warriors”.

# Key Network Security Functions

## Stateful Packet Inspection Firewall

- Packet filtering – inspects packet headers
- Stateful packet inspection – tracks events across a session to detect violations of normal processes
- Time-based rules and Policy-based routing

## Application-Level Deep Packet Filtering

- Scans packet payloads to enforce protocol-specific rules

## Security proxies to simplify management

- HTTP, POP3, SMTP, SIP, DNS, Socks, Ident

## NAT (Network Address Translation) and masquerading

## DoS (Denial of Service Attack) protection

## Transparent mode for High Availability / DR



# Intrusion Protection Functions

**Identify and Block Application related probes and attacks**

**Identify and Blocks Protocol related probes and attacks**

**Large Database (6,400) of IPS patterns and rules**

- Probing, port scans, interrogations, host sweeps
- Attacks on application vulnerabilities
- Protocol exploitations
- Messaging, chat and peer-to-peer (P2P) activities

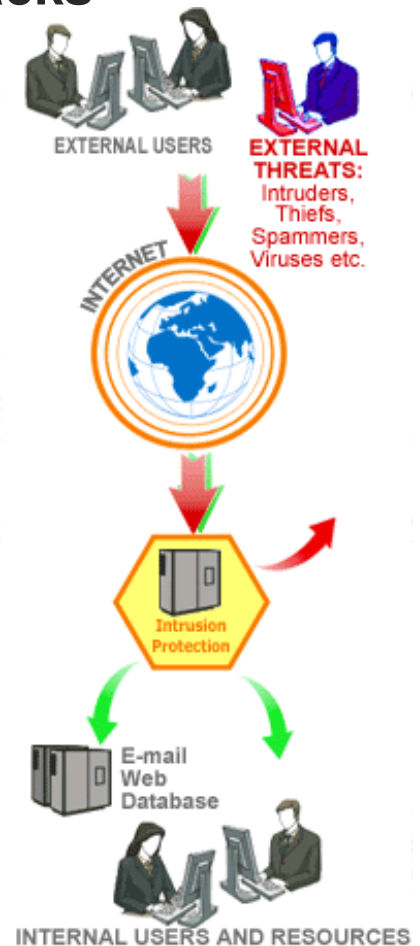
**Anomaly detection prevents “Zero-Day-Attacks”**

**Intrusion detection and prevention**

- Notify administrator, or block traffic immediately

**Integrated Management Interface**

- One click to enable and disable rules, change between detection and prevention



# VPN Gateway Functions

**Encrypts data to create a secure private communications “tunnel” over the public Internet**

**Support multiple architectures**

- Net-to-Net, Host-to-Net, Host-to-Host

**Advanced encryption**

- Support all major encryption methods  
(AES (128/192/256 Bit) 3DES, DES, Blowfish, RSA, etc.)

**Support SSL, IPSec, L2TP, and PPTP VPNs**

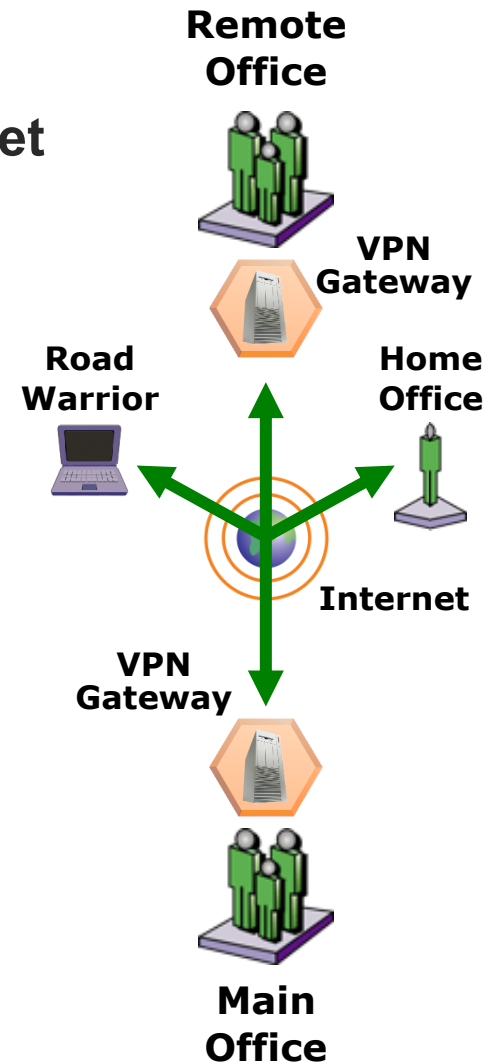
- Windows, MacOS x clients, IPSec, etc.

**Many Authentication methods**

**Internal certificate authority**

- Full Public Key Infrastructure (PKI) support

**Supports DynDNS based VPN tunnels**



# Web Security Technologies

**Spyware Protection** blocks incoming spyware, adware and other malicious applications, and prevents them from sending out confidential information.

**Virus Protection for the Web** defends computers against virus infections from web downloads and web-based email.

**Content Filtering** blocks Internet access to numerous categories of web sites during working hours.

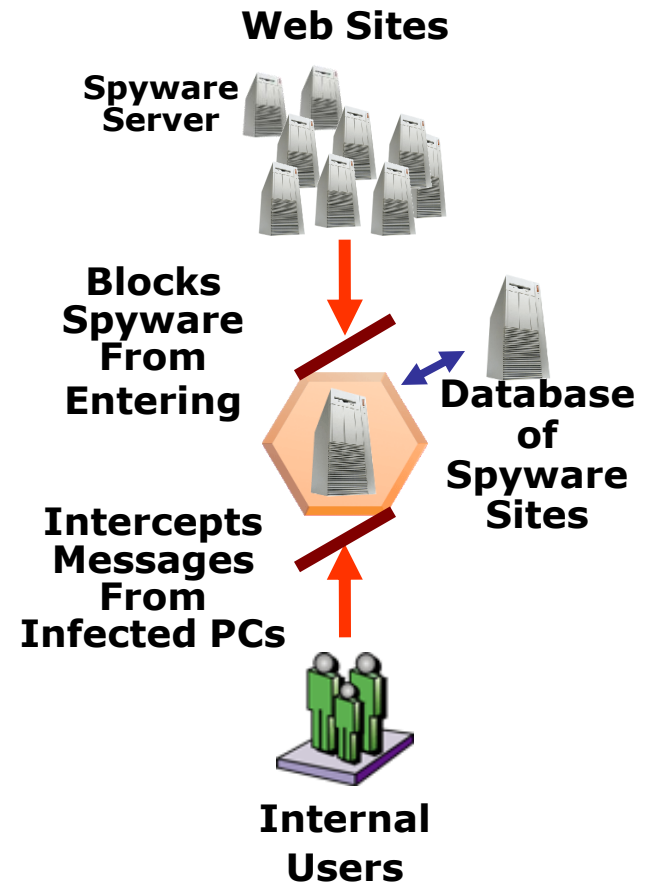
# Spyware Protection

Block downloads of spyware, adware, and other malicious software

Prevent infected systems from sending information back to the spyware server

Ability to Query against a large database of known Spyware URLs

Gateway spyware blocking complements desktop anti-spyware tools



# Anti Virus Protection for Web Traffic

Block viruses, worms, trojans, and other “malware” before they reach desktops

Scan HTTP traffic

- Web downloads
- Web-based email (MSN Hotmail, Yahoo! Mail)

Multiple virus scanners with multiple detection methods

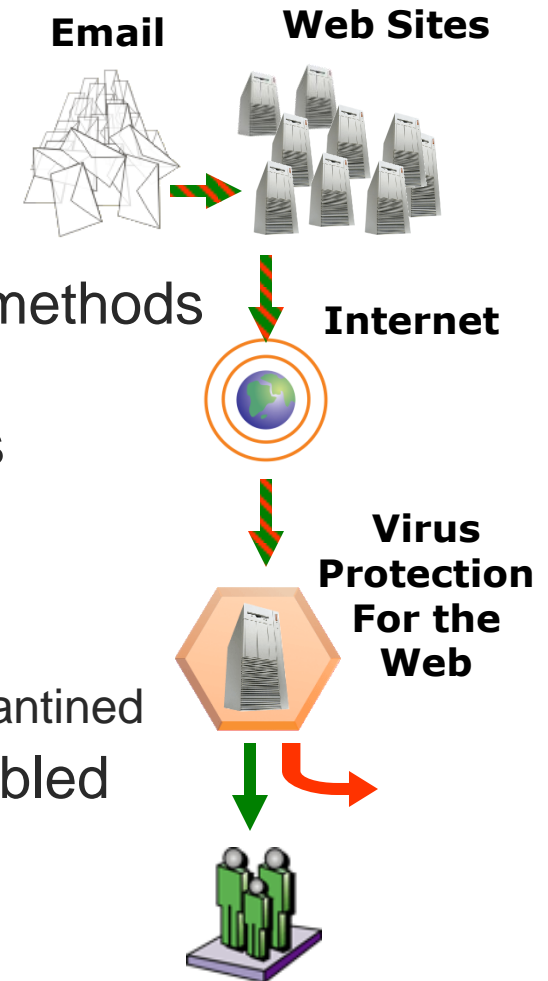
- Virus signatures, heuristics, code emulation

Large Database (300,000+) of Virus Signatures

Flexible management

- Specify file formats and text strings to block
- Emails and attachments can be dropped, rejected with message to sender, passed with a warning, quarantined

Ability to Scan downloaded Files in their assembled state.



# Content Filtering (URL Blocking) Technology

Ability to enforce policies on appropriate use of the web

Administrators can define web use policies based on

Enhanced Category Selection (60) of web sites

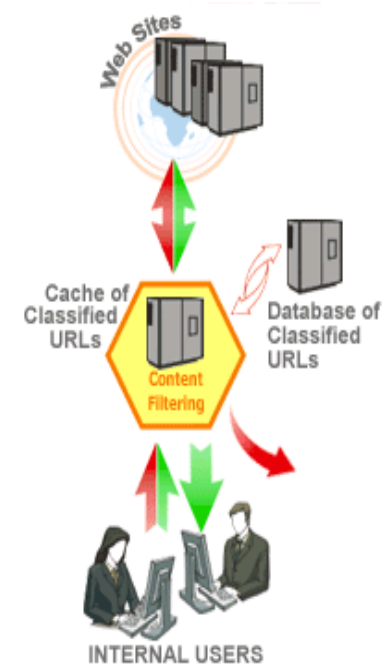
- Nudity, gambling, criminal activities, shopping, drugs, job search, sports, entertainment, etc.

Compare requests to Large (60M+)URL Database

- Sophisticated classification techniques – text classification, recognition of symbols and logos, flesh tone analysis, comparison with similar images
- Caching requests accelerates requests

Whitelists and Blacklists for Safety Net / Custom Use.

Ability to Measure and Report on activities, or actively block inappropriate URLs



# Content Filtering Success Factors

## Accuracy:

- If a filter misses web sites that should be blocked is known as “Underblocking”  
    “Underblocking” results in ineffective policy enforcement defeating the purpose of the solution.
- If a filter blocks a web site that does not violate policy is known as “Overblocking”  
    “Overblocking” may cause user dissatisfaction and productivity losses.

## Performance:

- Organizations and End users require a solution that ensures performance of each Application Session while ensuring Policy Compliance.

# Content Classification Techniques

## Manual:

### Advantages:

- Human intervention

### Disadvantages:

- Cannot classify the large and growing mass of internet
- Cannot keep up with changes in web site content
- Expensive
- Multi Language support if problematic

## Automatic:

### Advantages:

- Sites can be examined and reexamined rapidly.
- Classification of a large number of sites in multiple languages is possible.

### Disadvantages:

- Automated classification technology is complex.

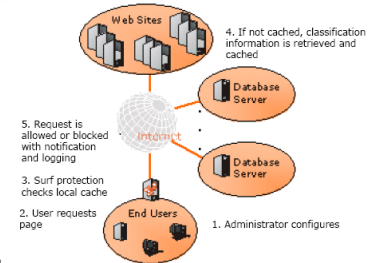
# Content Filtering Technologies

## Dynamic Filters:

- Attempts to Analyze requested Web content “on-the-fly”.
- Run time filtering is challenged by CPU power required to accurately analyze, categorize, and then compare to Policy before displaying content
- Will have difficulty in analyzing text embedded within graphics and sophisticated requirements such as flesh-tone analysis.
- Architecture suffers from excessive Overblocking and Underblocking
- Delays in displaying content to the User is not tolerated.

## Database Filters:

- All Content is analyzed and categorized by an enormous Web Crawling Server Farm.
- Overblocking and Underblocking is resolved by pre-analyzing Web Content.
- Performance is enhanced by a simple address lookup.
- Users experience consistent Content Delivery according to defined Security Policy.



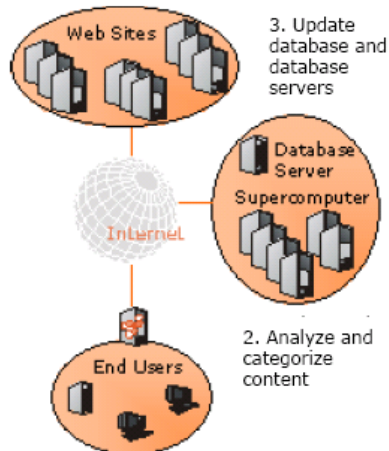
Implementing Web Filtering With Astaro Surf Protection

# Content Filtering Process

- Acquire Content from the web
- Analyze and Categorize Content
- Update Database and Database Servers

## Content Filtering Process Used By Astaro Surf Protection

1. Acquire content from Web



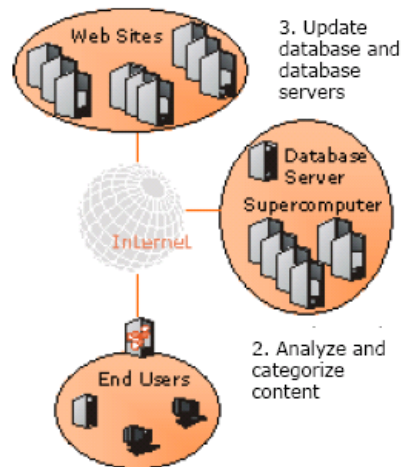
# Content Filtering Process

## Acquire Content from the web

- Supercrawler scans new/updated internet sites including Public Host Lists, domain registry information, hot links from other sites and customer feedback.
- Downloads all HTML text and Images from each sites.
- All Hyperlinks are followed and downloads all content until no-unknown links exist.
- Parallel Webcrawlers target both New and Existing Web Content
- Websites that are changed move often are crawled more often.

### Content Filtering Process Used By Astaro Surf Protection

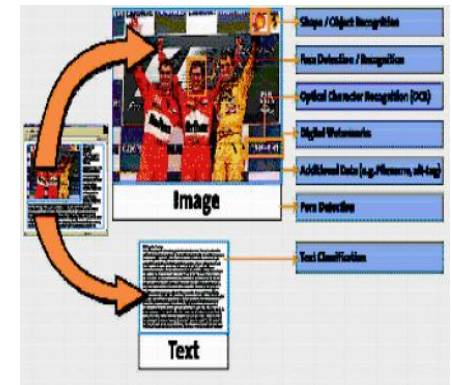
1. Acquire content from Web



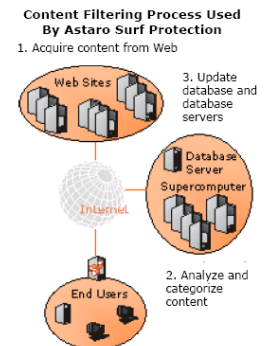
# Content Filtering Process

## Analyze and Categorize Content

- Content Analysis
- Text Classification
  - Keyword Searching, Intelligent text classification, and Word Heuristics
- Visual Porn Detection
  - Image Analysis, Face Recognition, Flesh Definition, Flesh Tone Detection
- Visual Object Recognition
  - Symbol Detection (Logos, Brands, Trademarks, Political, etc)
- Visual Object Character Recognition
  - Embedded Text / Photo Titles
- After factoring the above and other sophisticated techniques content assigned to a specific Category.



## Update Database and Database Servers



# Email Security Technologies

**Virus Protection for Email** catches viruses in SMTP and POP3 emails and attachments, even in compressed and archived formats.

**Spam Protection** uses eight different techniques to filter out spam without stopping legitimate emails.

**Phishing Protection** blocks emails from criminals trying to trick users into revealing confidential information.

# Anti Virus Protection for Email

Block viruses, worms, trojans, and other “malware” before they reach email servers or desktops

Scan SMTP and POP3 traffic

Multiple Virus scanners with multiple detection methods

- Virus signatures, heuristics, code emulation

Large Database (300,000+) of Virus Signatures

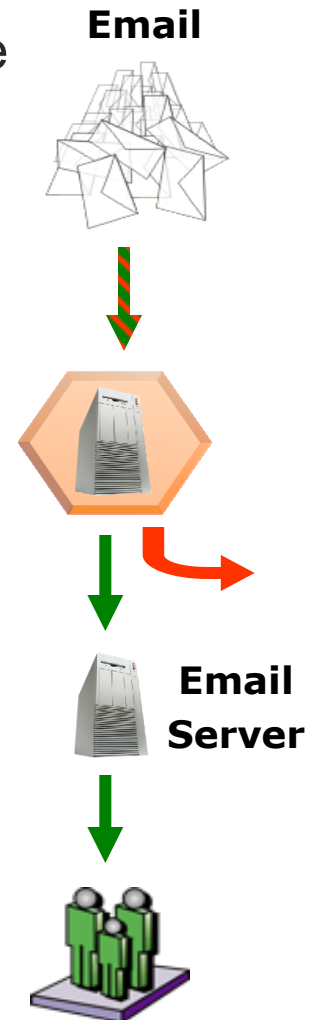
Flexible management

- Specify file formats and text strings to block
- Emails and attachments can be dropped, rejected with message to sender, passed with a warning, quarantined

Gateway virus protection supplements desktop virus scanning!

Ability to Scan Files in their assembled state

Alert end-user when infected messages are quarantined.



# Spam Protection Technology

Identify and Dispose of unsolicited emails (spam)

Multiple methods to identify spam

- Sender address verification, Realtime Blackhole Lists, header and text analysis, whitelists, blacklists, URL scanning, greylisting

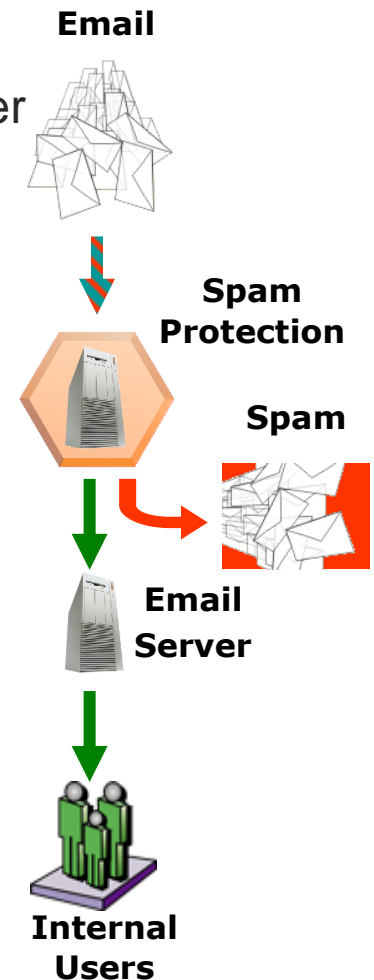
Flexible Rating System with Multiple Thresholds (Scoring)

- Quarantine or Simply reject if defined Thresholds are breached.

Flexible / Easy to Manage

- Emails and attachments can be dropped, rejected with message to sender, passed with a warning, or quarantined
- User can release messages from quarantine queue

Attaching headers to messages allow the email server to take additional actions (x-spam flag, x-spam-score, etc)



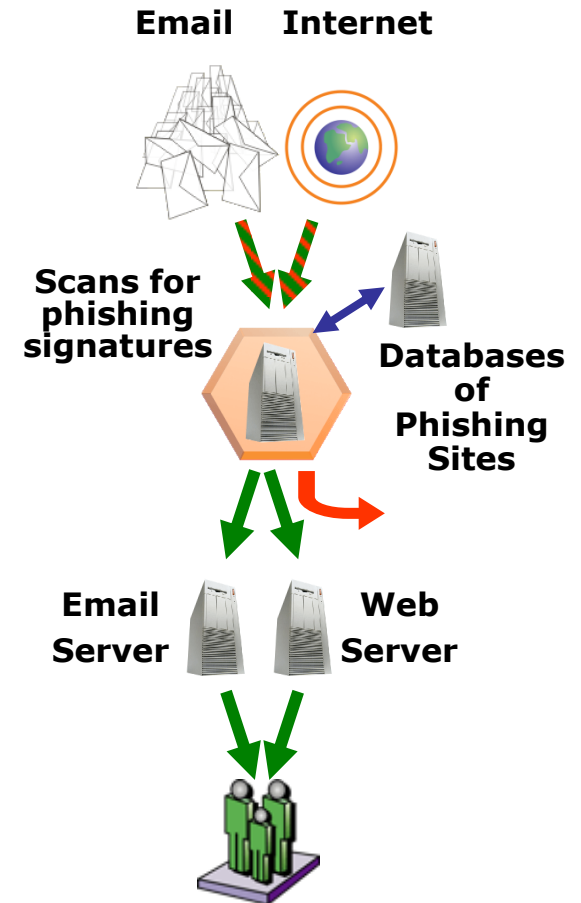
# Protection Against “Phishing”

## “Phishing”

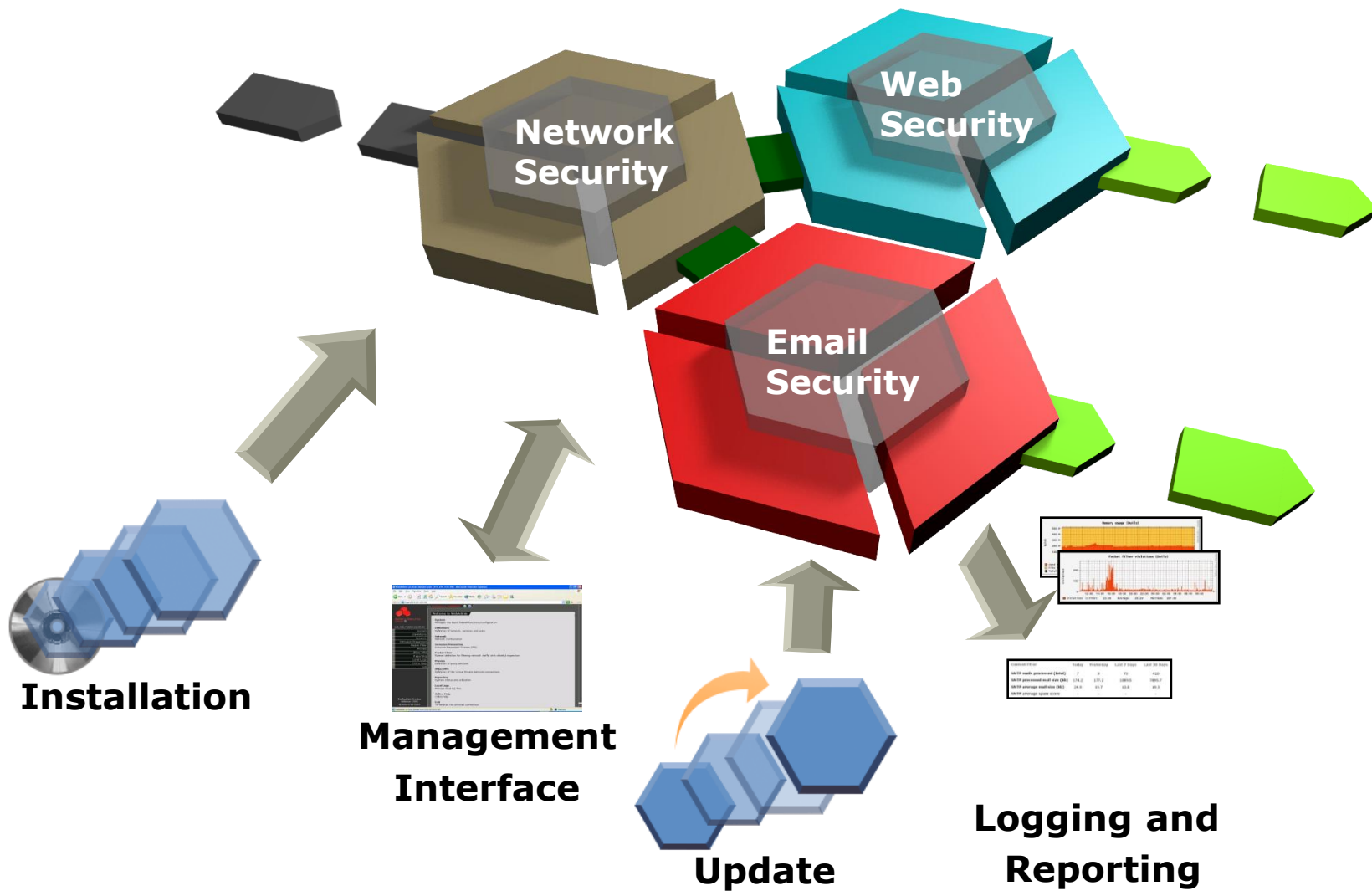
- Criminals imitate emails from banks, credit card companies, eBay and other sources to obtain confidential user information

## Block “Phishing” attempts with multiple technologies.






- Virus scanner identifies phishing signatures
- URL filtering database captures phishing servers in the “suspicious” category
- Content downloaded from web sites will be blocked if it matches patterns of phishing content



# Integrated Management and Control



# Astaro Security Gateway Appliances

	Astaro Security Gateway 110/120	Astaro Security Gateway 220	Astaro Security Gateway 320	Astaro Security Gateway 425	Astaro Security Gateway 525/525F
					
<b>Environments</b>	Small Campus/Business	Small / Medium Campus/Business	Medium Campus/Business	Medium / Large Campus/Business	Large Campus/Business
<b>Hardware specs</b>	177(w) x 43 (H) x 228.6 (D) mm VIA C3 800MHZ+ / Eden 667MHZ 256 MB memory 20 GB internal HD 3 Ethernet Ports	1 U - 426(W) x 305 (D) x 43.5(H) mm Intel Pentium III processor 1.2GHz 512MB SDRAM 40 GB Internal HD 8 x 10/100 Base-TX ports	1 U - 426(W) x 380(D) x 43.5(H) mm Intel Pentium 4 processor 2.4GHz 1 Gig DDR RAM 80 GB internal HD 4 x 10/100 Base-TX ports 4 x Gigabit Base-TX port	1 U - 426(W) x 432(D) x 43.5(H) mm Intel Pentium 4 processor 3.4GHz 2 Gig DDR RAM 74 GB internal HD S-ATA 4 x Gigabit ports – PCI bus 4 x Gigabit ports – PCI Express bus Hardware acceleration card	2 U - 426(W) x 460(D) x 88(H) mm Dual Intel Xeon processors 3.2GHz 4 Gig DDR RAM 2* 120GB internal HD S-ATA (RAID1) <sup>1)</sup> 10 x Gigabit ports – PCI Express bus - 525: 10 x Copper - 525F: 4 x Copper/6 x SFP Hardware acceleration card Redundant Power Supplies <sup>1)</sup>
<b>Performance Firewall (Mbps)</b> <b>VPN (Mbps)</b>	100 30	260 150	420 200	1,200 265	3,000 400

## Astaro Security Gateway Software

Runs on Intel-compatible PCs and servers



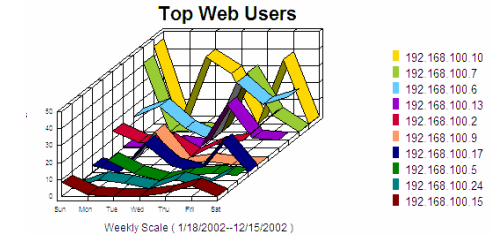
1) hot-swappable

# Complimentary Astaro Products



Astaro  
Report  
Manager

A centralized security reporting engine that collects, correlates and analyzes security data.



Astaro  
Command  
Center

An application for centralized management and real-time monitoring of installations with multiple ASG appliances



Astaro  
Secure  
Client

An advanced IPSec VPN client with personal firewall and integrated dialer.



# Free Evaluation options

## 14 DAY Appliance Evaluation



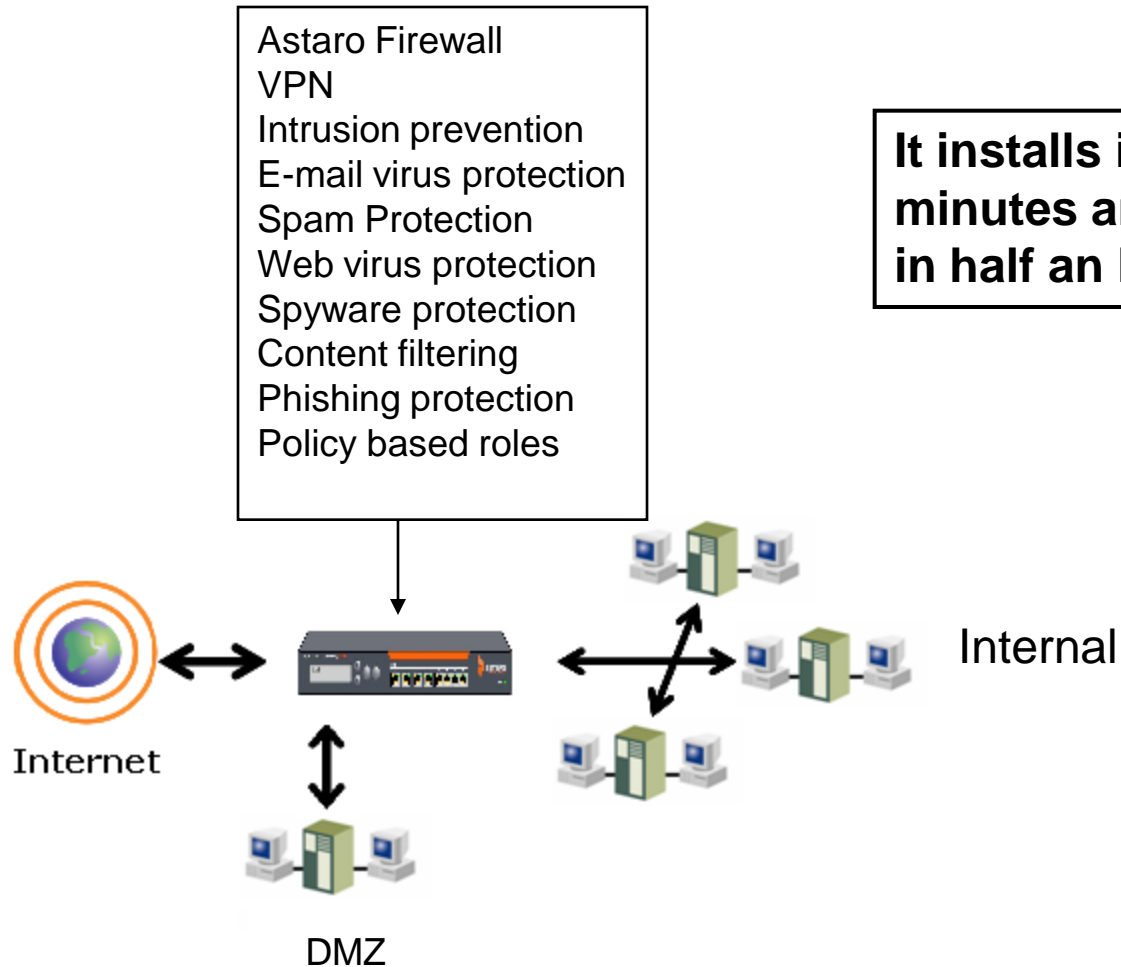
**FREE TRIAL**

FULL-FEATURED SOFTWARE FOR  
A 30-DAY EVALUATION

**DOWNLOAD  
NOW!**

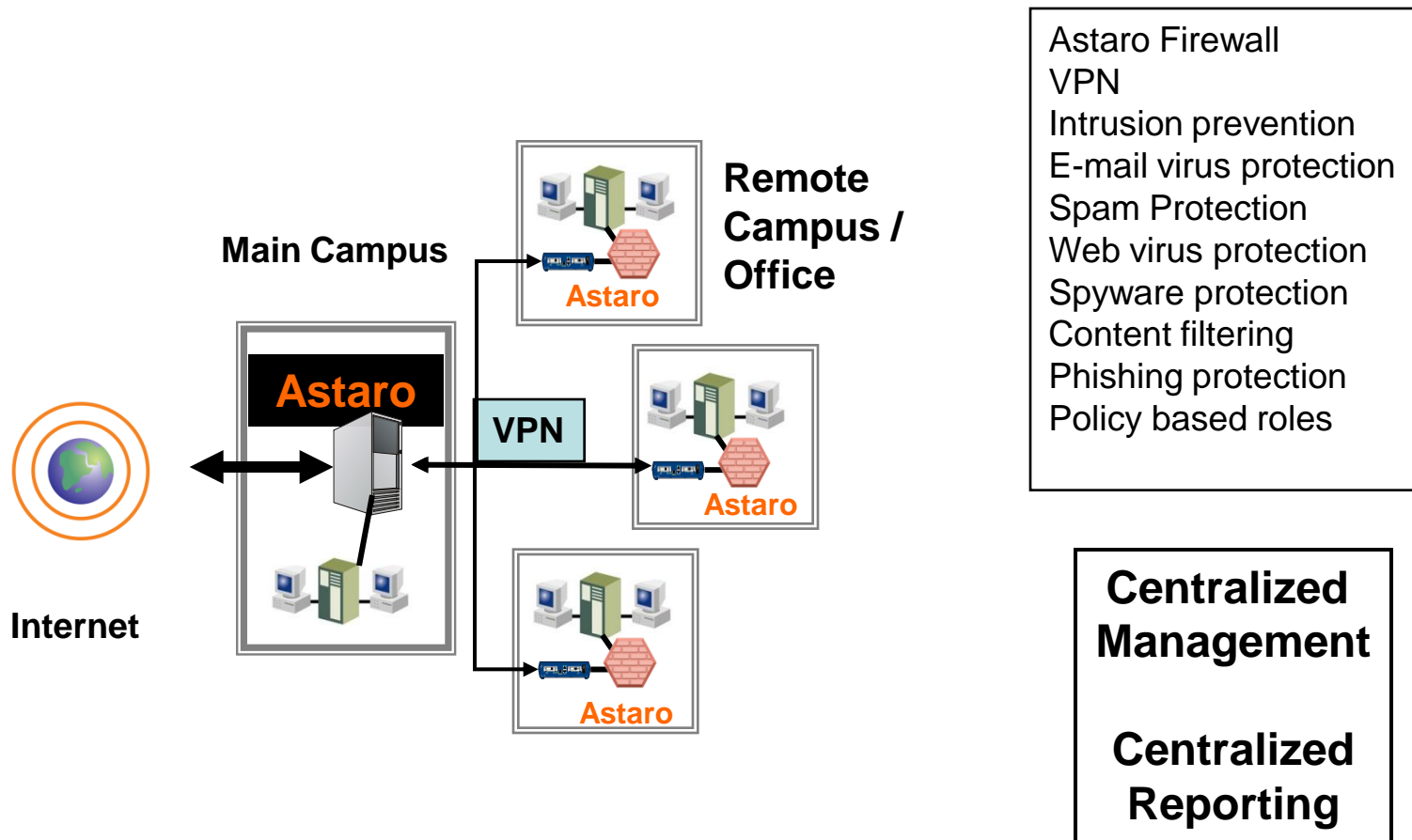
QUICK DOWNLOAD, 15-MINUTE INSTALLATION

# Sample Deployment



**It installs in less than 15 minutes and is activated in half an hour.**

# Main Campus / Remote Site

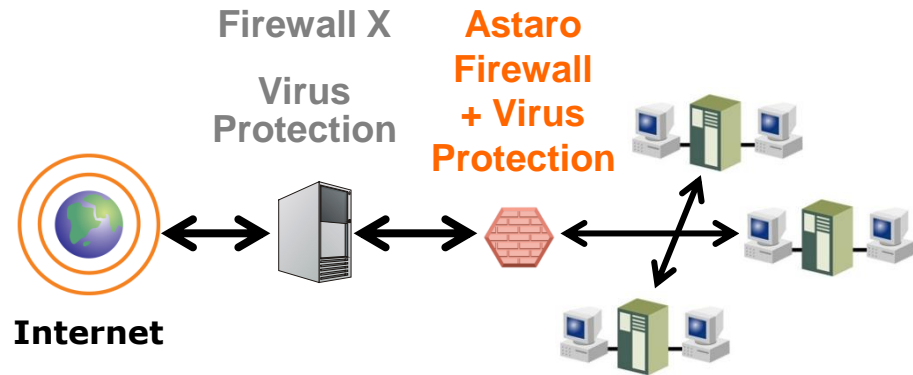


# Working with other vendors

## Using best practices

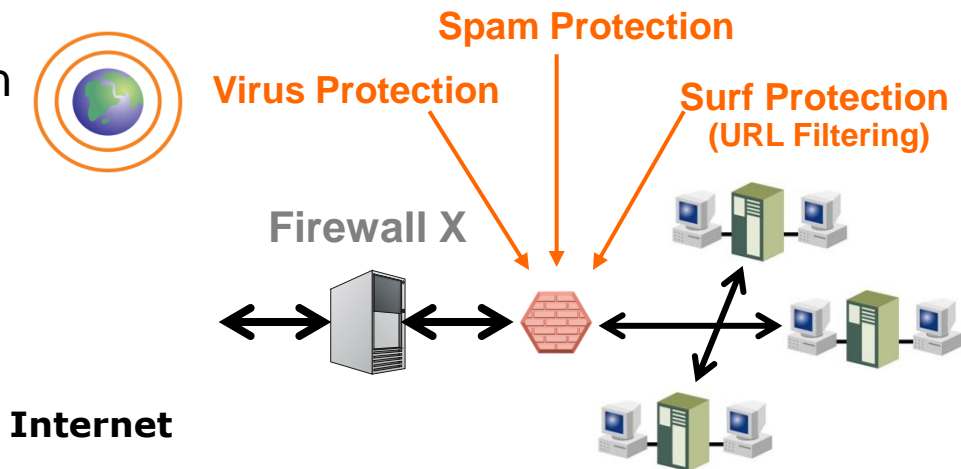
### *Duel firewalls - Duel Vendors*

- Redundancy
- Seamless failover
- Independent reporting



## Optimized Appliance for:

- Intrusion detection & Prevention
- Spam & Virus filters
- Wireless firewall
- Content filtering
- Policy based QOS
- Spyware protection
- VPN termination



# Centralized Security Enhances Organizational Value

## Enhance Security

- Block threats with complete perimeter security
- Integrated management reduces human error and increases speed of response

## Increase Productivity

- Keep systems, networks and web sites up and running
- Increase productivity by blocking spam and inappropriate web surfing



## Simplify Management

- A complete perimeter security solution that is easy to deploy, manage, and update, and that scales seamlessly from small offices to large headquarters installations.

# External Data

CSI-FBI Survey (US) <http://www.gocsi.com/>

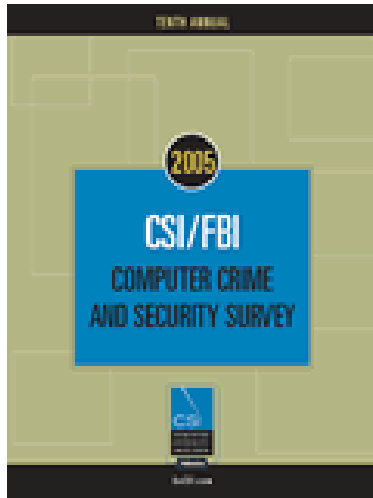
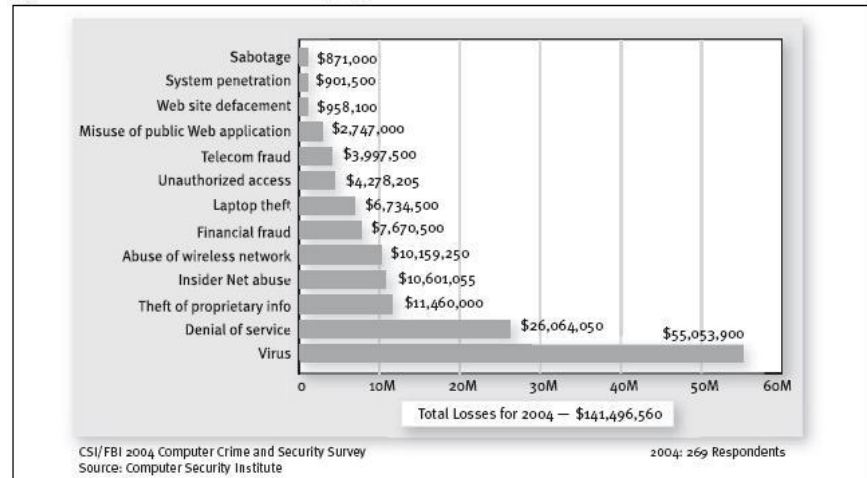


Figure 15. Dollar Amount of Losses by Type



# Resources and Education

## Security Now! Podcast

- Sponsored by Astaro

## Astaro.com

- Astaro Border Manager Migration Wiki: <http://wiki.astaro.com>
- V7 Demo Site: <https://v7demo.astaro.com/>
- Free Home Use License and Training

## SANS Institute – Internet Storm Center

- <http://isc.sans.org/>

## Computer Crime and Security Survey

- <http://www.gocsi.com>

## SearchSecurity

- <http://www.searchsecurity.com>

## US-Cert (Computer Emergency Readiness Team)

- <http://www.us-cert.gov/>

## Privacyrights.org

- <http://www.privacyrights.org/>



Dashboard
Dashboard for *Wed Mar 7 01:19:22 2007* Refresh:

- Management
- Network
- Users
- Definitions
- Network Security
- Web Security
- Email Security
- VoIP Security
- IM/P2P Security
- Site-to-site VPN
- Remote Access
- Logging
- Reporting
- Support
- Log off

**v7demo2.astaro.com**

**Model:** ASG525  
**License ID:** 000000  
**Uptime:** 0d 15h 37m

**Version information**

**Firmware version:** 7.002  
**Pattern version:** 1774  
**Last check:** 11 minutes ago

**Resource usage**

**CPU** 4%  
**RAM** 30% of 1011 MB  
**Swap** 0% of 1027 MB  
**Log Disk** 2% of 11 GB  
**Data Disk** 6% of 8 GB

**Today's threat status**

**Firewall:** 18486 packets filtered  
**IPS:** 0 attacks blocked  
**Anti-Virus:** 0 items blocked  
**Anti-Spam:** 0 emails blocked  
**Anti-Spyware:** 0 items blocked  
**Web Filter:** 0 URLs filtered

**Current system configuration**

- Firewall** is active with 0 rules
- Intrusion Protection** is inactive
- HTTP Proxy** is active, 0 requests served today
- FTP Proxy** is active
- SMTP Proxy** is active, 0 emails processed, 0 emails blocked
- POP3 Proxy** is active, 0 emails processed, 0 emails blocked
- Anti-Virus** is active for protocols HTTP,FTP,SMTP,POP3
- Anti-Spam** is active for protocols SMTP,POP3
- Anti-Spyware** is active
- Email Encryption** is active with 0 users
- Site2Site VPN** is active with 1 of 1 online tunnels
- Remote Access** is inactive
- HA/Cluster** is inactive

**Network**

Port	Name	Type	State	Link	In	Out
eth0	Internal	Ethernet	Up	Up	125.0 kB/s	5.9 kB/s
eth1	external	Cable Modem	Down	Up	0 kB/s	0 kB/s
eth2	VPN-Link	Ethernet	Up	Up	13.0 B/s	11.0 B/s
eth3	unused					

Release 7.002  
© Astaro AG 2000-2007

Done

Internet

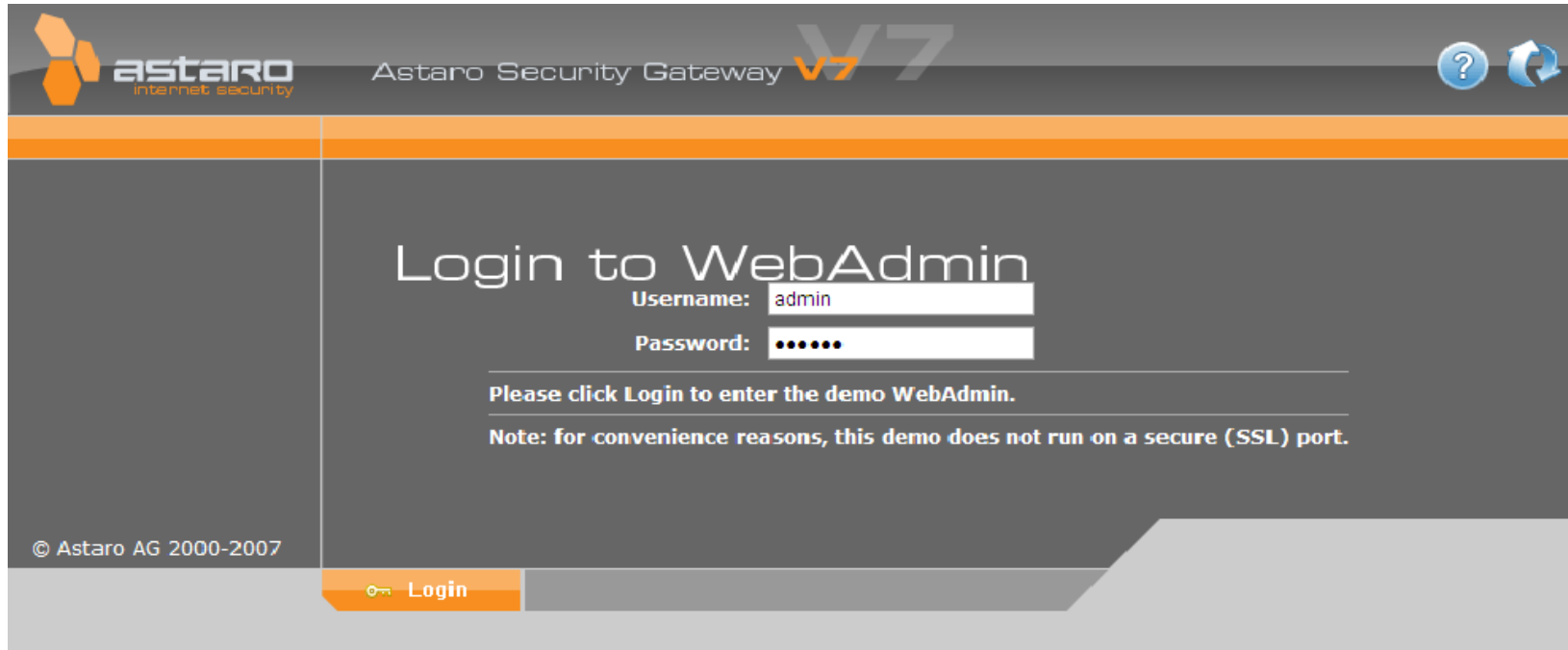
100%

Astaro Security Gateway

February 15, 2007 - Slide - 37

# Version 7.x – Demo Site

http://demo.astaro.com



The screenshot shows the login interface for the Astaro Security Gateway V7 WebAdmin. The page has a dark grey background with orange accents. At the top left is the Astaro logo (three orange hexagons) and the text "astaro internet security". To the right of the logo is "Astaro Security Gateway" and a large "V7" logo. In the top right corner, there are two circular icons: a question mark and a refresh symbol. The main content area is titled "Login to WebAdmin" in a large white font. Below the title are two input fields: "Username:" with the text "admin" and "Password:" with six black dots. Below the password field is a horizontal line, followed by the text "Please click Login to enter the demo WebAdmin." and another horizontal line. Below that is a note: "Note: for convenience reasons, this demo does not run on a secure (SSL) port." At the bottom left of the page, there is a copyright notice: "© Astaro AG 2000-2007". At the bottom center, there is an orange button with a key icon and the text "Login".

astaro  
internet security

Astaro Security Gateway V7

?

Refresh

## Login to WebAdmin

Username:

Password:


---

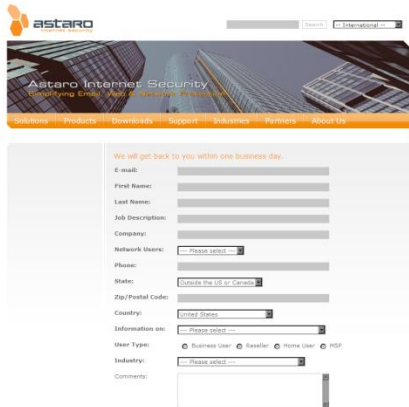
Please click **Login** to enter the demo WebAdmin.

---

**Note:** for convenience reasons, this demo does not run on a secure (SSL) port.

© Astaro AG 2000-2007

 Login



# Thank You!

To Request an Evaluation Unit, please visit:

[www.astaro.com/contact](http://www.astaro.com/contact)



Product of the Year 2005

Bill Prout  
Application Engineer  
Astaro Internet Security  
Phone: 781-345-5000  
Fax: 781-345-5100  
Email: [bprout@astaro.com](mailto:bprout@astaro.com)  
Website: [www.astaro.com](http://www.astaro.com)