



# Astaro Corporation

## Technology at the Perimeter

781-345-5000

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

### web

- Surf Protection
- Spyware Protection
- Virus Protection

### network

- Virus Protection
- Spam Protection
- Phishing Protection

### e-mail

- Firewall
- VPN
- Intrusion Protection

### security

# Agenda

- Astaro Company Profile
- The Security Challenge
- Vulnerability Points
- Network Security Architecture
- Additional Resources

# Corporate Overview

- **#1 Supplier of Open Source Based Security Software**
  - Protecting Over 30,000 Networks in over 60 countries
  - “Best of Breed” Open Source and Patented Technologies
- **Worldwide Presence**
  - Established in 2000
  - Headquartered in Karlsruhe, Germany and Burlington, MA
  - North American Support Center in Burlington, MA
  - Offices in the UK, United States, Australia and Japan
  - 1000+ Solution Providers Worldwide
- **Corporate Overview**
  - 1st to Market with UTM Solution in 2000.
  - Available as Appliances or as Software
  - Astaro Security Gateway – Integrated and Flexible approach to securing the network perimeter.
    - ✓ Network Security – Firewall, IDS/IPS, and VPN Gateway (SSL VPN now available)
    - ✓ Email Security – Spam Filtering, Anti-Virus, and Phishing Protection
    - ✓ Web Security – Content (URL) Filtering, Anti-Virus, and Spyware Protection
  - Astaro Command Center – Management Platform supporting up to 500 installations.
  - Clustering and High Availability Configurations for demanding environments.
  - Robust for Today, Scalable for Tomorrow!
  - Extensive features, Excellent Quality, and Easy to Deploy
  - Available as Appliances or as Software
- **Product Distribution**
  - Astaro Products and Services are available exclusively through our network of Authorized Partners.



# Customers



The Washington Times

Pilgrim Telephone



SHARP  
..... be sharp

Stanford University

1-800-PetMeds®

America's Largest Pet Pharmacy



ThyssenKrupp  
Automotive



BlueCross  
BlueShield  
Association

ROHM  
HAAS

HARTE  
HANKS

SIEMENS

Dreyer's  
Grand Ice Cream

COLT

Fiserv®

MARITIM

CORNELL

HOUSTON  
ROCKETS

NYU  
New York University

JOHNS HOPKINS  
UNIVERSITY

micros®

US DigitalMedia

INTRANSIT®

mck communications

alibris

Oakland County  
Michigan

wine.com

# Recognition and Awards



**SC Magazine 2007 Europe Awards  
"Best Network Security"**

**SC Magazine "Best of 2006"**

**Common Criteria Certified - 2006**

**Firewall ICSA Labs Certified**

**Product of the Year 2005 & 2006  
- CRN**

**SC Magazine "Best of 2005"**

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

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

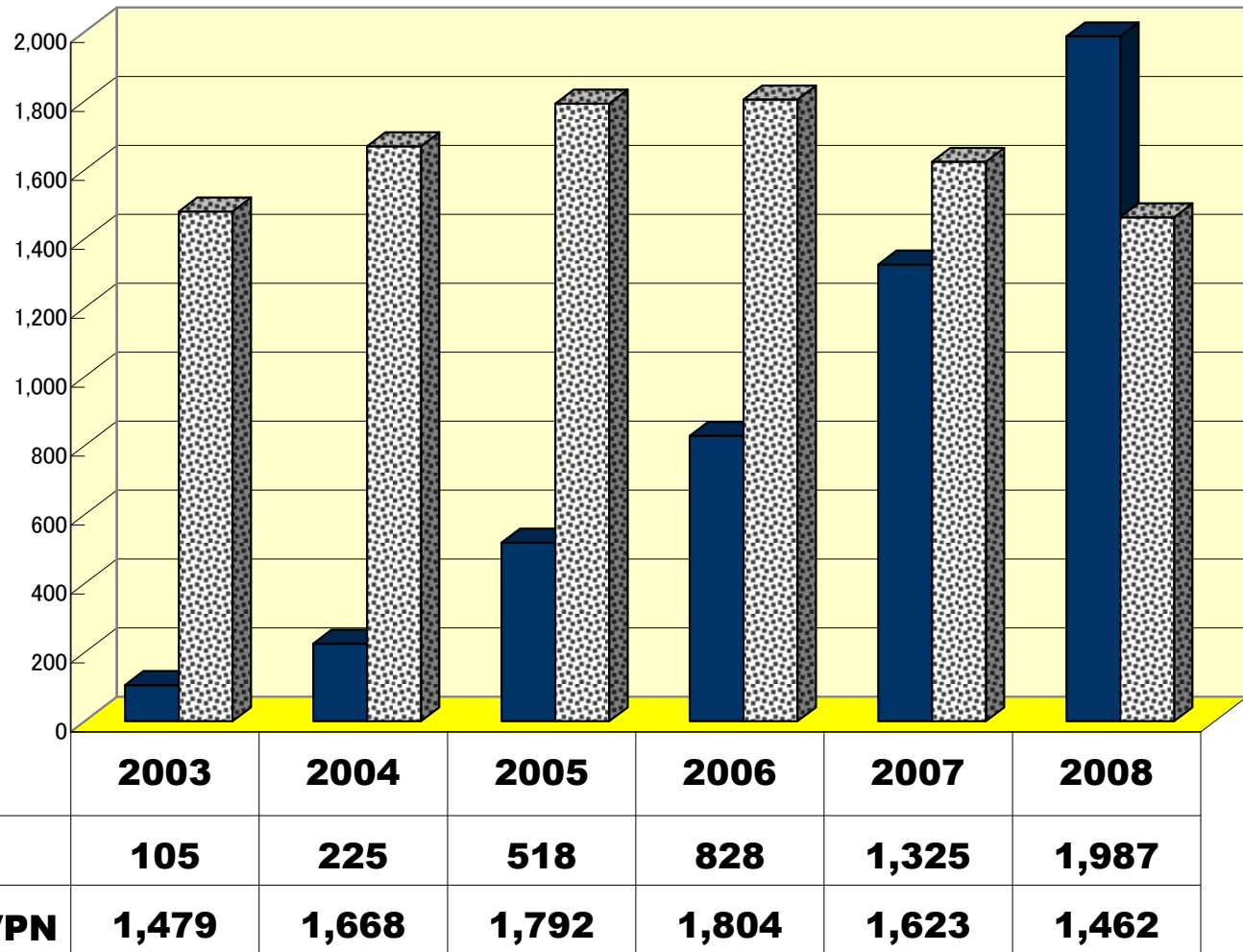


Common Criteria Arrangement



# WW IDC Forecast

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.



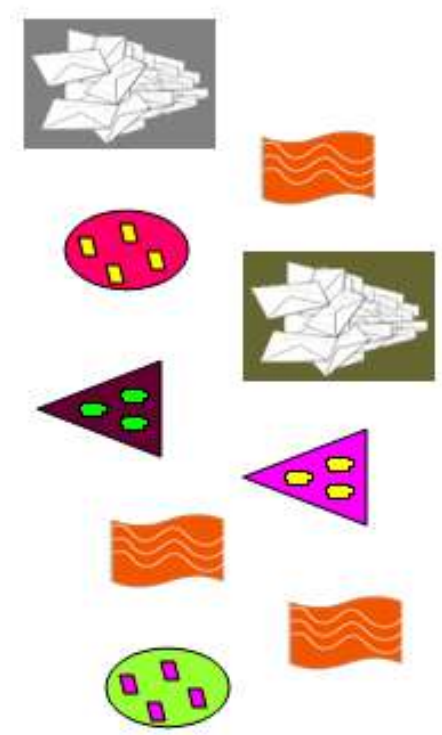
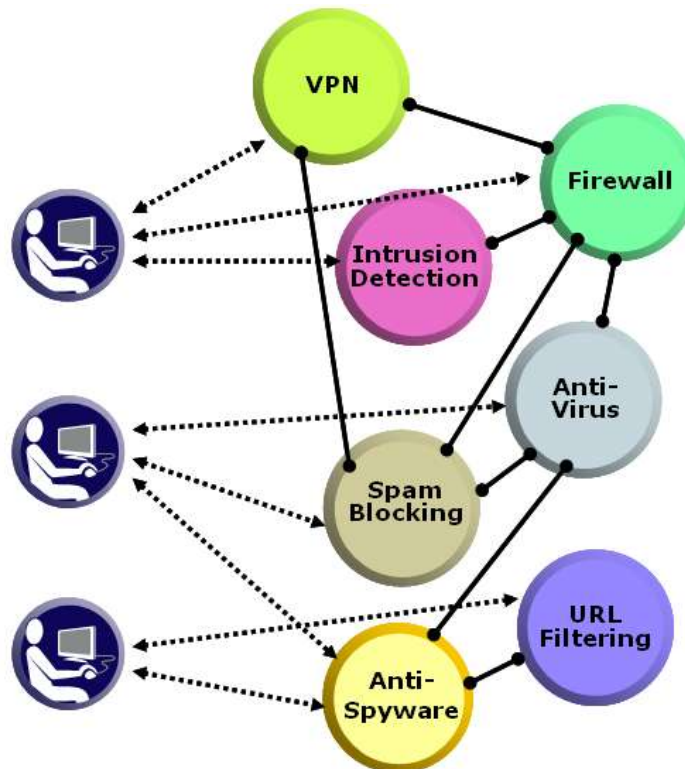
# Customer Challenges

Difficult to Deploy and Manage

Expense to Maintain (People and System)

Ongoing and Emerging Threats

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



# Network Security Architecture

web

network

e-mail

security

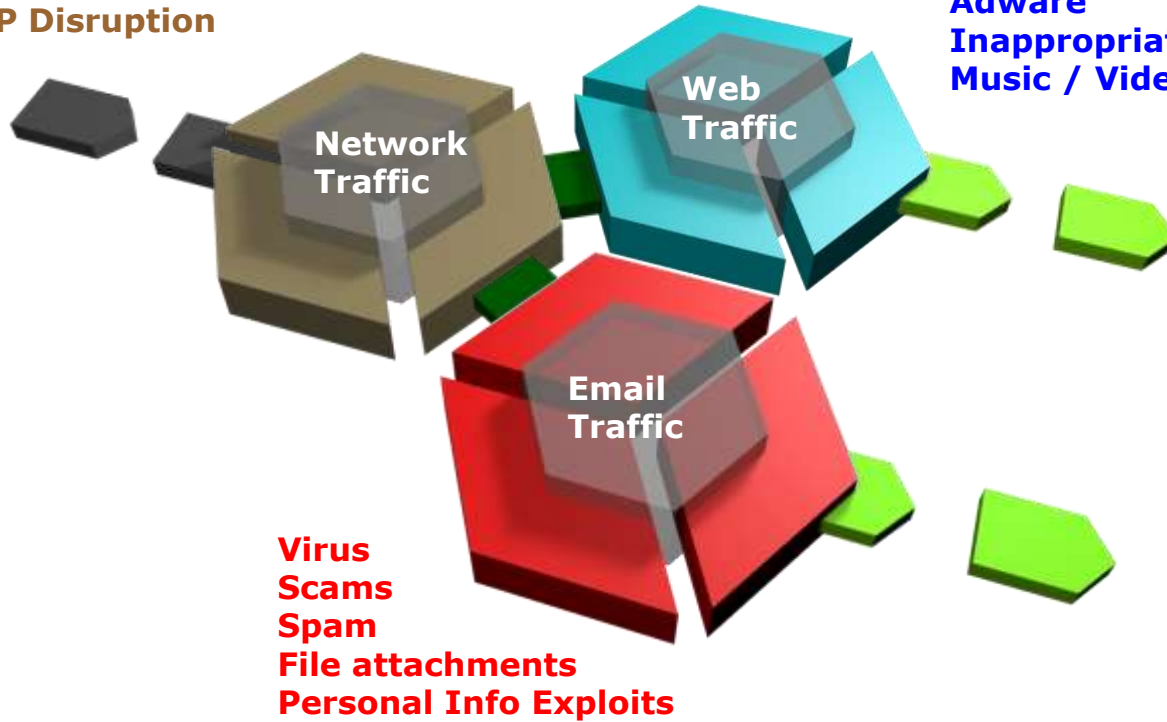


**astaro**  
internet security

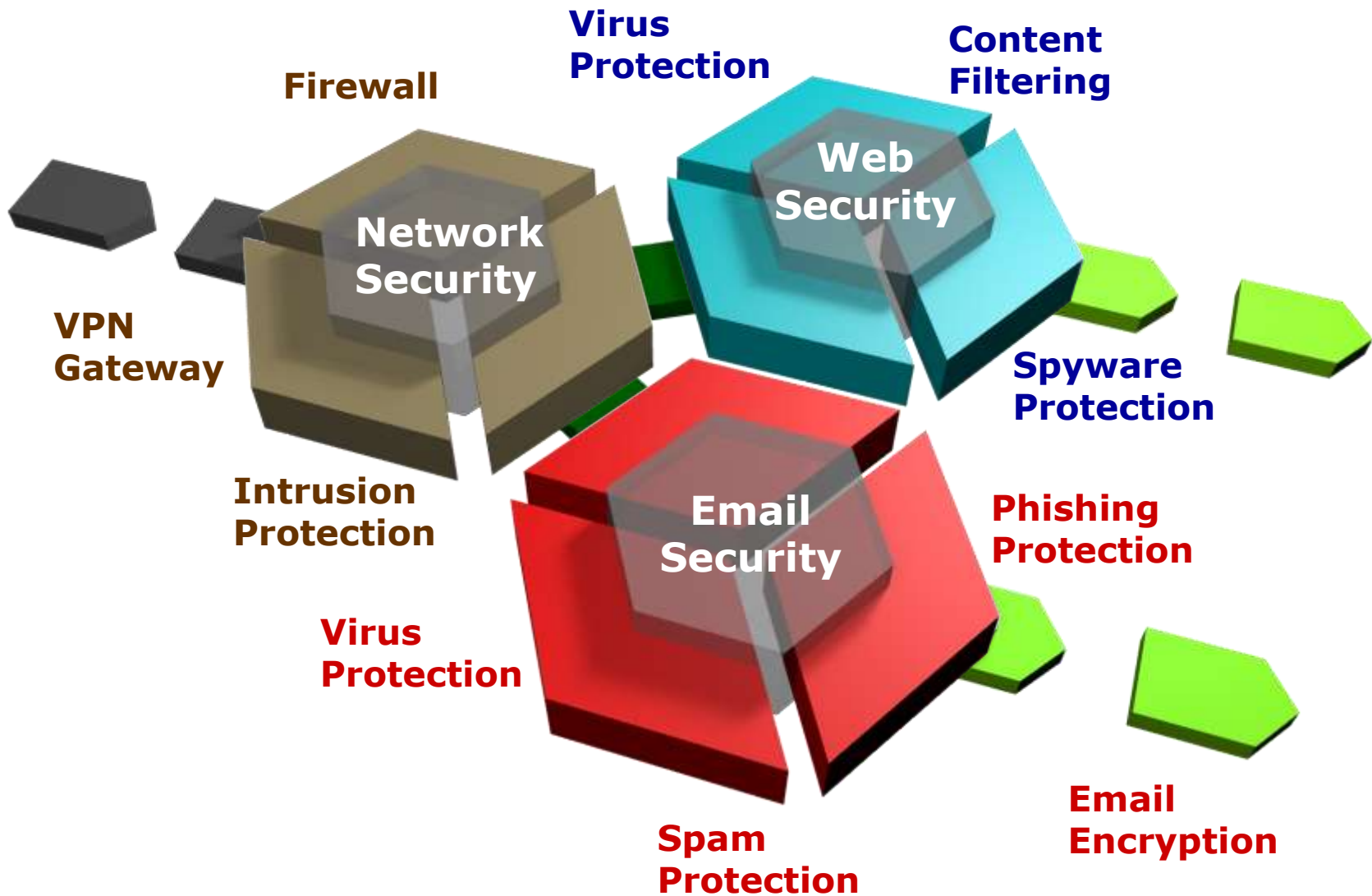
# Major Vulnerability Points

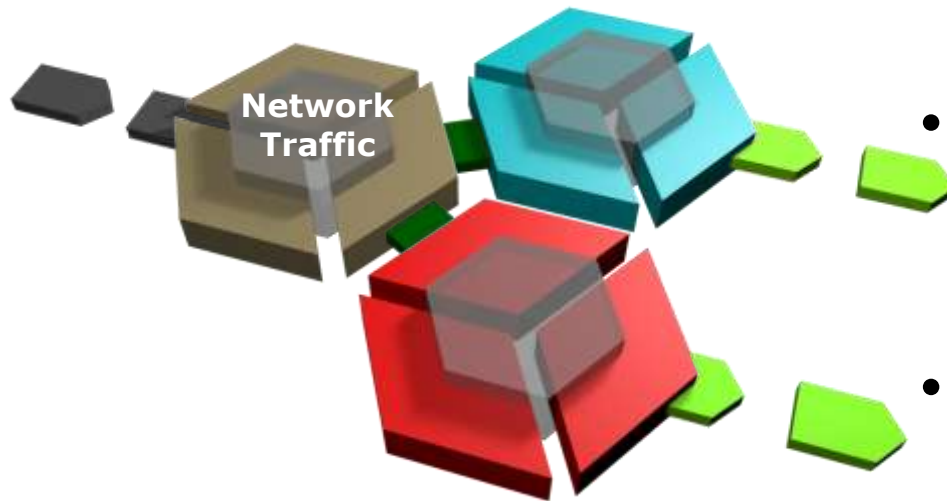
**Hack Attacks**  
**Attack traffic**  
**Connection Hijacking**  
**Denial of Service**  
**Probes**  
**VOIP Disruption**

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



# Protective Technologies





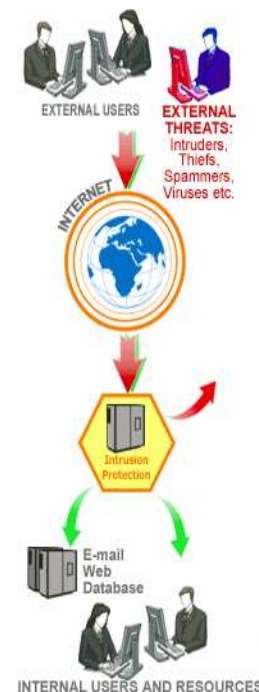
- **Firewall** with stateful packet inspection and application-level proxies, guards Internet communications traffic in and out of the organization.
- **Intrusion Protection** detects and blocks probes and application-based attacks using heuristics, anomaly detection, and pattern-based techniques.
- **Virtual Private Network Gateway** assures secure communications with remote offices and “road Warriors”.

# Key Firewall Functions

- Stateful Packet Inspection
  - 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

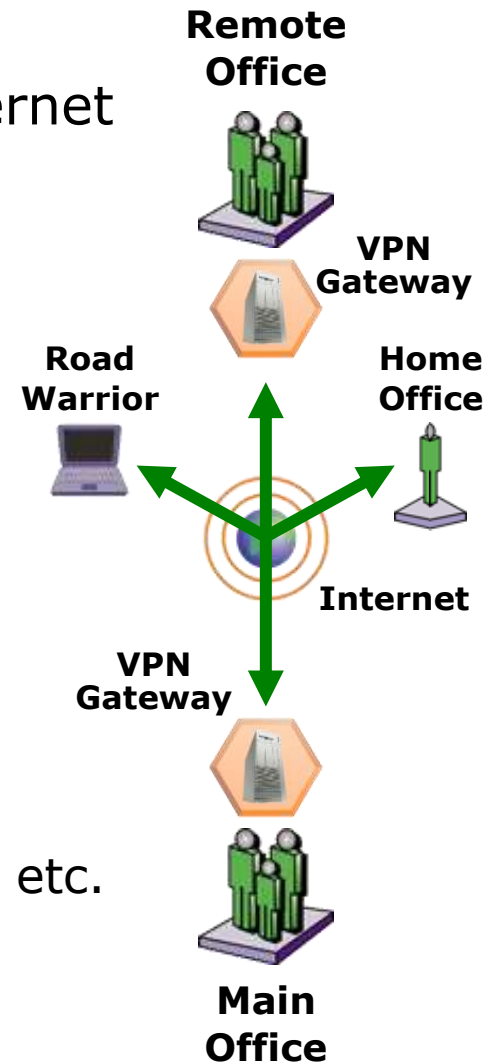


- Identify and Block Application related probes and attacks
- Identify and Block Protocol related probes and attacks
- Large Database (7,000) of IPS patterns and rules
  - Probing, port scans, interrogations, host sweeps
  - Attacks on application vulnerabilities
  - Protocol exploitations
  - Messaging, 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
  - Easy to add and customize rules



# 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
  - Active Directory, eDirectory, LDAP, Open LDAP, etc.
- Internal certificate authority
  - Full Public Key Infrastructure (PKI) support
- Supports DynDNS based VPN tunnels

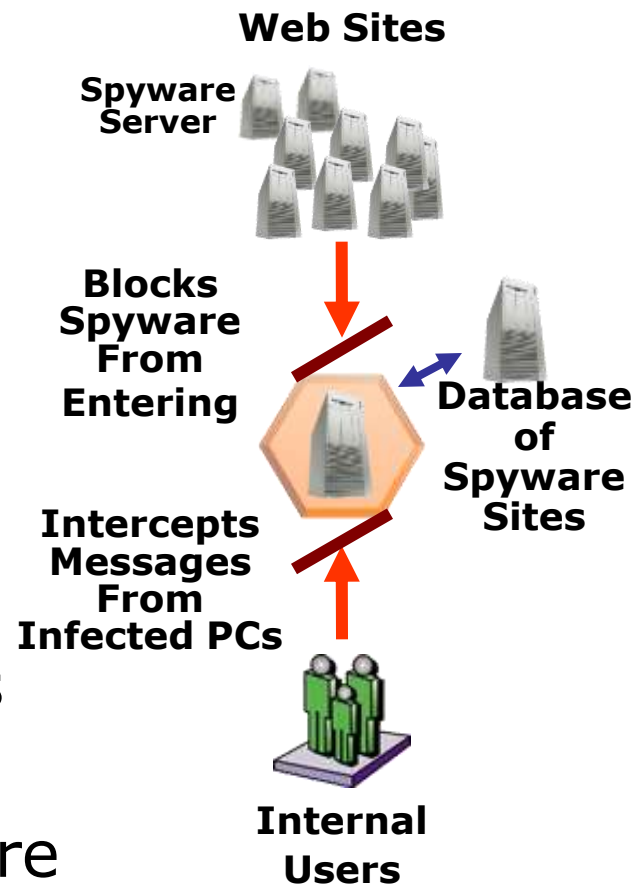




- **Spyware Protection** block incoming spyware, adware and other malicious applications, and prevents them from sending out confidential information.
- **Virus Protection for the Web** defend computers against virus infections from web downloads and web-based email.
- **Content Filtering** block Internet access to numerous categories of web sites during working hours.

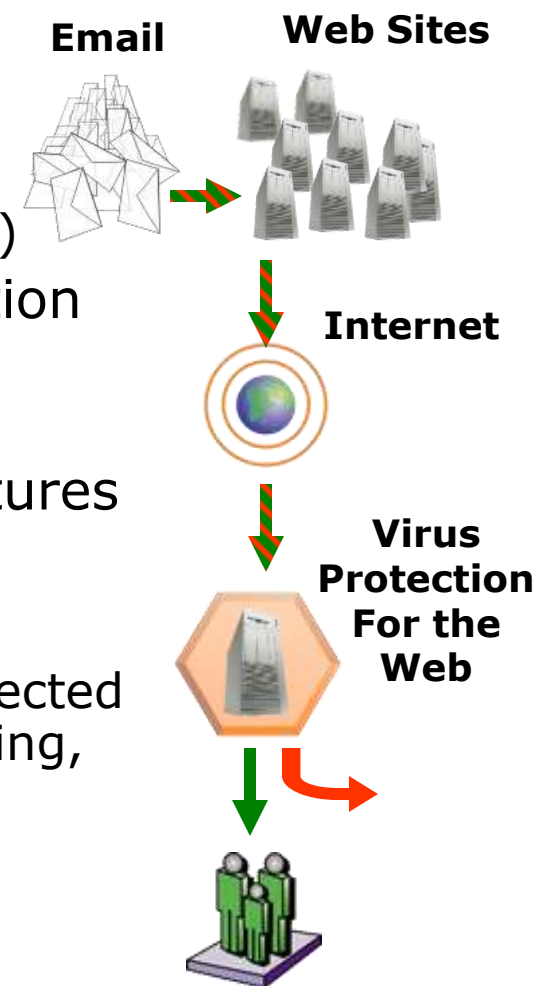
# Spyware Protection

- 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!



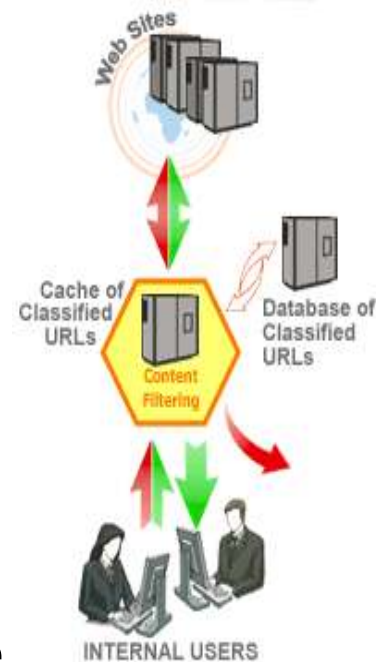
# Virus Protection for Web Traffic

- 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)

- 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 (3B+)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



## 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:

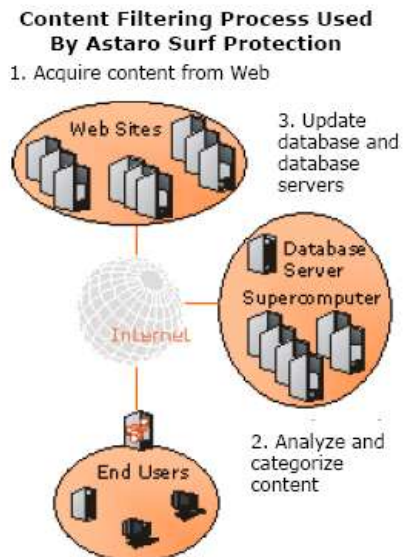
- All Content is analyzed and categorized by an enormous Web Crawling Server Farm.
- Overblocking and Underblocking is minimized by analyzing Web Content prior to the Content Request.
- Performance is enhanced by a simple DB lookup.
- Users experience consistent Content Delivery according to defined Security Policy.
- Decreased Administrative burden.

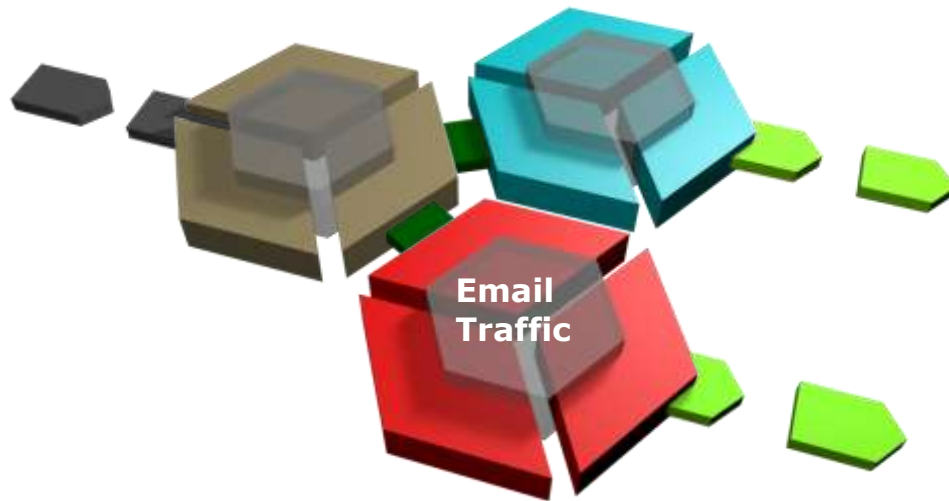


Implementing Web Filtering With Astaro Surf Protection

# 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 more often are crawled more often.





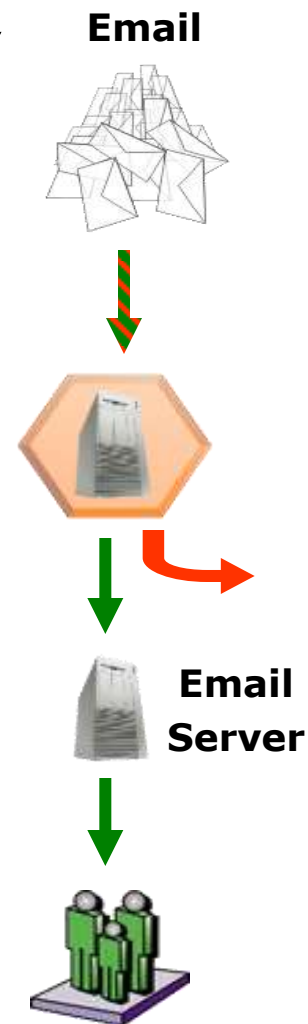
**Virus Protection for Email** catch viruses in SMTP and POP3 emails and attachments, even in compressed and archived formats.

**Spam Protection** multiple techniques to filter out spam without stopping legitimate emails.

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

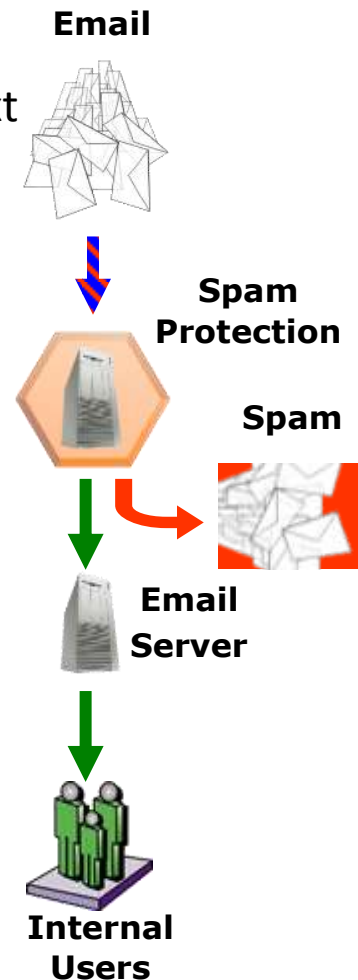
# Virus Protection for Email

- 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
- Provide Alerts when infected messages are quarantined.



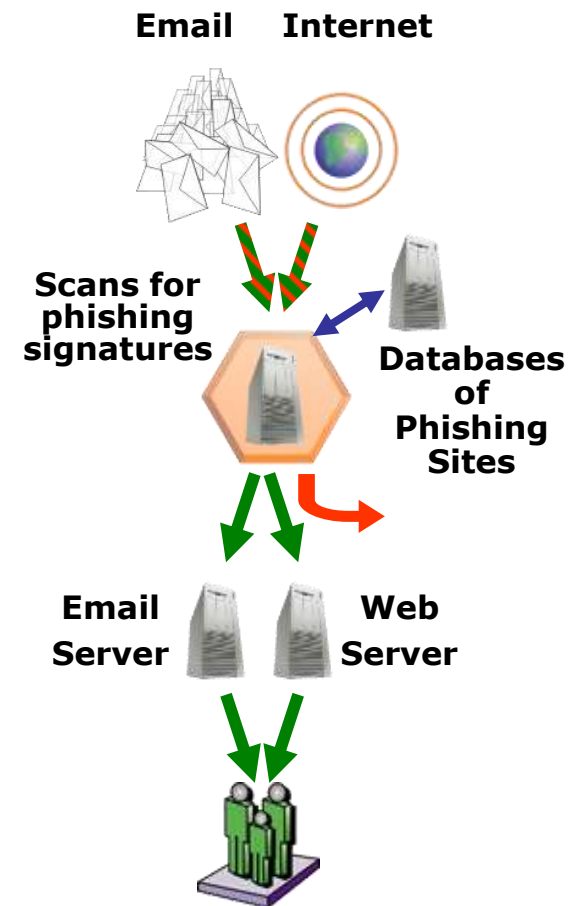
# Spam Protection Technology

- 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)
- Real Time Identification of Outbreaks.

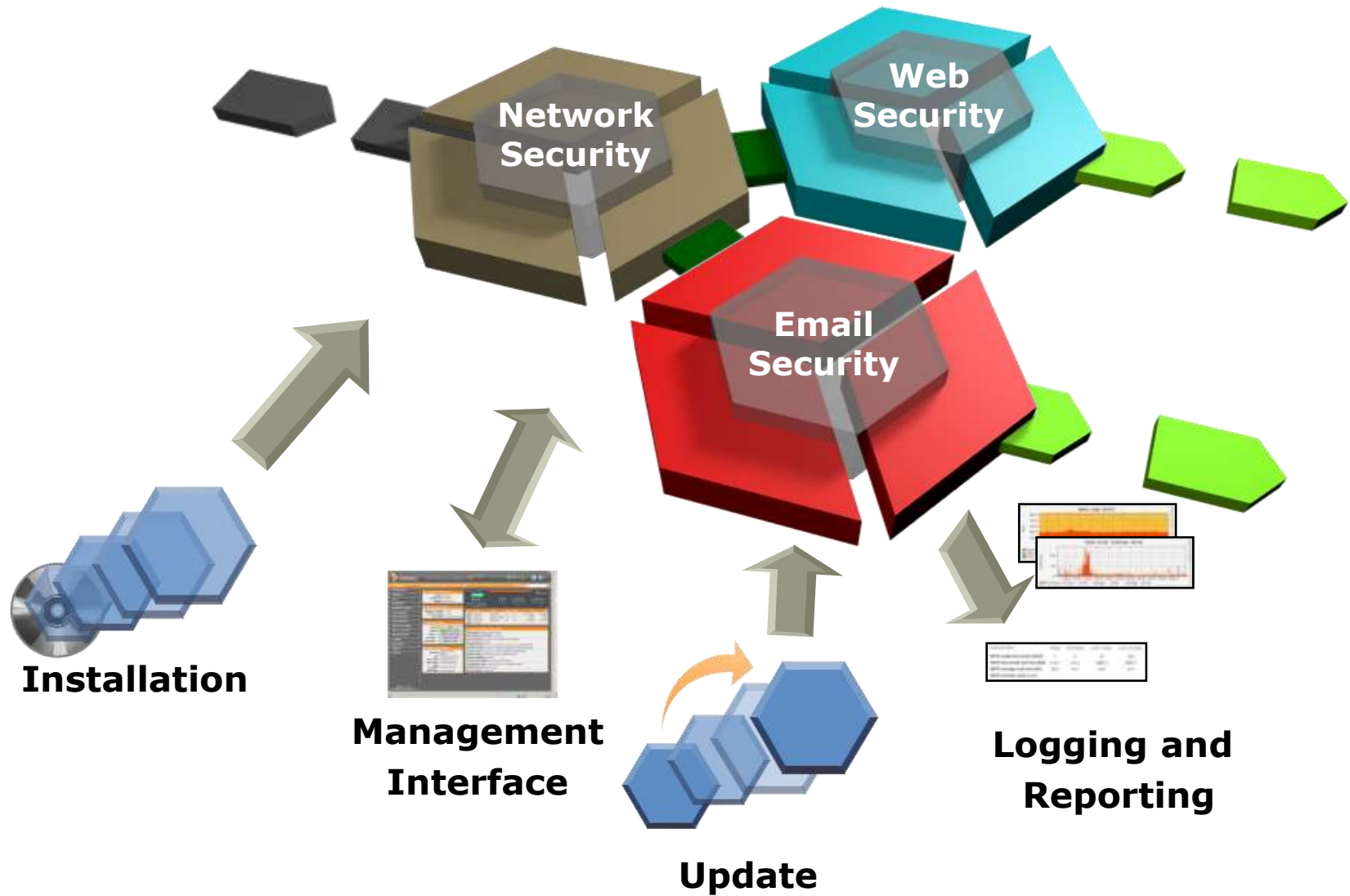


# Protection Against “Phishing”

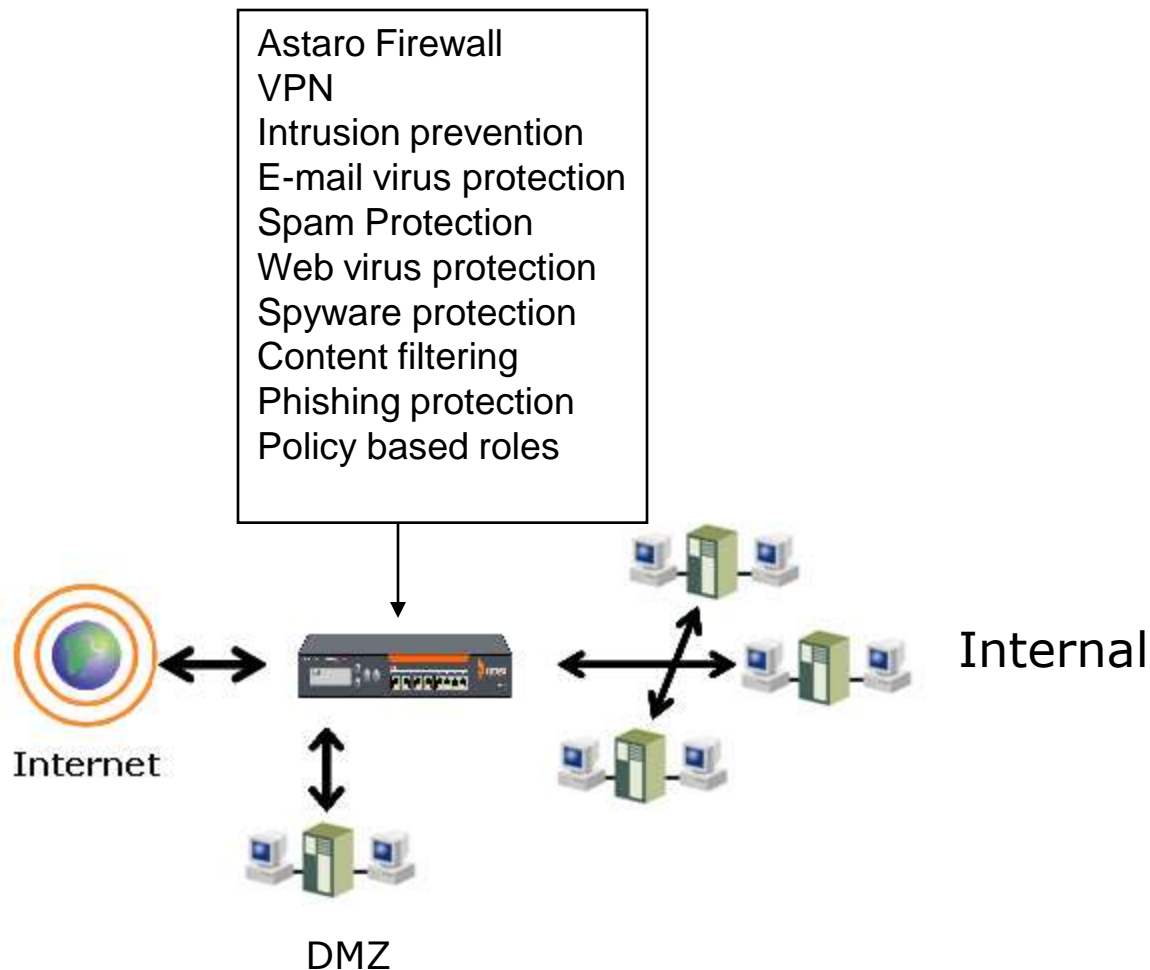
- “Phishing”
  - Criminals imitate emails from banks, credit card companies, eBay and other sources to obtain confidential user information
- Block “Phishing” attempts with multiple technologies.
  - Virus scanner identifies phishing signatures
  - URL filtering database captures phishing servers in the “suspicious” category
  - Content downloaded from web sites will be blocked if it matches patterns of phishing content



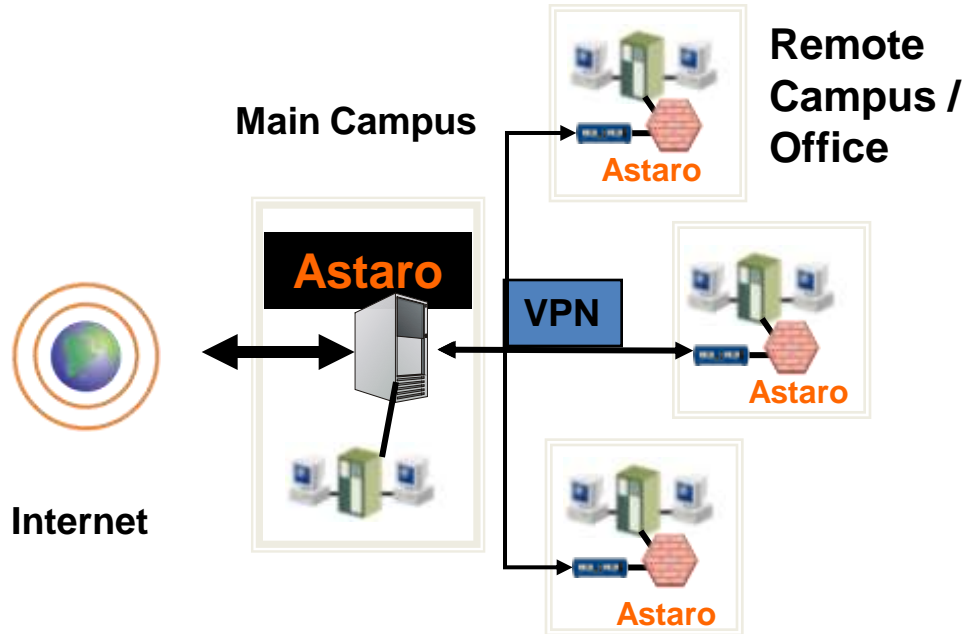
# Integrated Management and Control



# Sample Deployment



# Main Campus / Remote Site



- Astaro Firewall
- VPN
- Intrusion prevention
- E-mail virus protection
- Spam Protection
- Web virus protection
- Spyware protection
- Content filtering
- Phishing protection
- Policy based roles

**Centralized Management**

**Centralized Reporting**



- **Enhance Security**

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

- **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.
- Allow IT Staff to focus and administer one Security Solution

# Astaro Security Gateway – Main Console


Astaro Security Gateway **v7**

admin  
75.37.101.105




---

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

**1 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



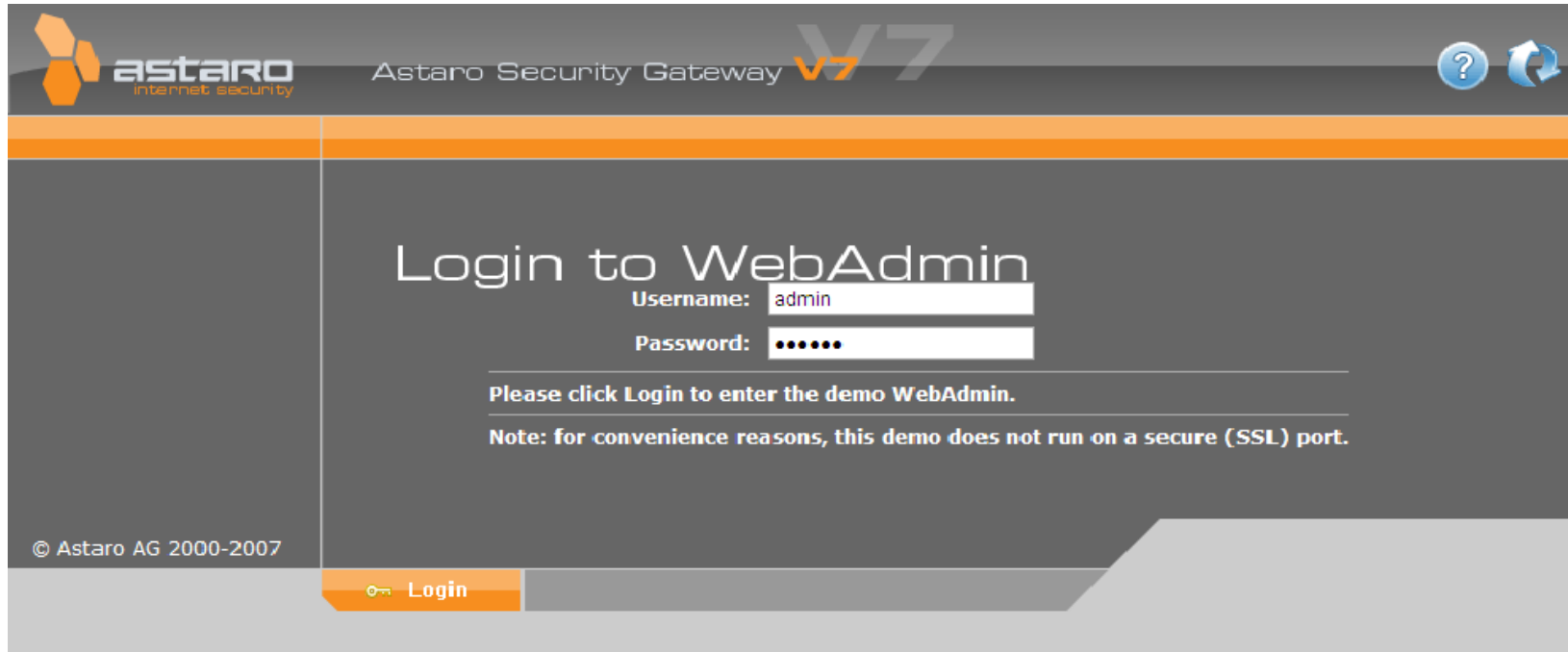
Port	Name	Type	State	Link	In	Out
eth0	Internal	Ethernet	Up	Up	125.0 kB/s	5.9 kB/s
eth1	external	Cable Modem	Down	Up	0 kB/s	0 kB/s
eth2	VPN-Link	Ethernet	Up	Up	13.0 B/s	11.0 B/s
eth3	unused					

**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

Release 7.002
© Astaro AG 2000-2007
Done
Internet
100%

http://demo.astaro.com



The screenshot shows the login interface for the Astaro Security Gateway V7 WebAdmin. The page has a dark grey header with the Astaro logo and 'Astaro Security Gateway V7' text. Below the header is an orange horizontal bar. The main content area is dark grey and contains the text 'Login to WebAdmin'. There are two input fields: 'Username: admin' and 'Password: .....'. Below the fields is a 'Login' button. A note at the bottom of the main area states: 'Please click Login to enter the demo WebAdmin. Note: for convenience reasons, this demo does not run on a secure (SSL) port.' The footer of the page includes the copyright notice '© Astaro AG 2000-2007' and a 'Login' button.

astaro  
internet security

Astaro Security Gateway V7

?

?

## 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

## 14 DAY Appliance Evaluation



**FREE TRIAL**

FULL-FEATURED SOFTWARE FOR  
A 30-DAY EVALUATION



**DOWNLOAD  
NOW!**

QUICK DOWNLOAD, 15-MINUTE INSTALLATION



**astaro**  
internet security

Thank You!

781-345-5000

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

web

- Surf Protection
- Spyware Protection
- Virus Protection

network

- Virus Protection
- Spam Protection
- Phishing Protection

e-mail

- Firewall
- VPN
- Intrusion Protection

security

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