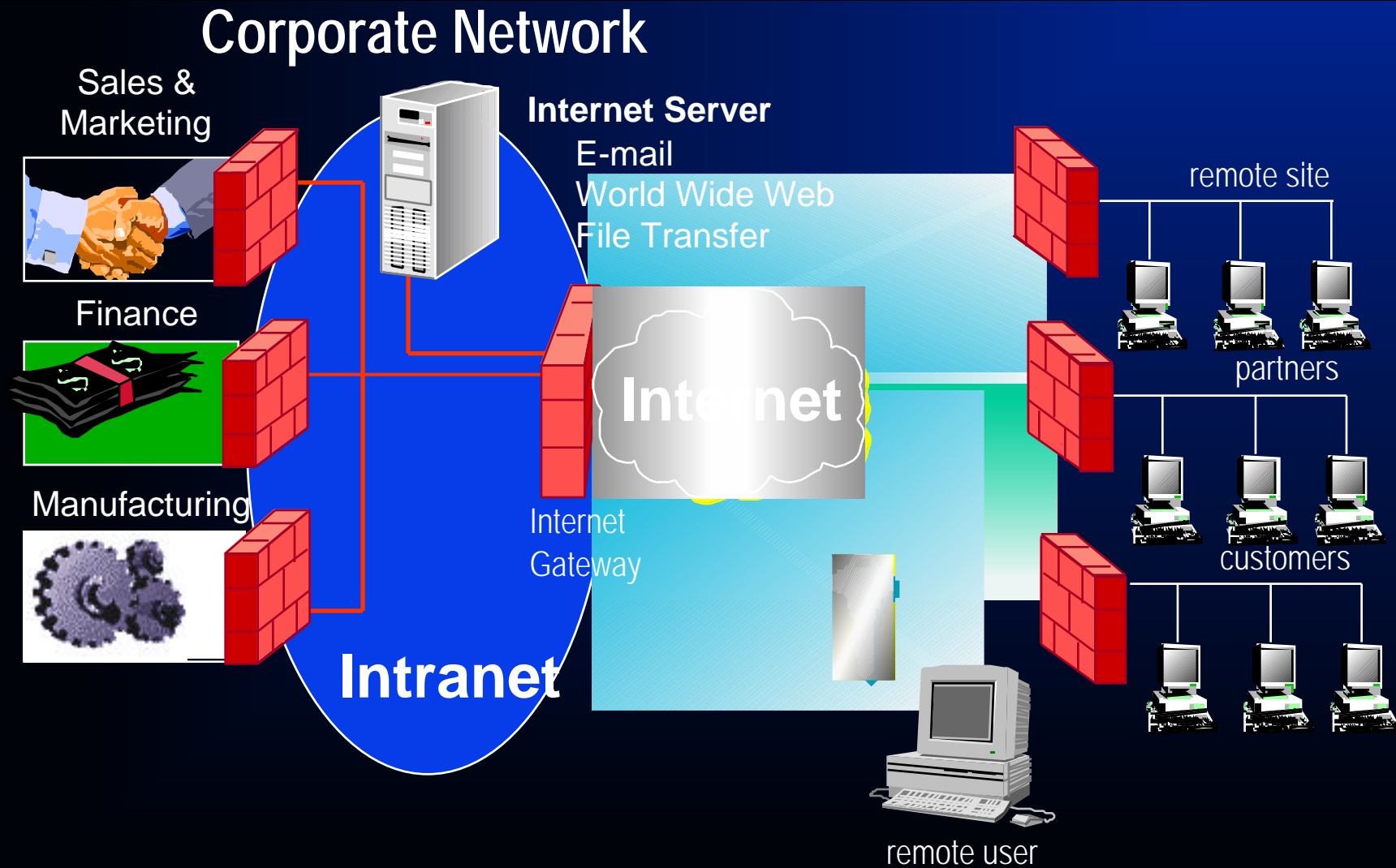


# The New Approach to Network Security



	<b>Old Paradigm</b>	<b>CHECK POINT's Approach</b>
<b>Security</b>	Restrict Access	Enable Secure Connectivity
<b>Technology</b>	Conservative and Proprietary	Open and Extensible
<b>User Interface</b>	Manage Features	Define Policy
<b>Network Management</b>	Manage Network Devices	Manage Network Traffic

# Emerging Requirements for the Enterprise Network



# Building Blocks of Effective Security Policies



**Access Control**

**Authentication**

**Encryption**

**Network Address Translation**

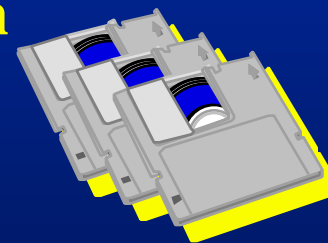
**Auditing and Accounting**

**Content Security**

**Connection Control**

**Others to come...**

**Application Support**



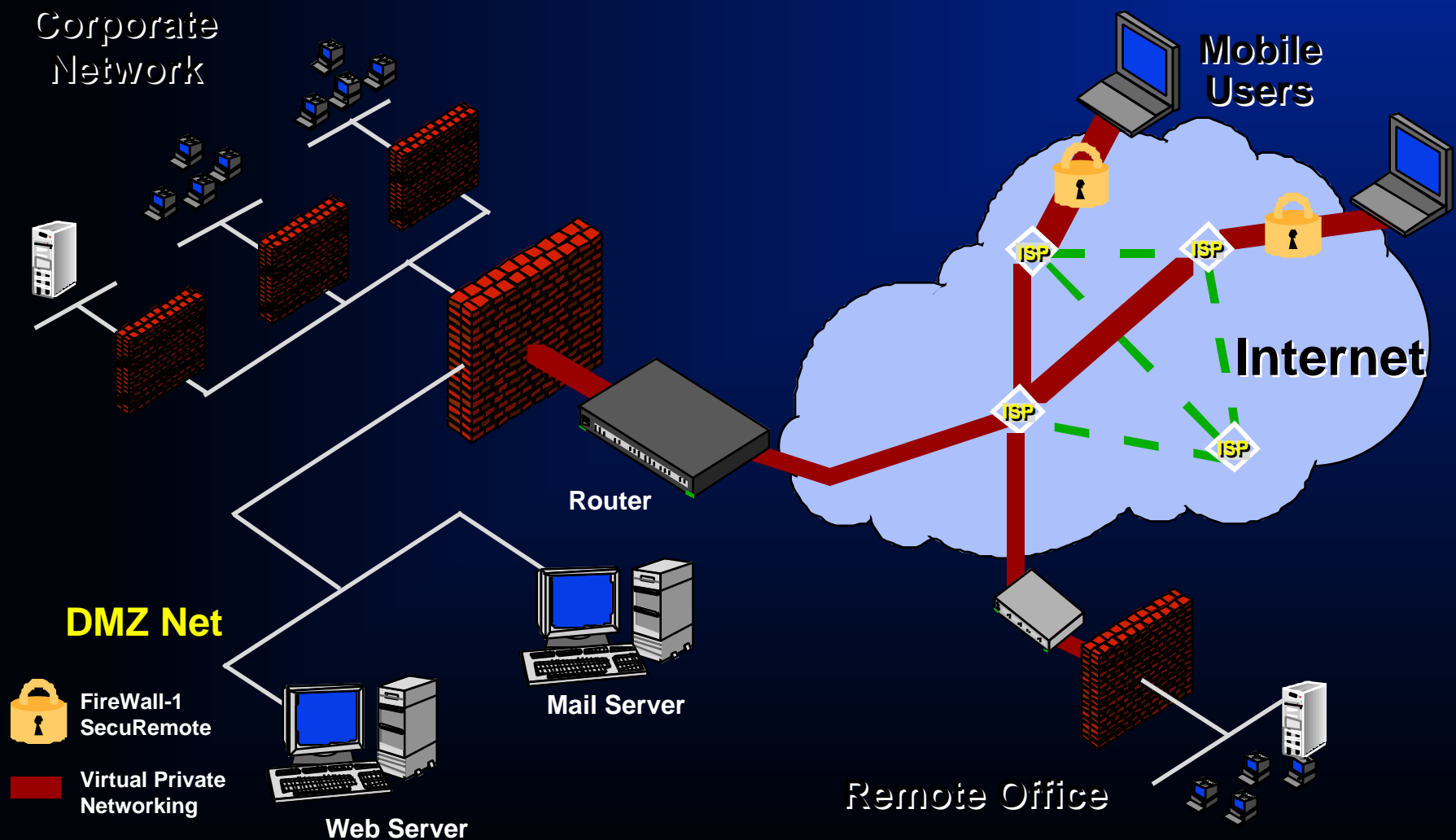
**Network Security**



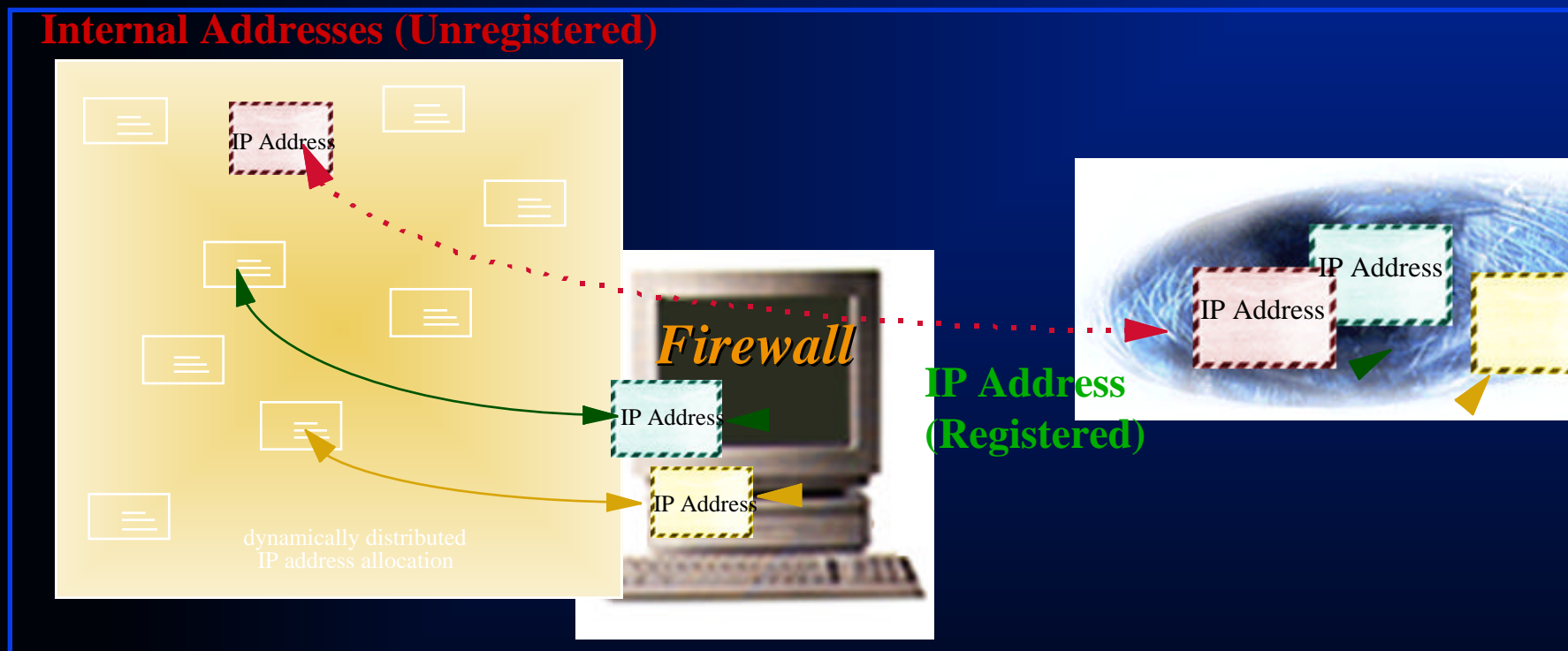
**Distributed Management**



# Enterprisewide Access Control



# Network Address Translation



**Address Translation** Overcomes IP Addressing Limitations  
and Hides Internal Addresses from the Internet

# Content Screening - Anti-Virus

Protocols:

- FTP
- HTTP
- SMTP

File “vectored”

Content Screening  
Application



Cheyenne  
Integralis  
McAfee  
Symantec  
Trend Micro

Only clean  
files pass

# Content Screening - Other

- URL Screening:
  - Screen traffic by URL
  - Monitor Web usage
  - Provide access partitioning based on Web pages
  - Free trial subscriptions to leading URL list providers
- Java Security
  - Block Java applets
  - Most common Java security attacks

# Connection Accounting

- Customers want collection of connection oriented data on selected rules
  - Elapsed time of the connection
  - Number of packets and bytes passed over the connection.
- Data must be viewable in real time via the Log Viewer
- Log export utilities are essential for the creation of charge-back and billing reports



# Content Security Requirements

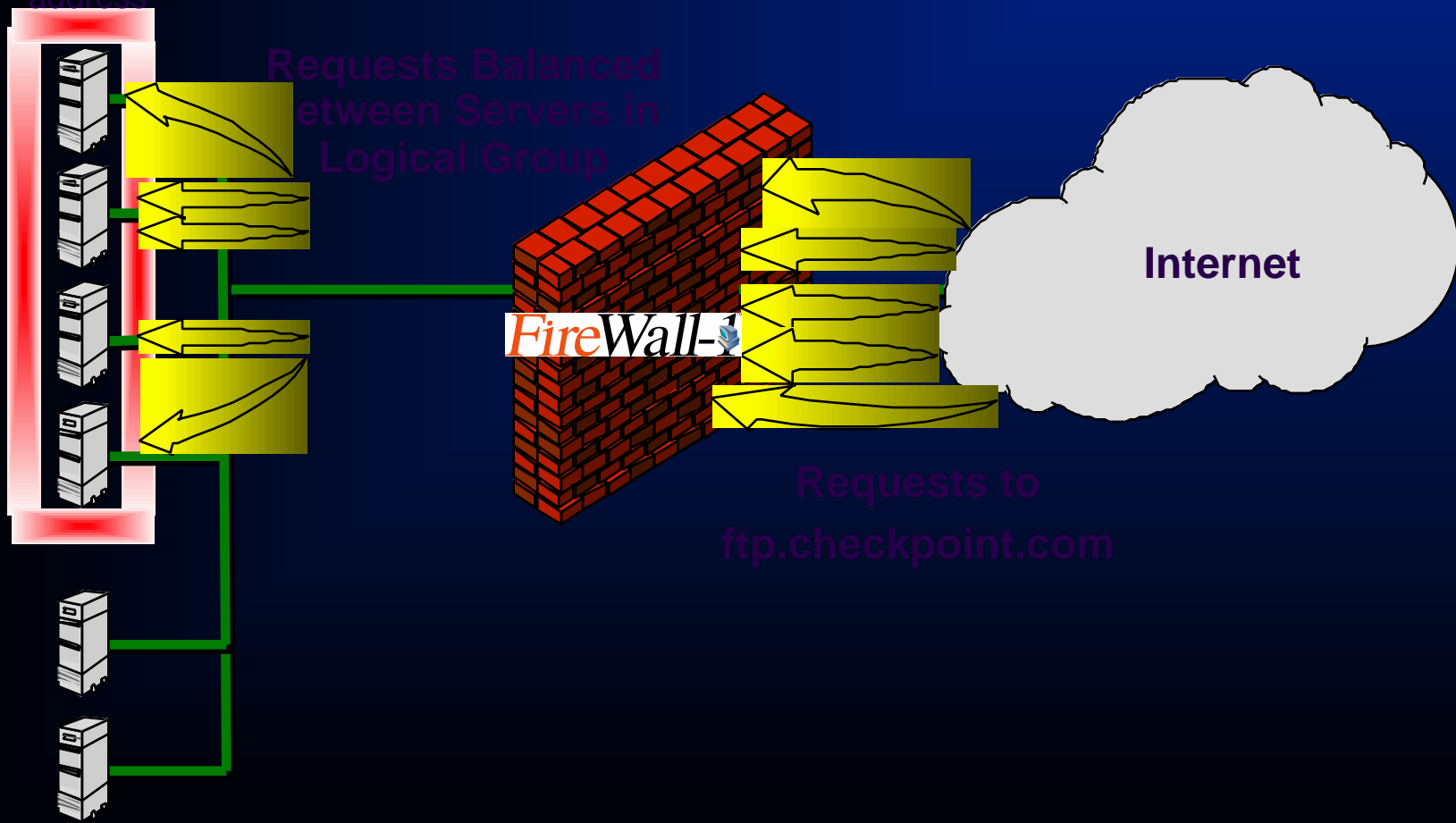
- Customers need more control over data streams for the commonly-used services
  - Enables solutions for data-driven attacks (malicious Java applets, Viruses, Trojan horses)
- Customers want to include content security definition and enforcement in the enterprise-wide security policy
  - define it once
  - distribute it to multiple firewall gateways throughout the enterprise
- Customers require auditing capabilities; want detailed reports on specific resource usage (URLs, files, Email addresses)

# Connection Control Requirements

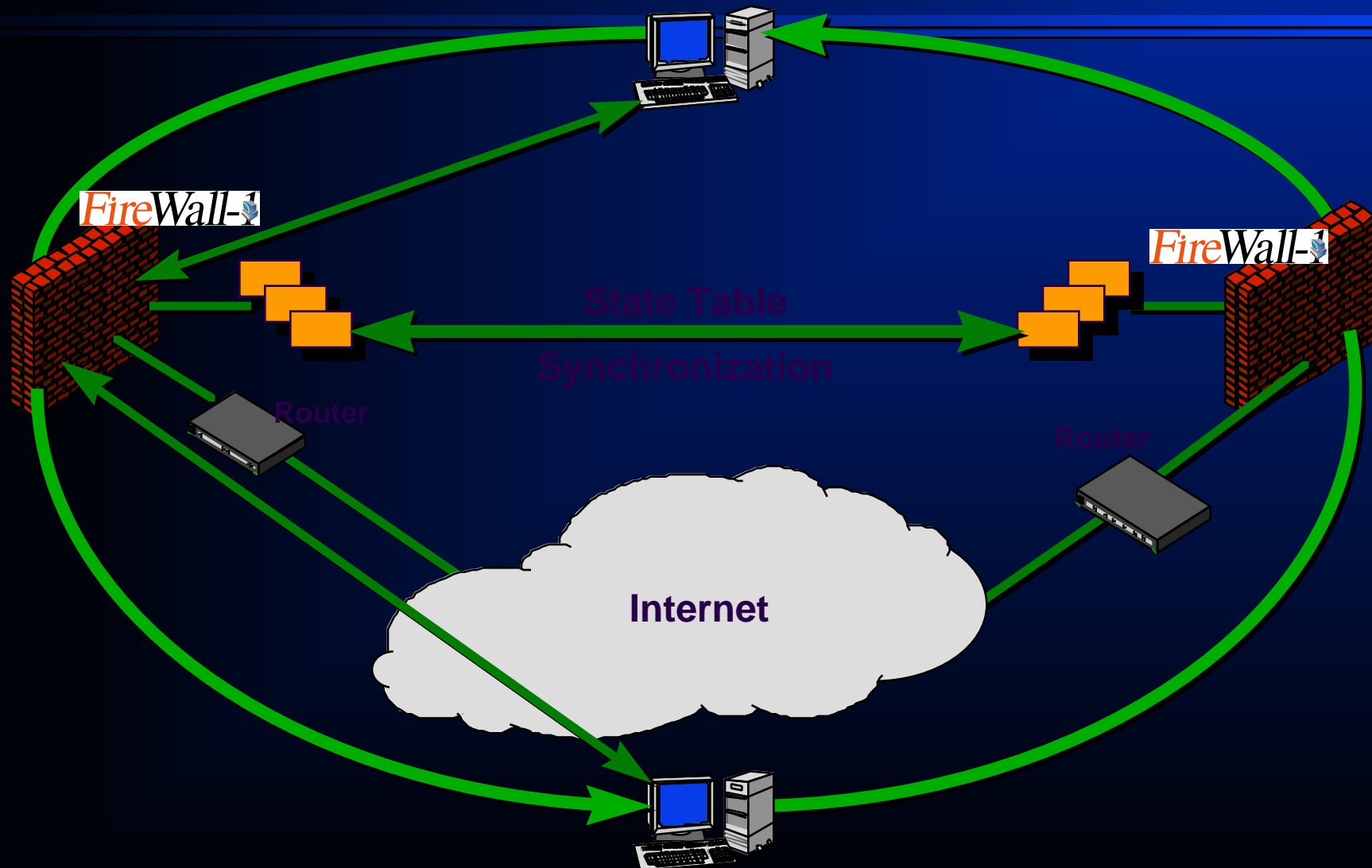
- As IP-based networks continue to grow in size and importance to organizations, all components of network infrastructure - e.g., hubs, routers, servers and software - need to provide solutions to increase availability of resources.
- Firewalls are deployed at key network access points. Customers want to leverage that deployment by extending the security policy to control quality of service on the network
- Connection control is required to cope with the growing connectivity challenges of the enterprise
  - Application support
  - High bandwidth
  - Network complexity

# Server Load Balancing

Identical FTP Servers  
with common IP  
address



# High Availability Firewalls

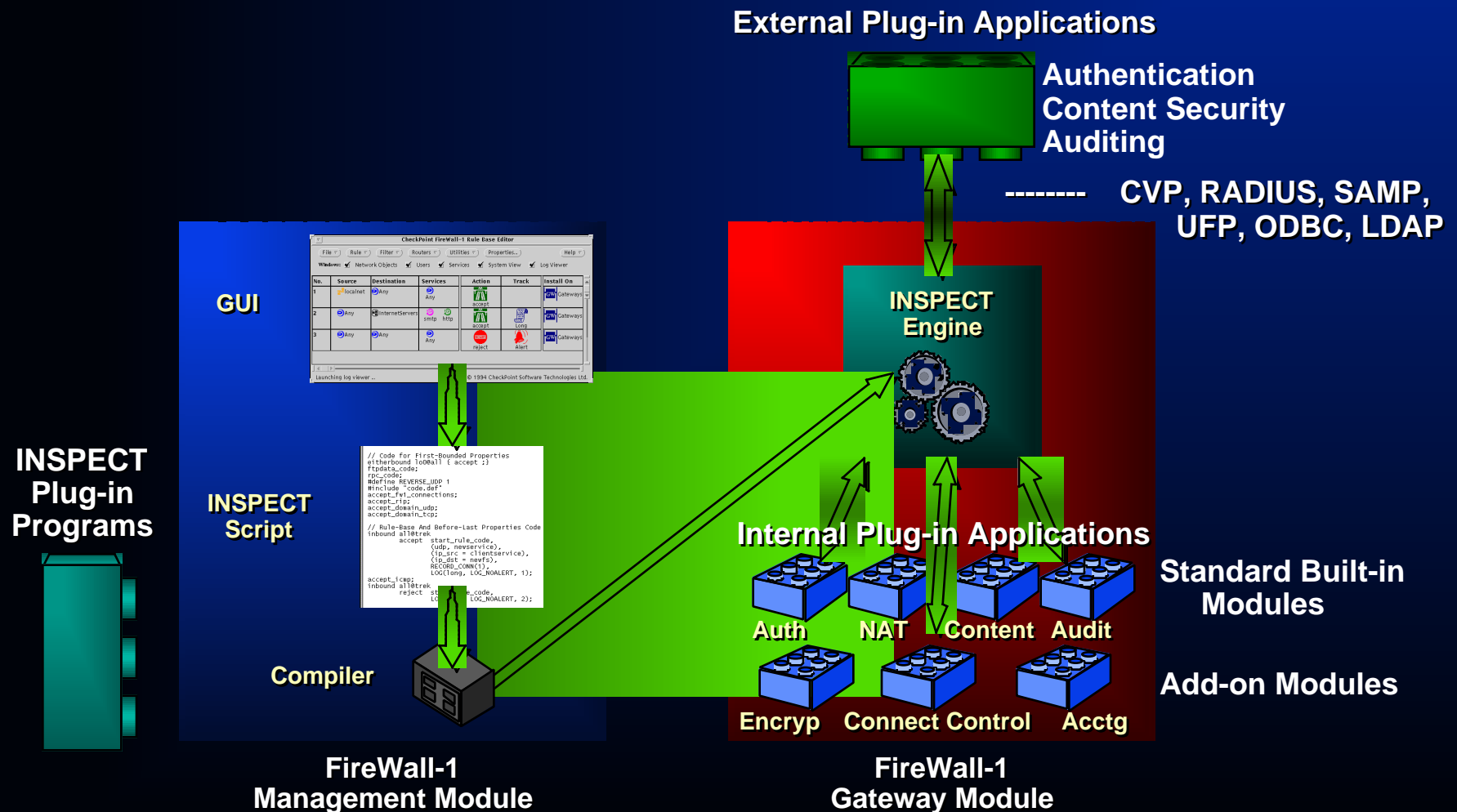


# CHECK POINT's OPSEC



## Open Platform for Secure Enterprise Connectivity

# The OPSEC Architecture



# Why An Open Network Security Platform?



- Open, flexible system design
- Scalable for enterprise growth
- Rapid extensibility to new functions and applications
  - Leverages Check Point and third party technology developments
- Makes network security the easiest, most cost-effective and most manageable it's ever been
- Customizable

# OPSEC Enables Secure Enterprise Connectivity



- Distributed client/server architecture
  - Centralized, policy-based management
- Enable plug-in functions through API's and standards support
- Customizable and extensible through INSPECT language
- Active management of network traffic