Security Architectures

Cyber Security Lab

Spring 2010

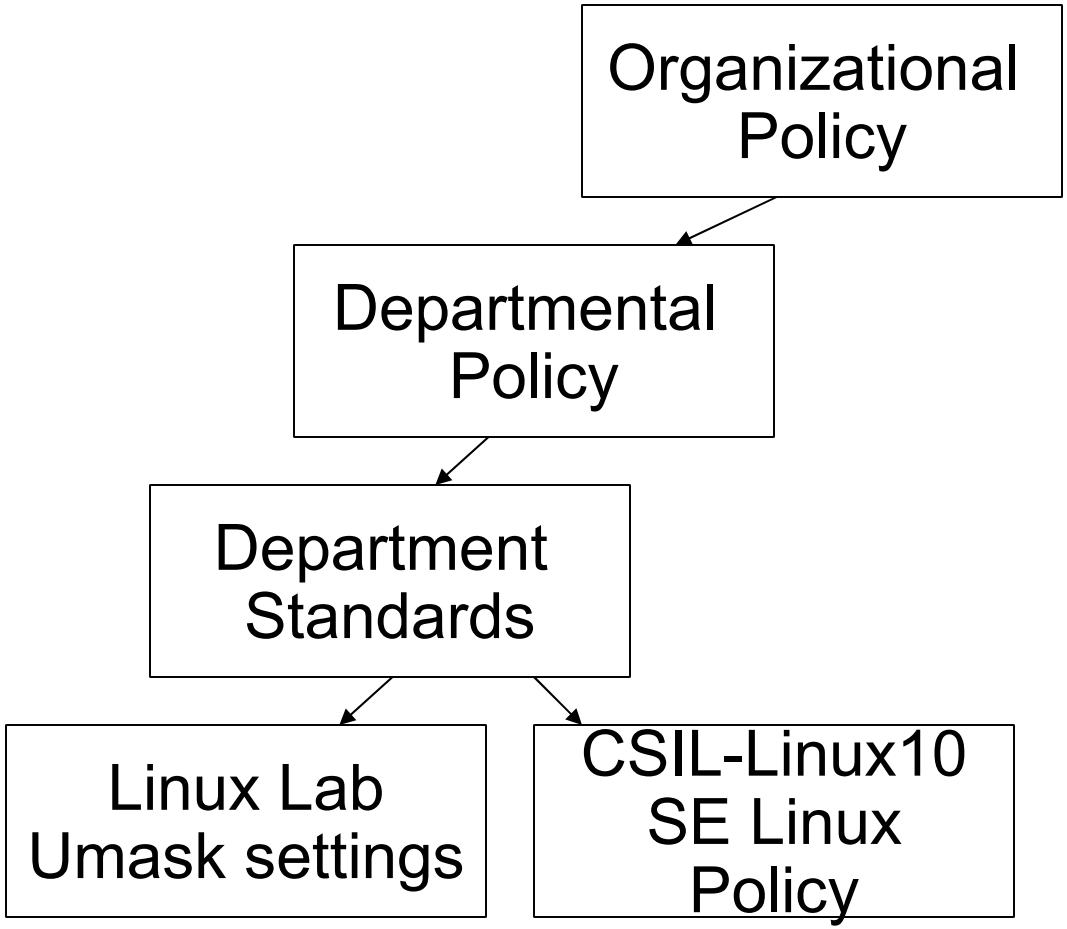
Security Policy

- *A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide* – RFC 2196
- Security policy separates the world into secure and insecure states
  - What is the information to be protected?
  - Who is responsible?
- Dictating what not how
- Must be feasible to implement

Security Policy

- The organizational security policy guides the requirements for a security design
  - The security policy is an English document
  - Hopefully rather precise
  - Defines the goals of the security implementation
- Often there is a hierarchy of policy
  - From broad organizational policy
  - To more detailed technology specific security guidelines

Hierarchy of Policies



Natural Language Security Policies

- Targeting Humans
  - Written at different levels
    - To inform end users
    - To inform lawyers
    - To inform technicians
    - Users, owners, beneficiaries (customers)
- As with all policies, should define purpose not mechanism
  - May have additional documents that define how policy maps to mechanism
- Should be enduring
  - Don't want to update with each change to technology

Security Policy References

- RFC 2196 – Site Security Handbook
  - Discusses policy and more general design and implementation issues. Published in 1997, so some of the technology references are dated, but the general recommendations are still valid
- SANS policy examples
  - http://www.sans.org/resources/policies/
- *Information Security Policies and Procedures*, Thomas Peltier
  - In the library

University of Illinois Information Security Policies

- University of Illinois Information Security Policies
  - System wide policy; Identifies what, not how
  - http://www.obfs.uillinois.edu/manual/central_p/sec19
- CITES UIUC standards and guidelines
  - DNS - http://www.cites.uiuc.edu/dns/standards.html
  - FERPA - http://www.cites.uiuc.edu/edtech/development_aids/f
- CS Department policies
  - https://agora.cs.illinois.edu/display/tsg/Policie

What is a security architecture?

- A framework that guides the security implementation
  - Guided by the security policy
  - Breaks the problem into modular pieces
    - Can implement and perfect a module
    - Can repeat implementation of proven modules and organization grows, e.g. remote office module
- Abstracting from implementation specifics aids in understanding the guiding structure of the system

Architecture Abstractions

- May be useful to think in terms of physical analogs
  - Data in file cabinets
    - Drawer granularity
    - Locks
  - Fortresses or silos
    - Gates or guards at limited access points
    - Toll booths

Security Architectures

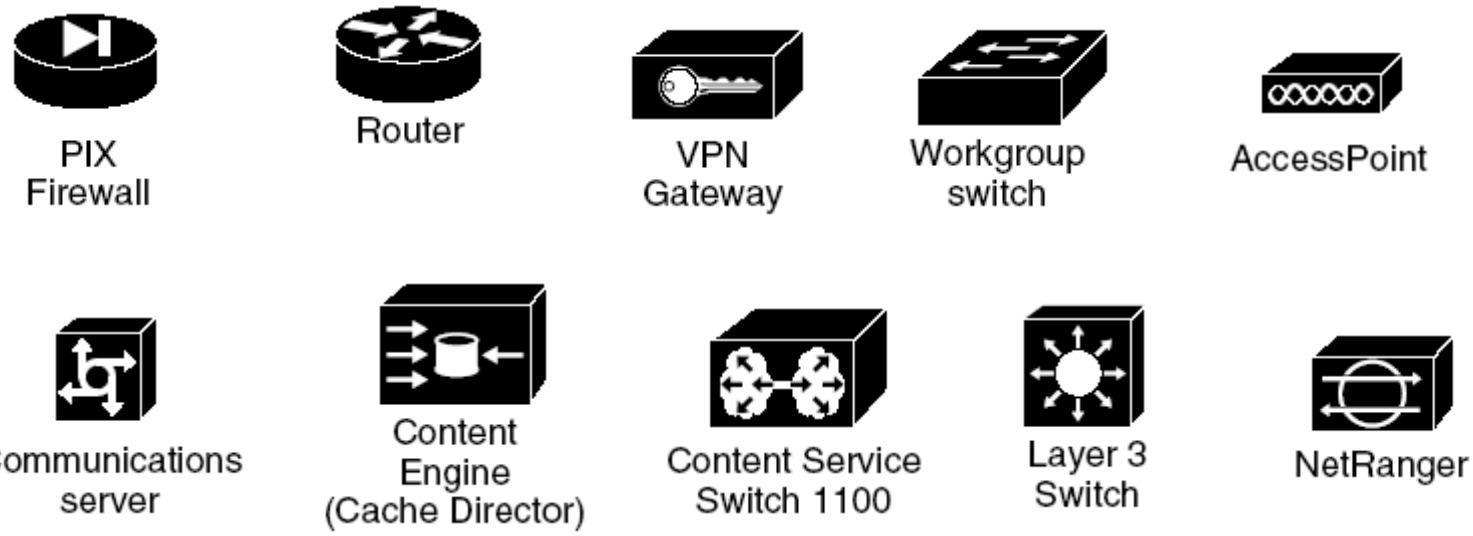
- Can generalize security architecture for classes of systems
- Can be found for many general system elements
  - J2EE applications
  - Client server applications
  - .Net applications

Cisco SAFE

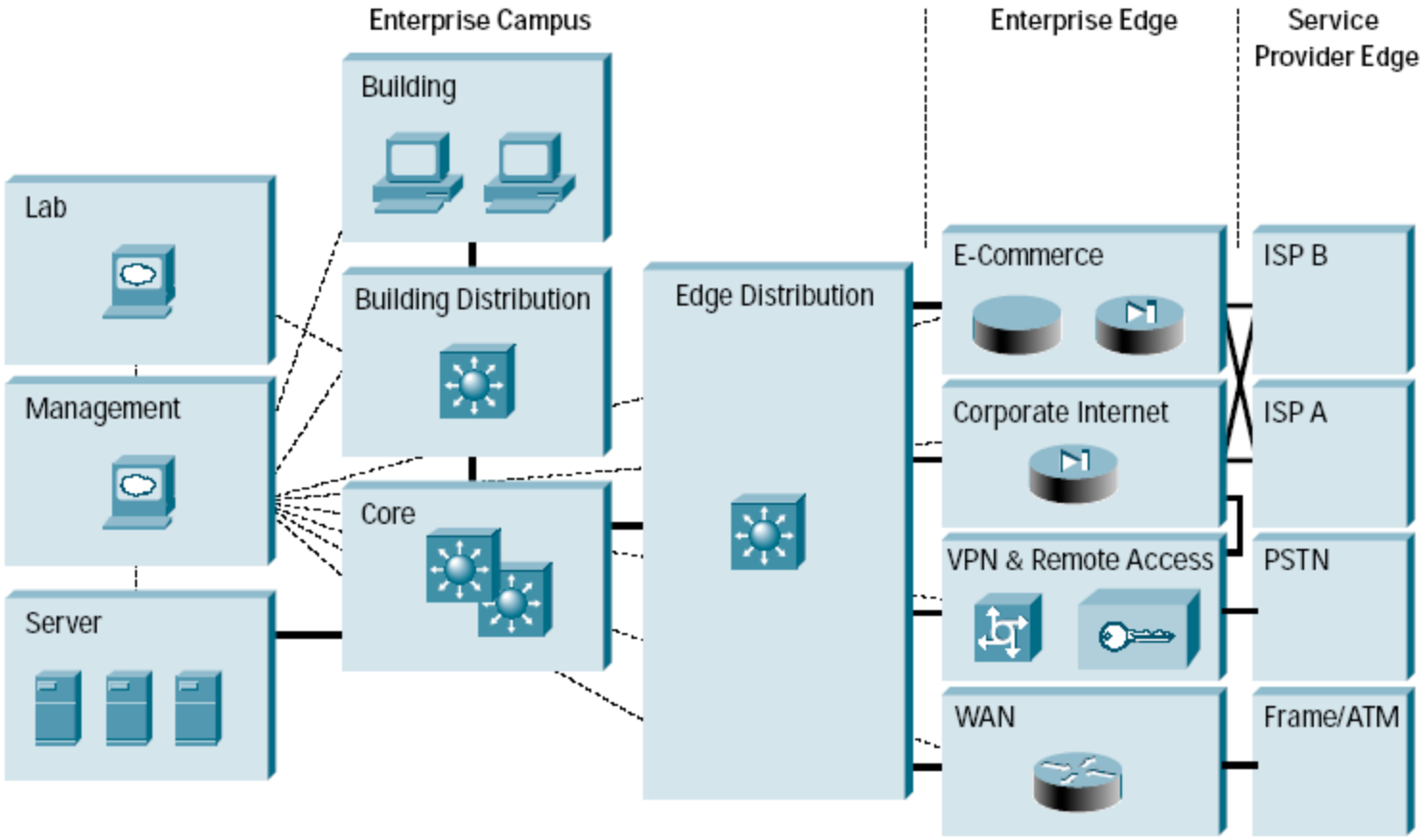
- A series of network security architecture blueprints
  - Identifies frameworks for particular scenarios
  - Analyzes placement of security enforcement devices in the network design
    - Even if you don't use these modules, the analysis can help you understand reasons for using mechanisms at various points
- Modules enable people to incorporate portions of the blueprint into their environment
- Following diagrams are from the SAFE Enterprise document
  - Copies handed out in class

Cisco Icon Overview

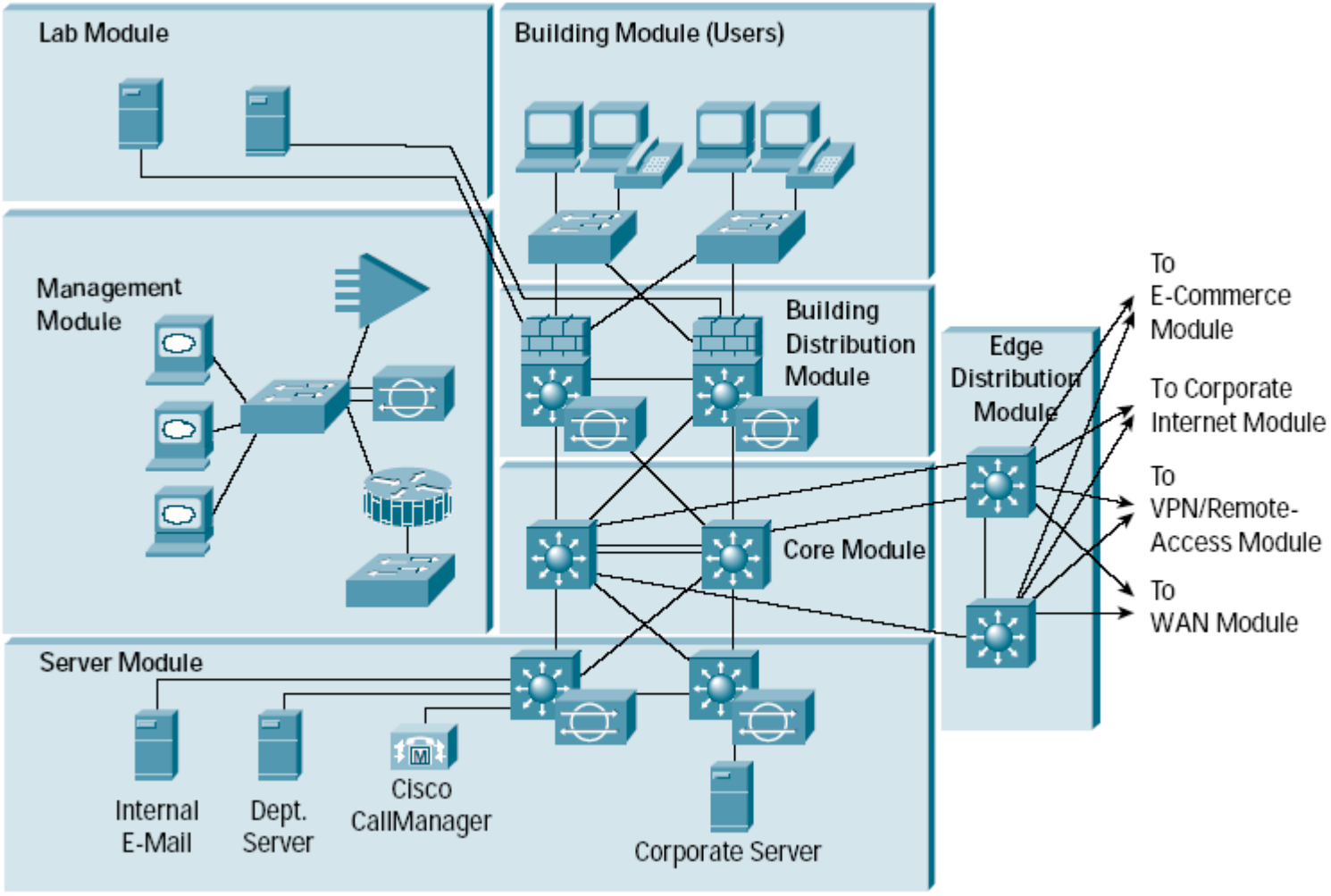
- Complete overview at http ://www.cisco.com/warp/public/503/2.html



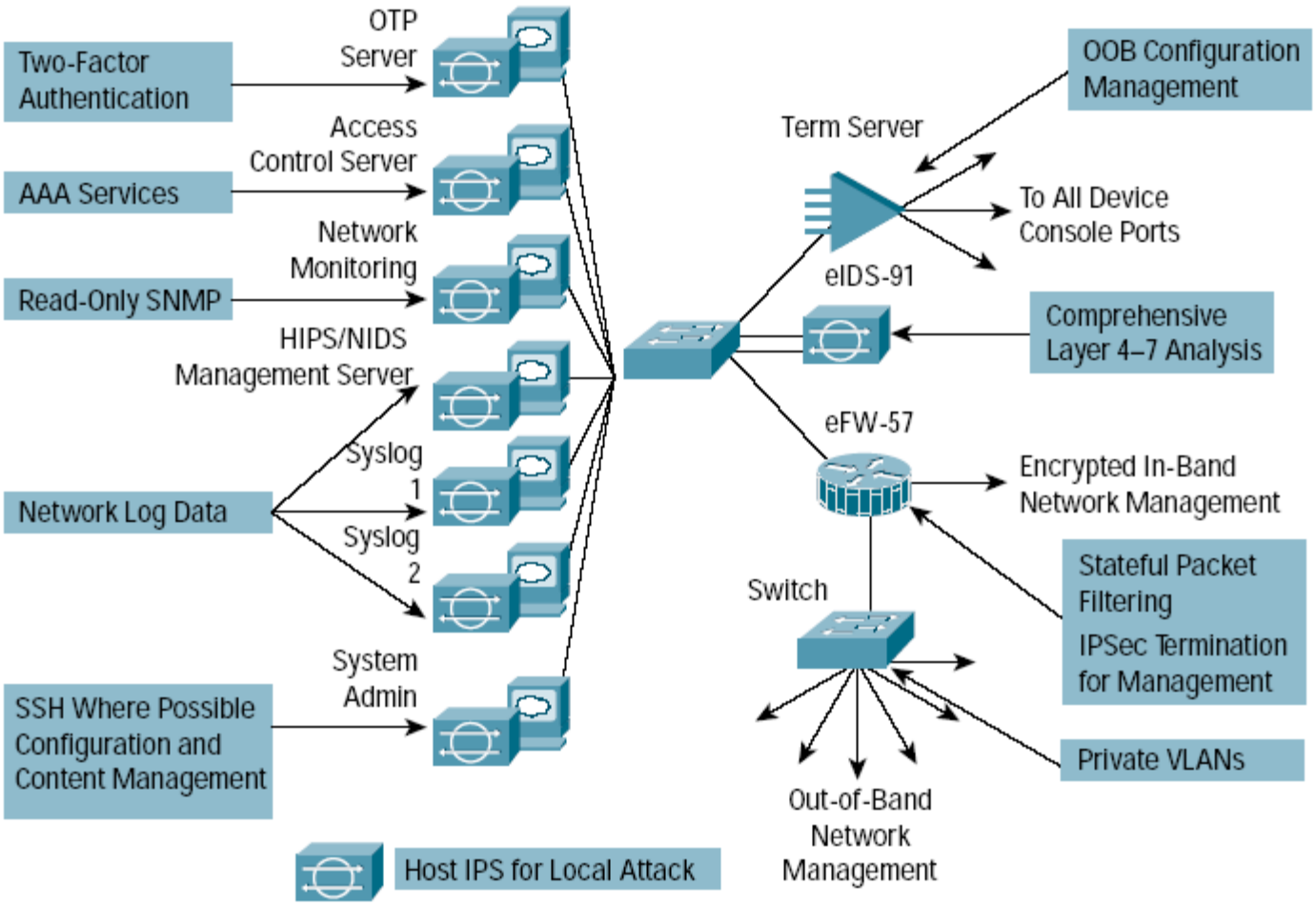
Overall Enterprise Design



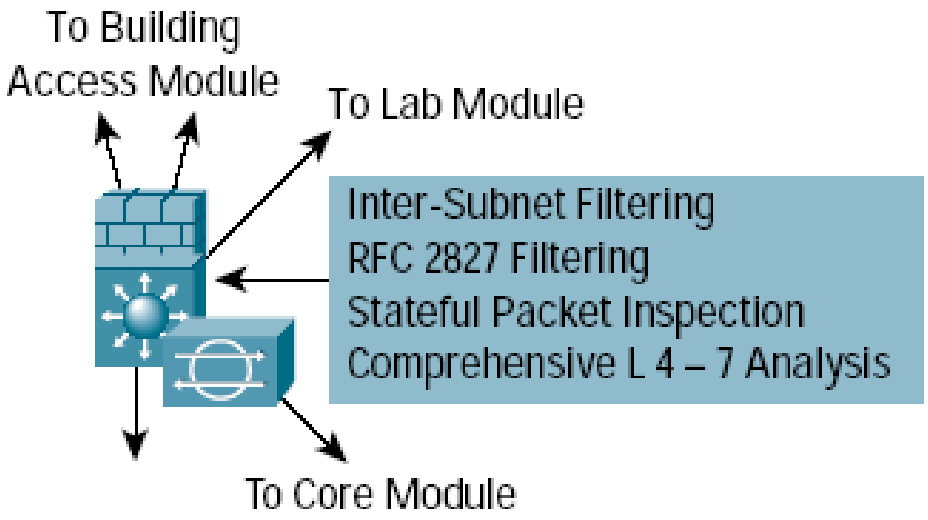
Enterprise Campus



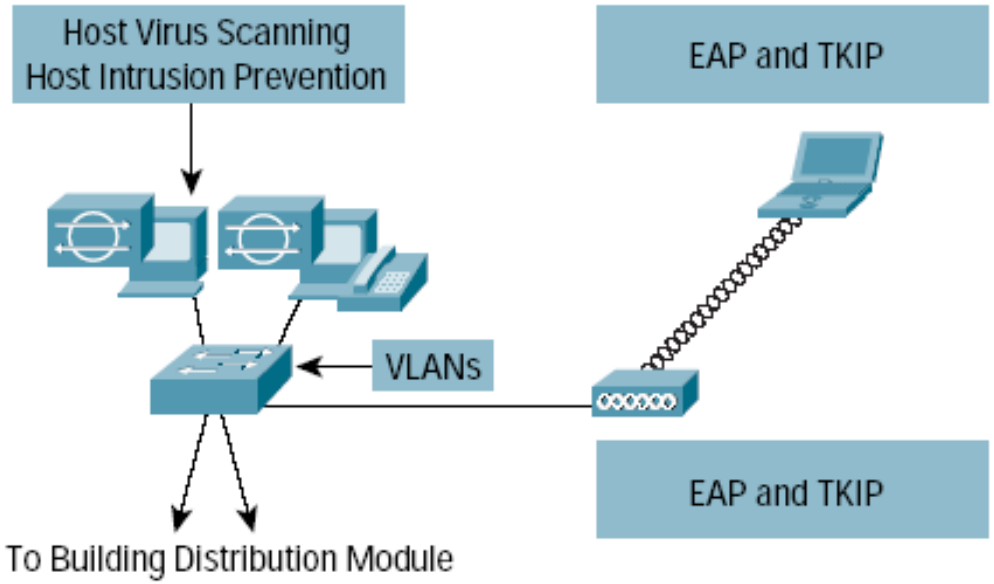
Management Module



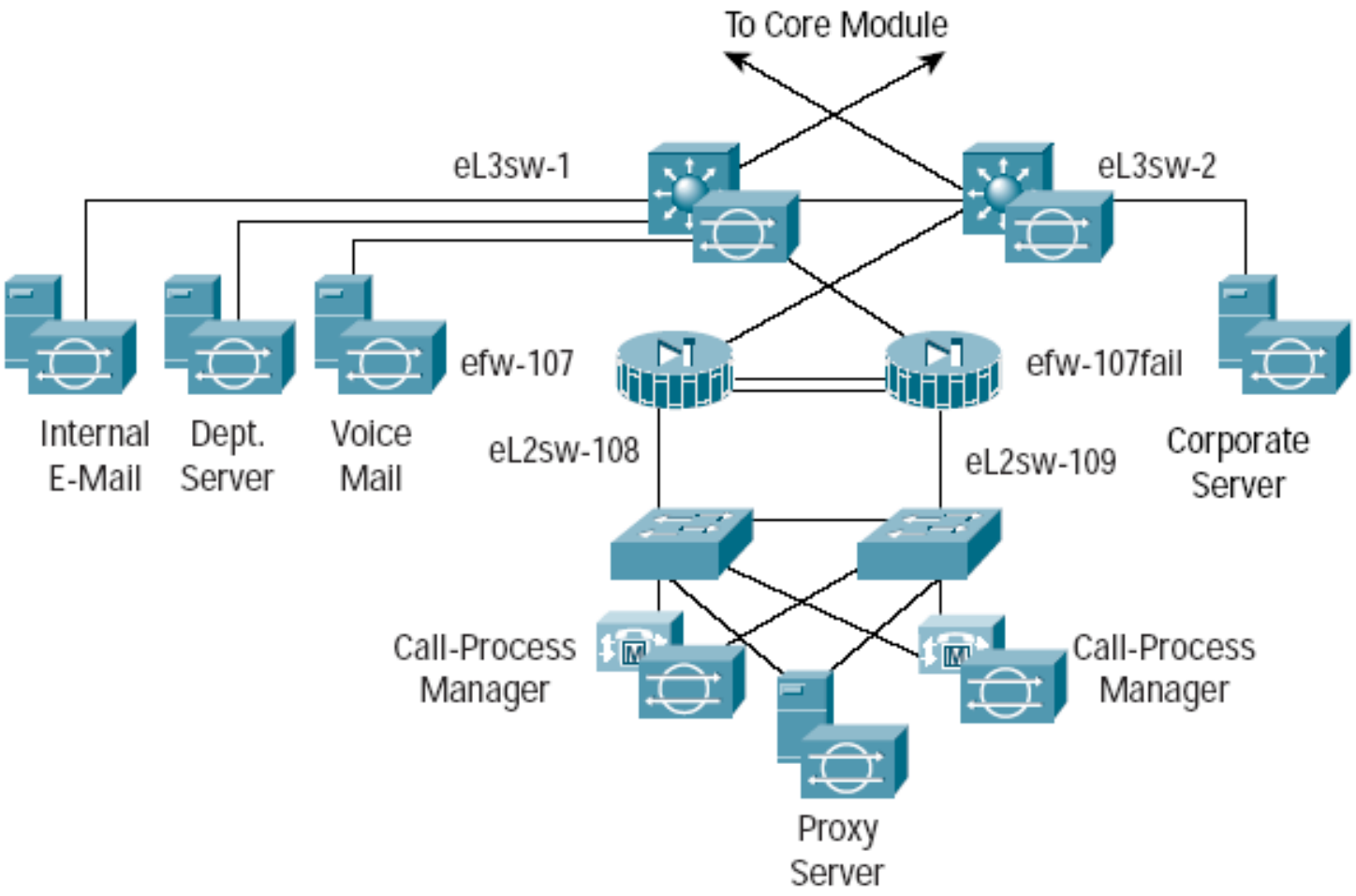
Building Distribution Module



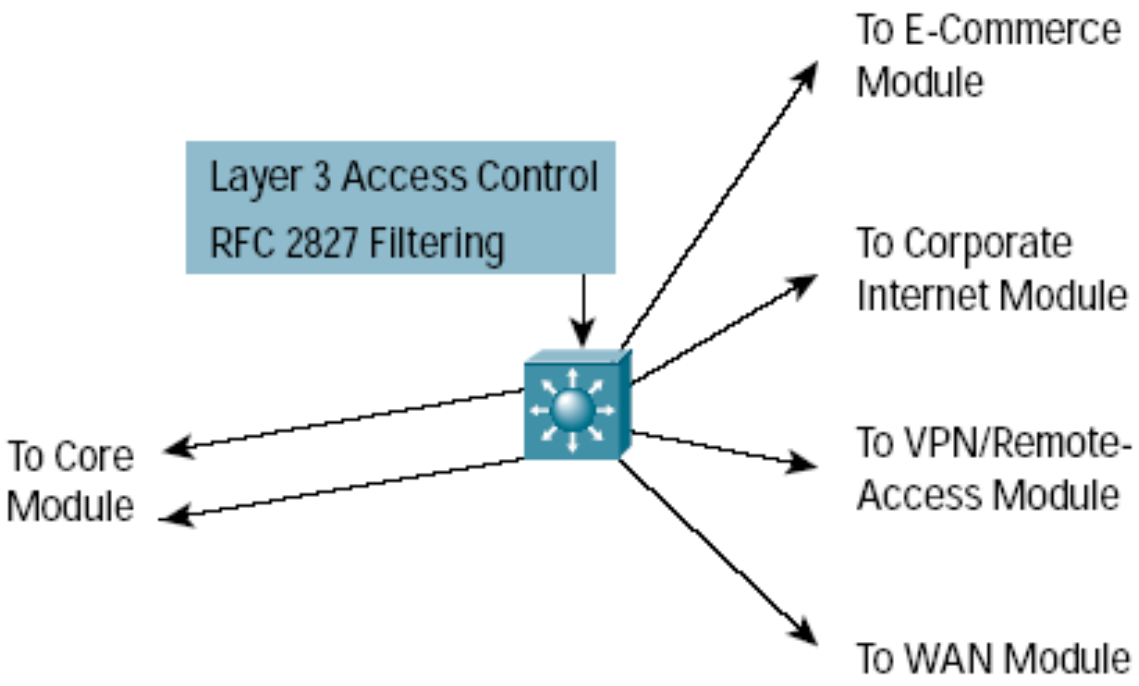
Building Module



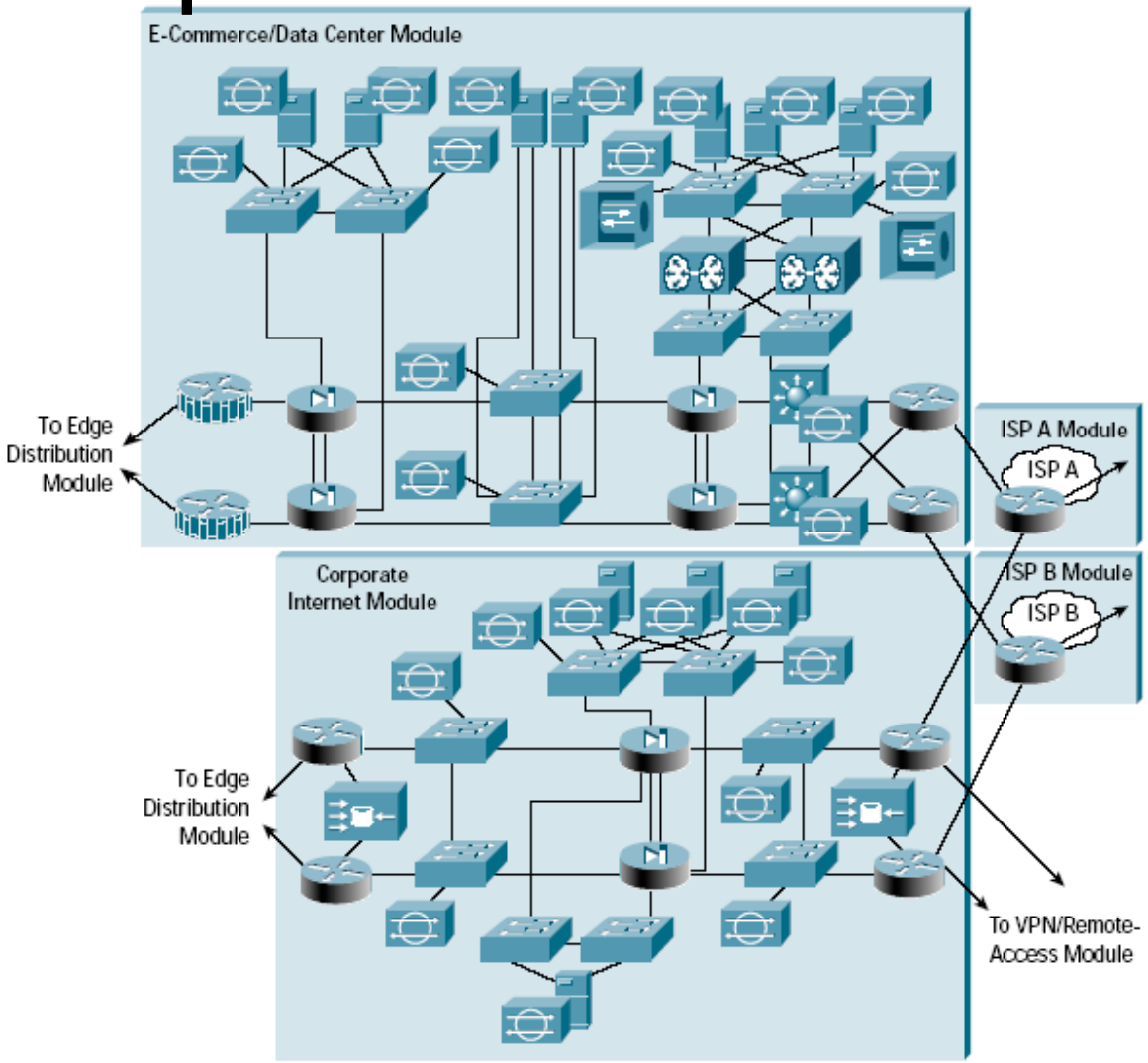
Server Module



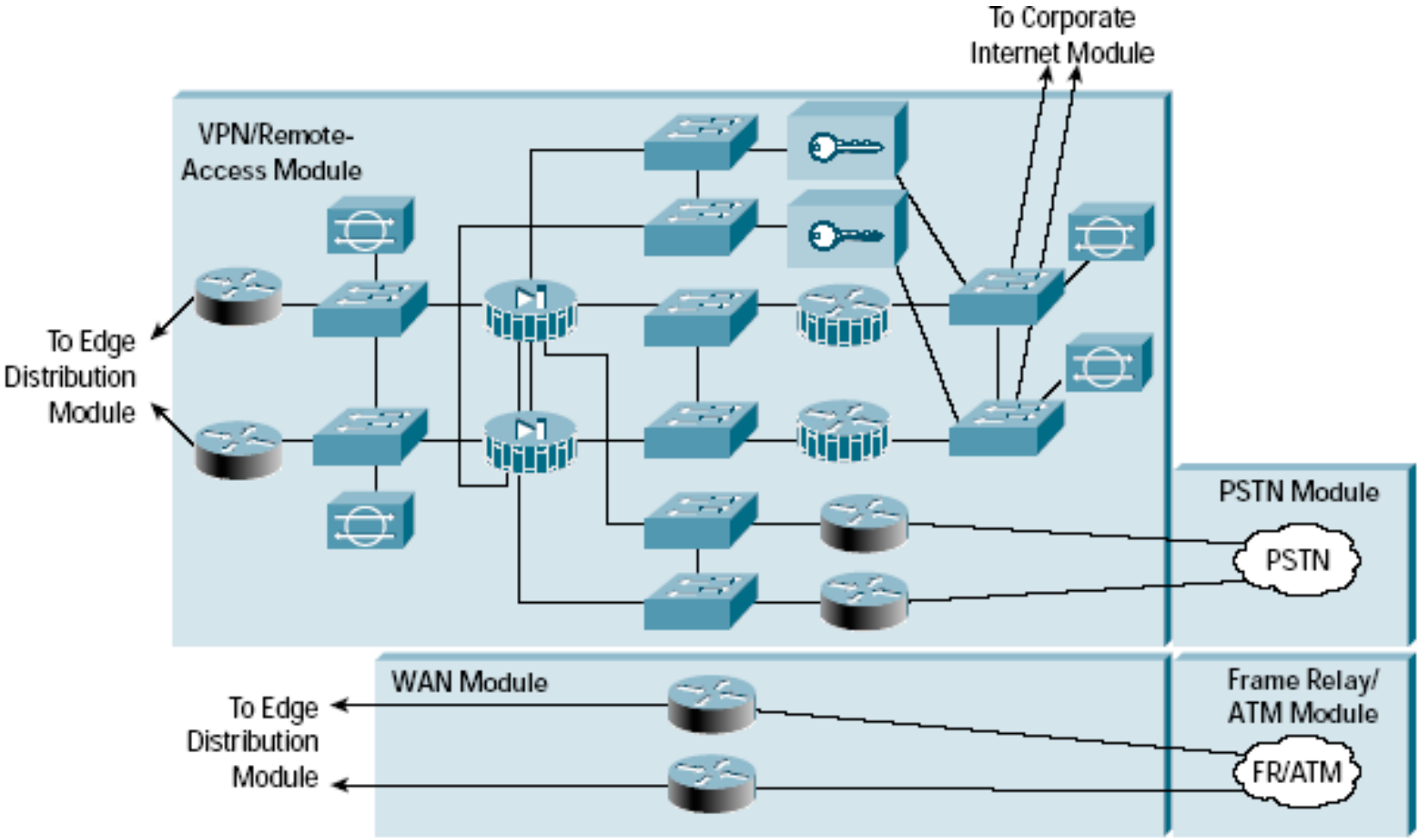
Edge Distribution Module



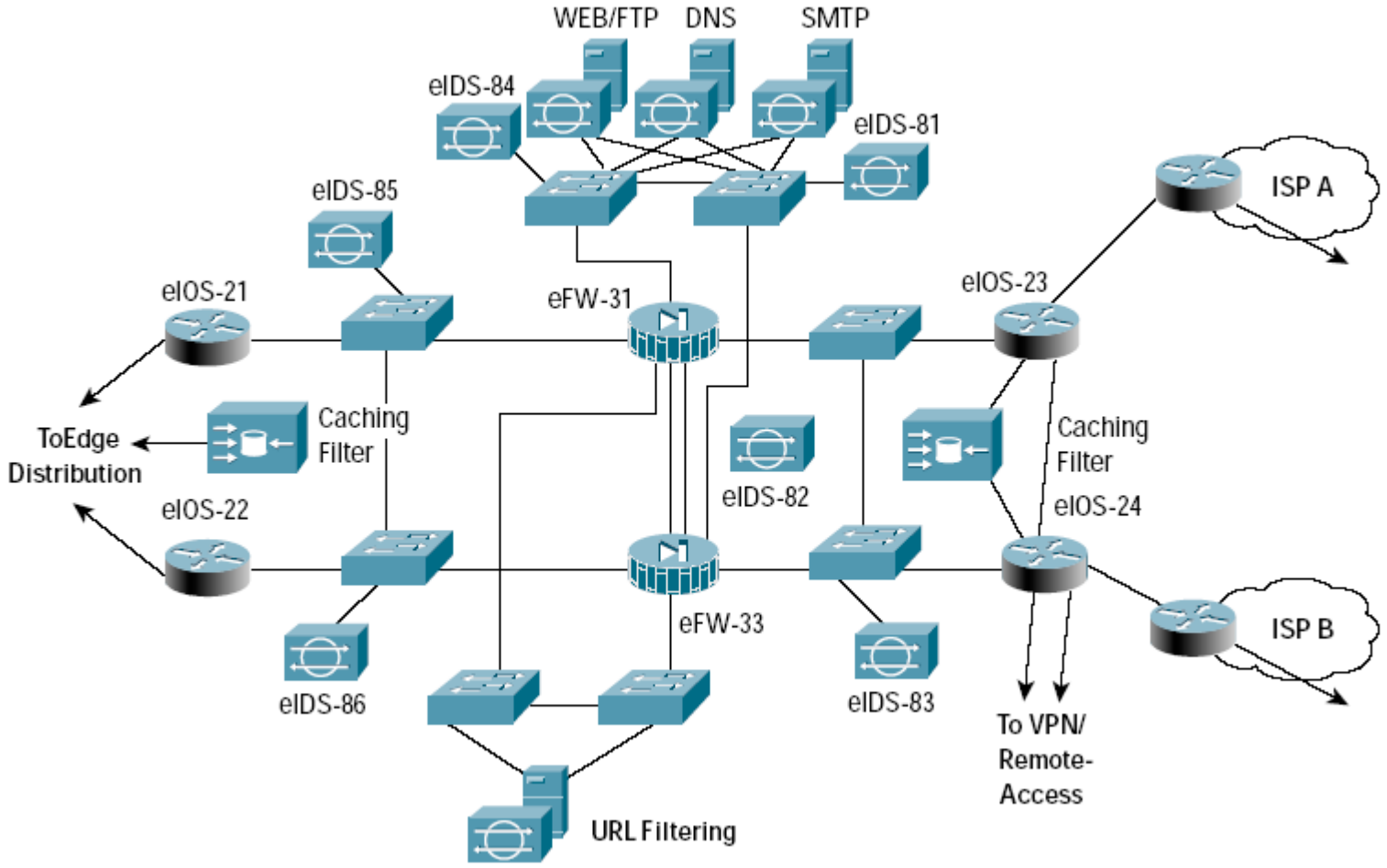
Second portion of architecdture



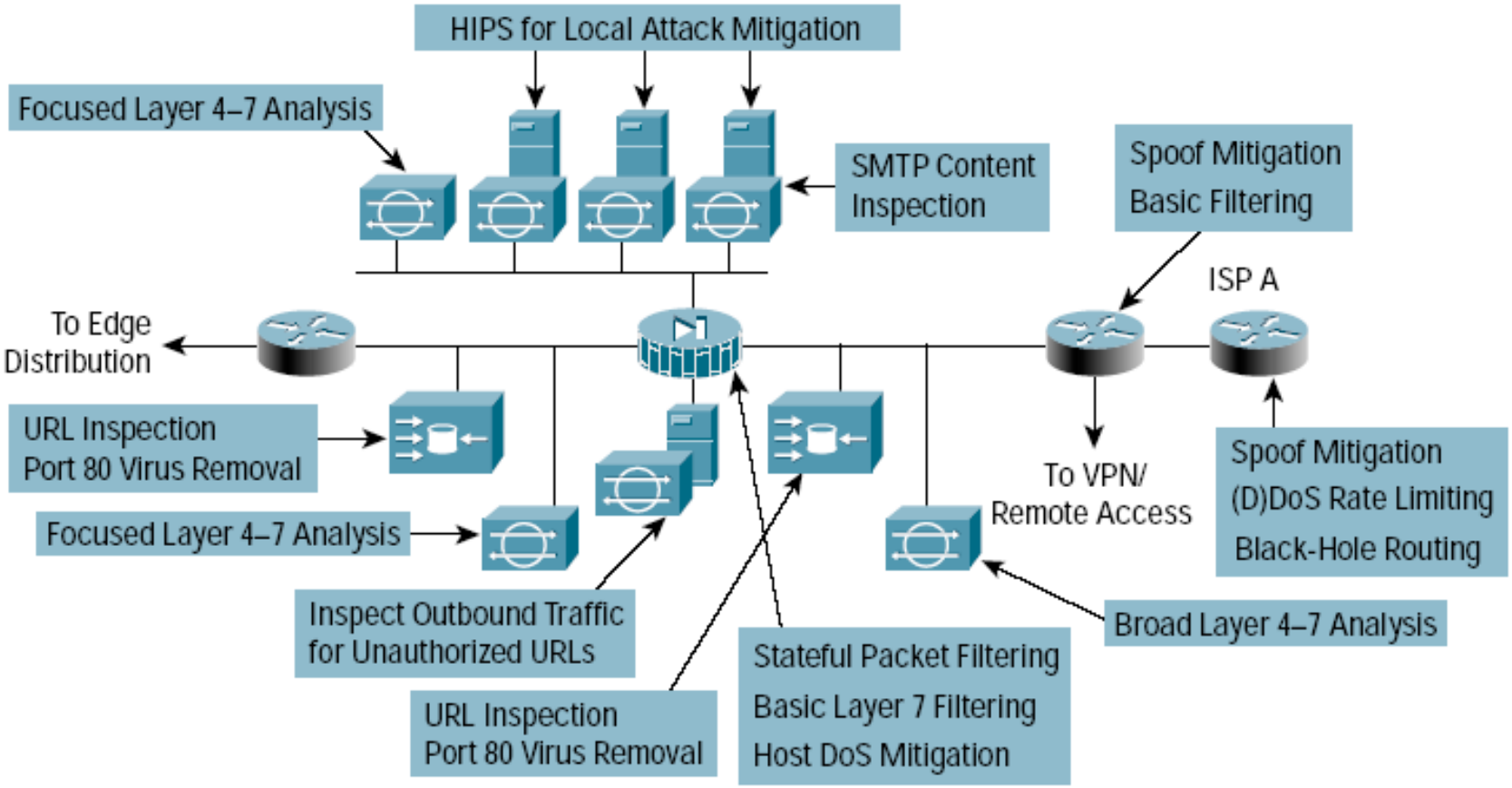
More of the second portion



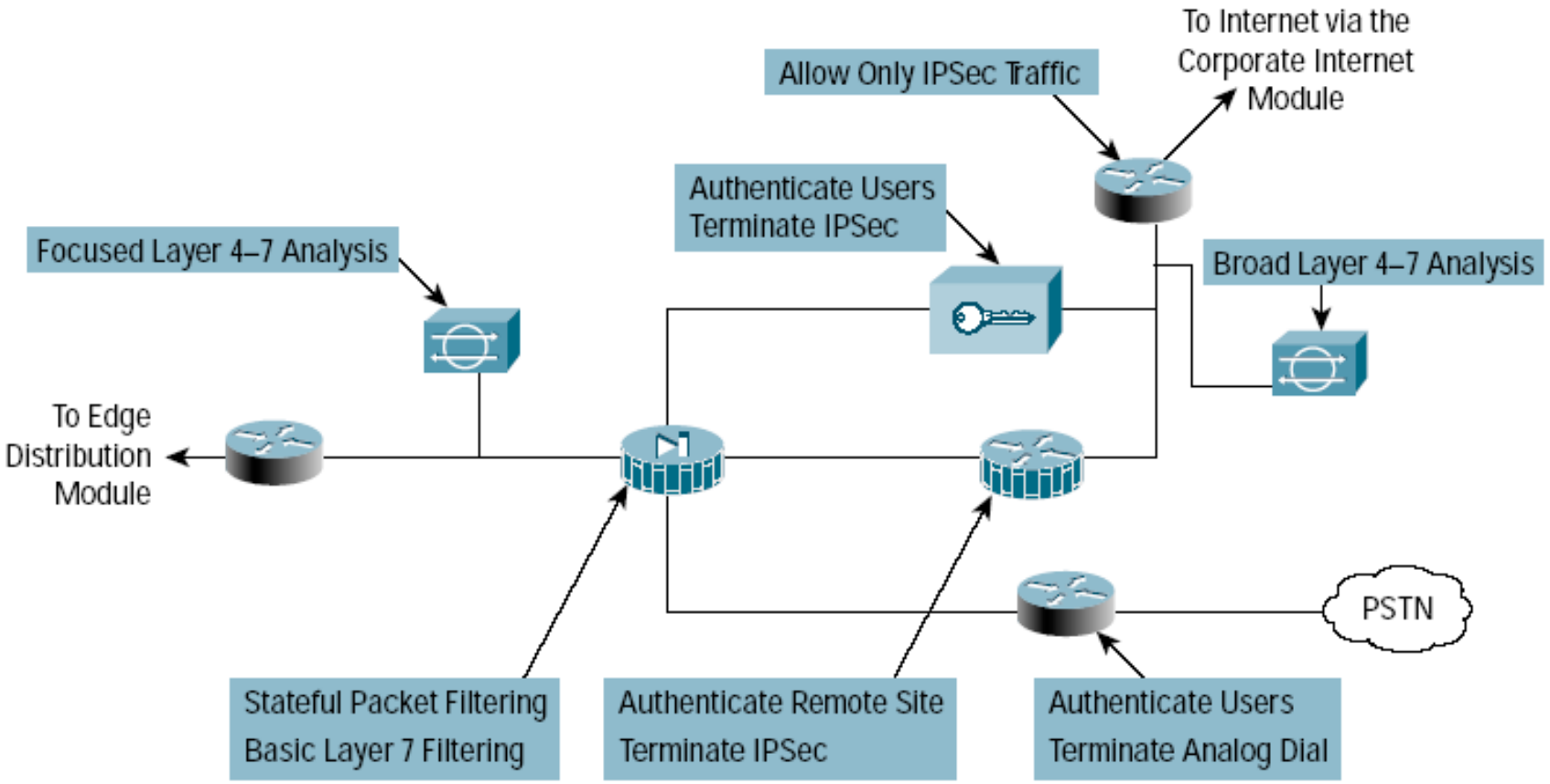
Corporate Internet Module



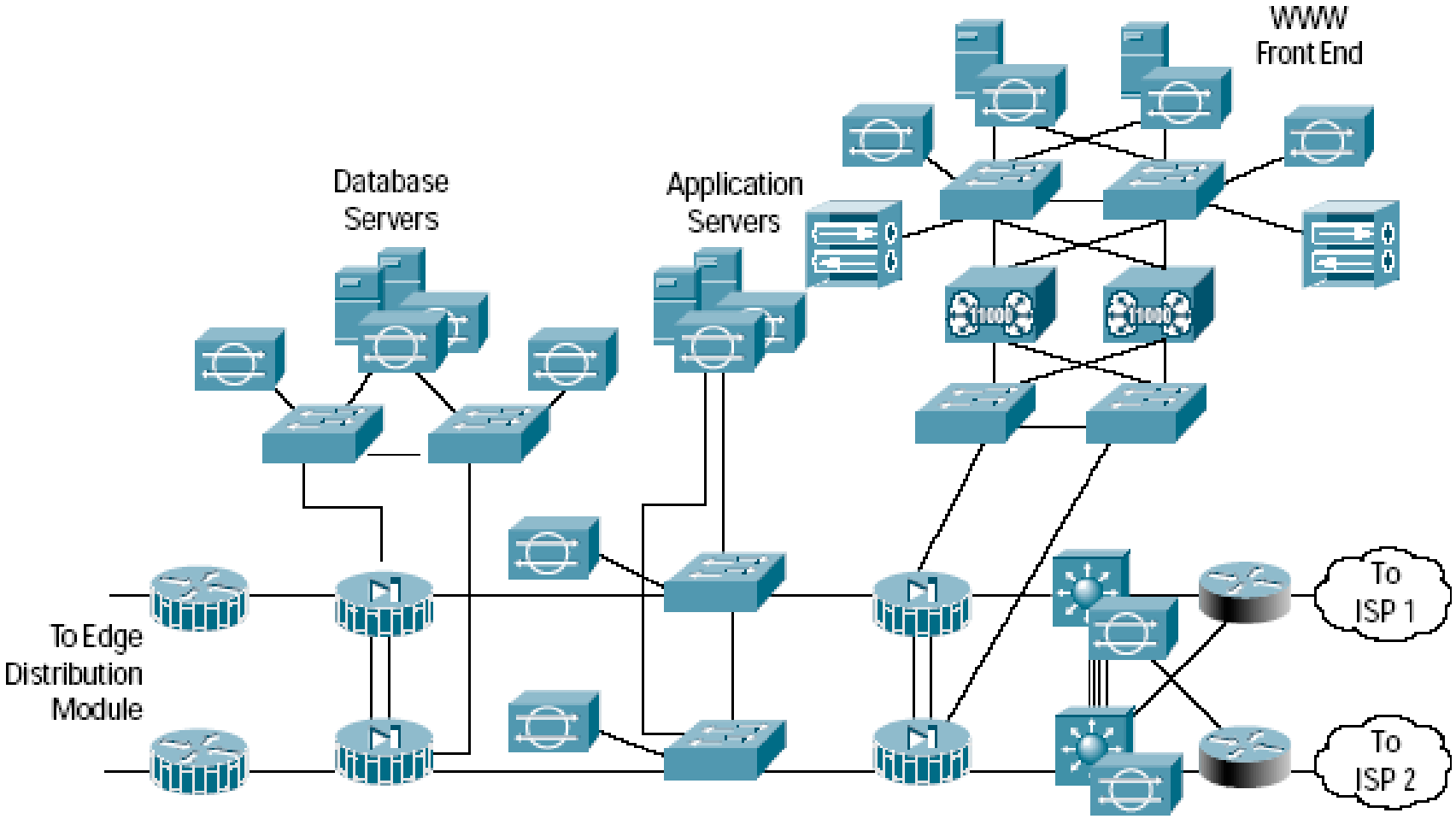
Corporate Internet – Another View



VPN/Remote Access Module



E-Commerce Module



E-Commerce Module, another view