

Network Security Architecture

Cyber Security Lab

Spring 2006

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
- References for security policy
 - SANS policy examples
<http://www.sans.org/resources/policies/>
 - University of Illinois' Security policy
<http://www.ait.s.uillinois.edu/webtrans/live/Site.xml?document=SecurityStandards.xml&focus=null>

Excerpt from the U of I Security Policy

- **B. Categories:**

- Different types of data require different levels of security. The University classifies data into three categories: Public, Proprietary, and Restricted. It is the Data Custodian's responsibility to establish authentication and authorization guidelines for custodial data. Please note that:
 - Public data can generally be made available or distributed to the general public.
 - Proprietary data is for internal University use and not for external distribution.
 - Restricted (moderately or highly sensitive) data is to be used only by individuals who require it in the course of performing their University responsibilities, or data which is protected by federal and/or state regulations

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

Security Architectures

- Can be found for many general system elements
 - J2EE applications
 - Client server applications
 - .Net applications

Cisco SAFE

- A series of network security architecture blueprints
 - http://cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_package.html
 - 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
 - http://cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml

Cisco Icon Overview

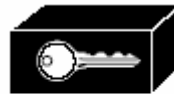
- Complete overview at <http://www.cisco.com/warp/public/503/2.html>



PIX
Firewall



Router



VPN
Gateway



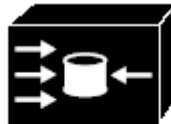
Workgroup
switch



AccessPoint



Communications
server



Content
Engine
(Cache Director)



Content Service
Switch 1100

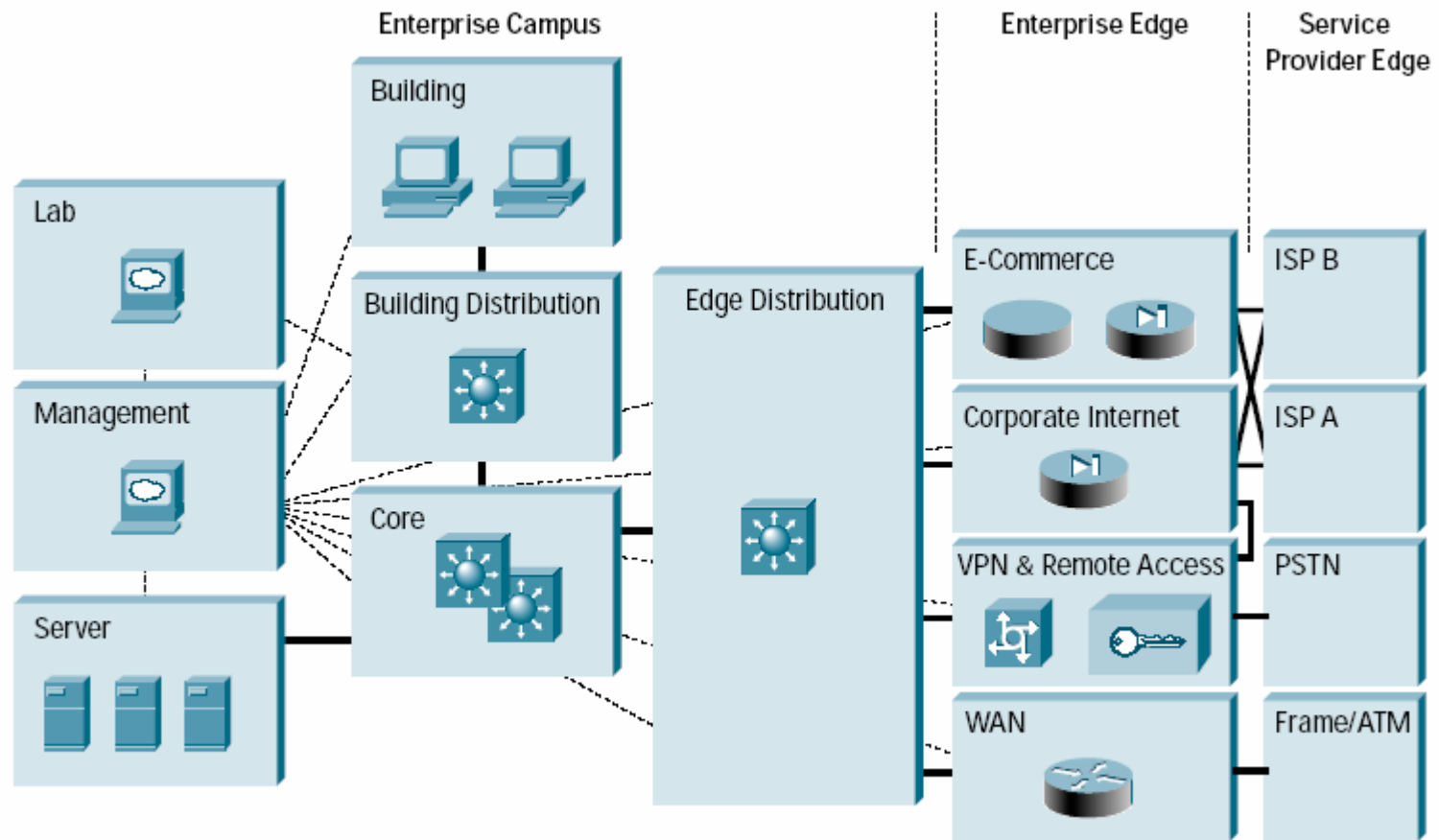


Layer 3
Switch

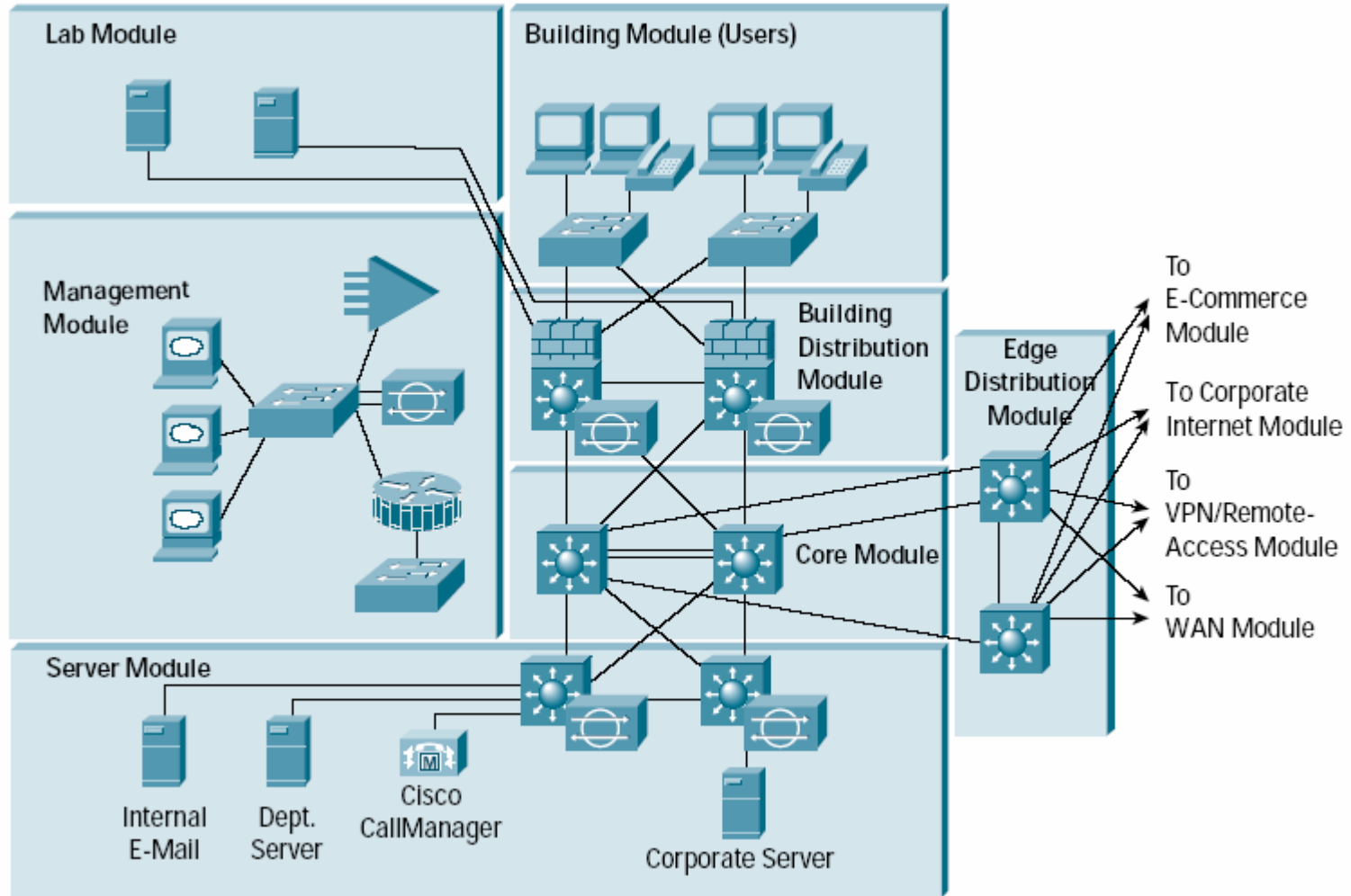


NetRanger

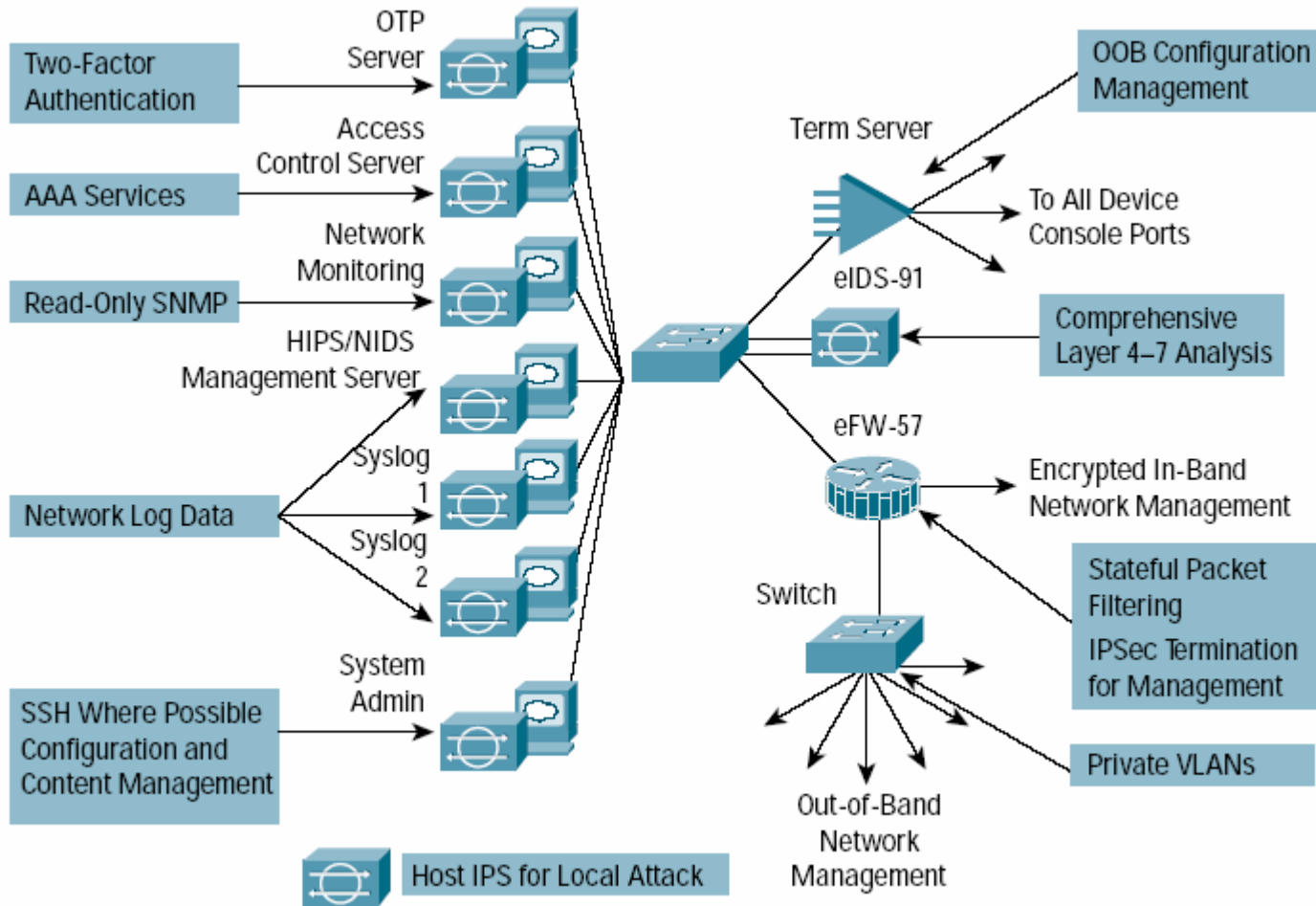
Overall Enterprise Design



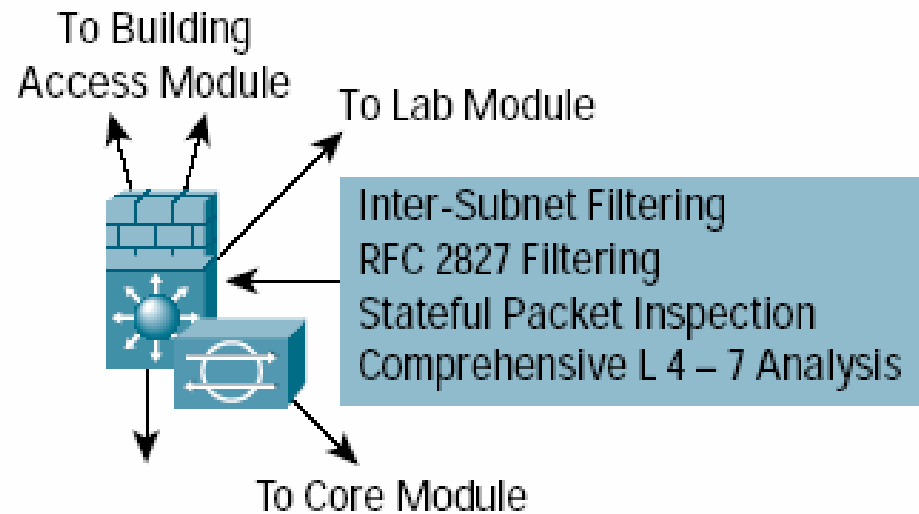
Enterprise Campus



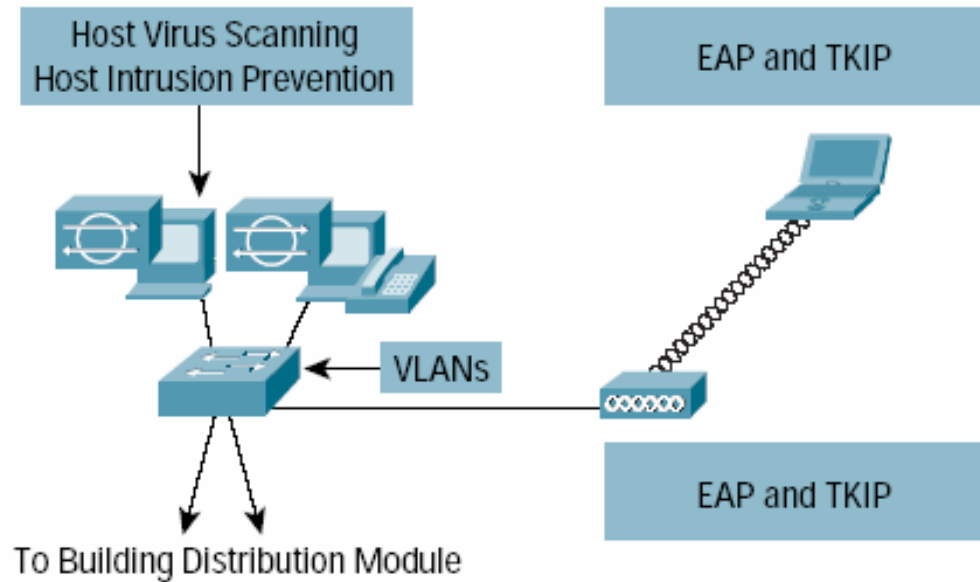
Management Module



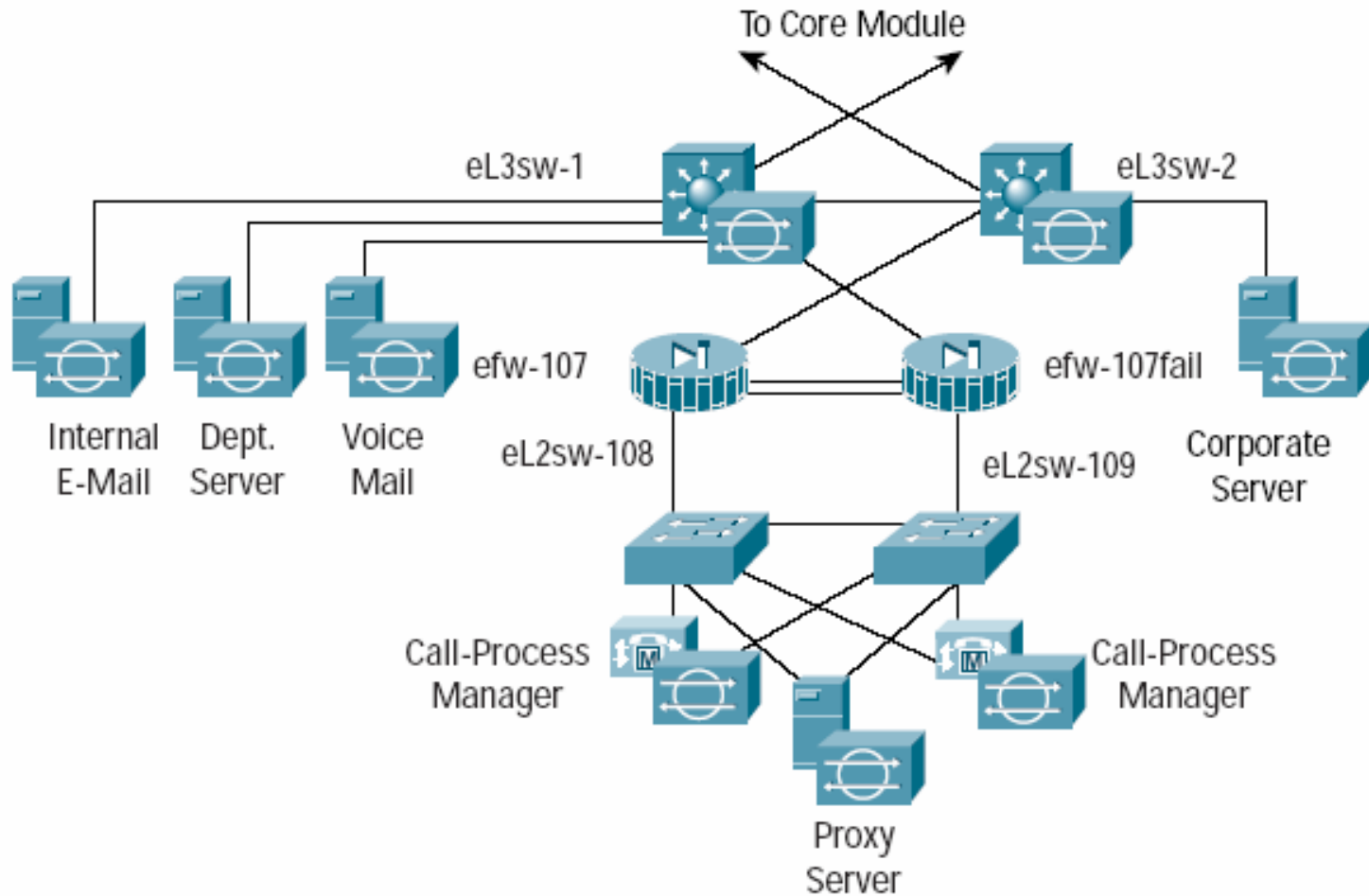
Building Distribution Module



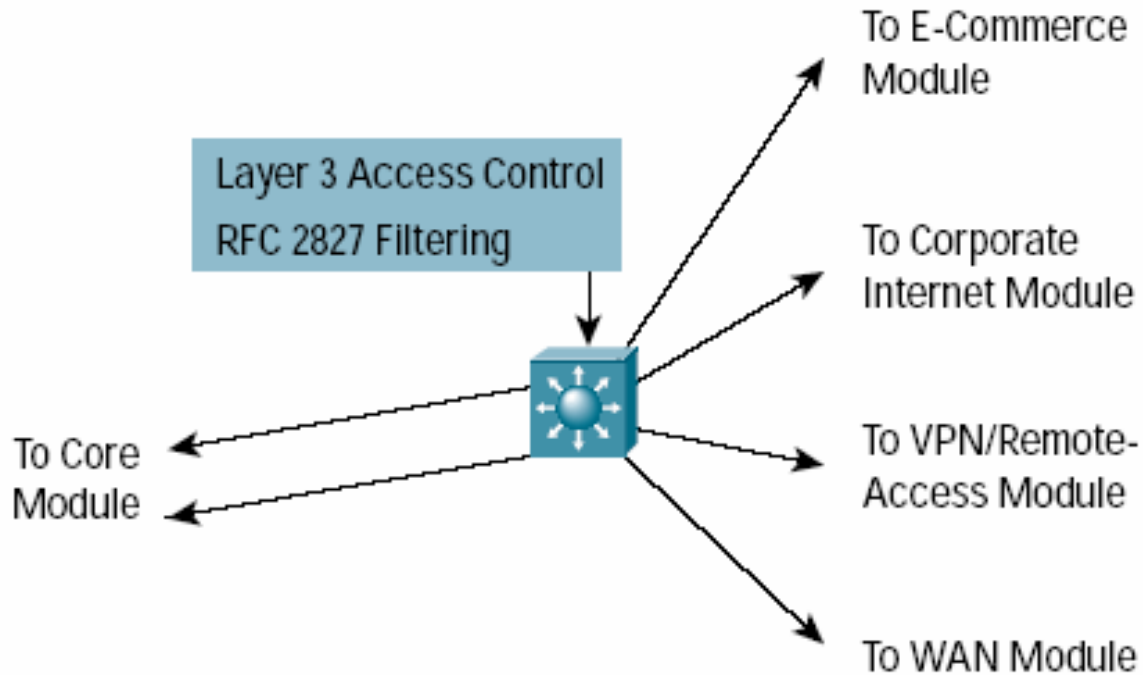
Building Module



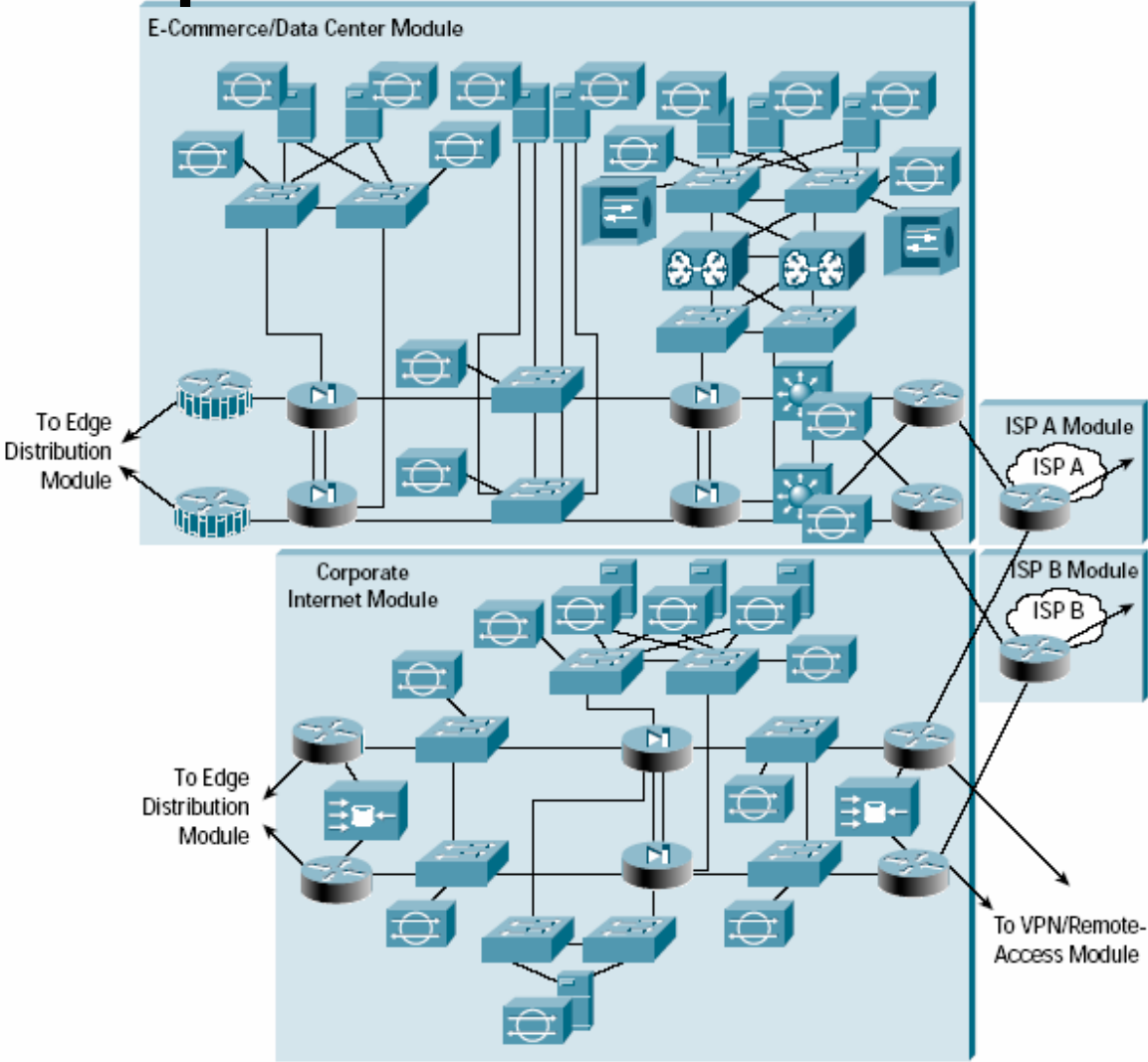
Server Module



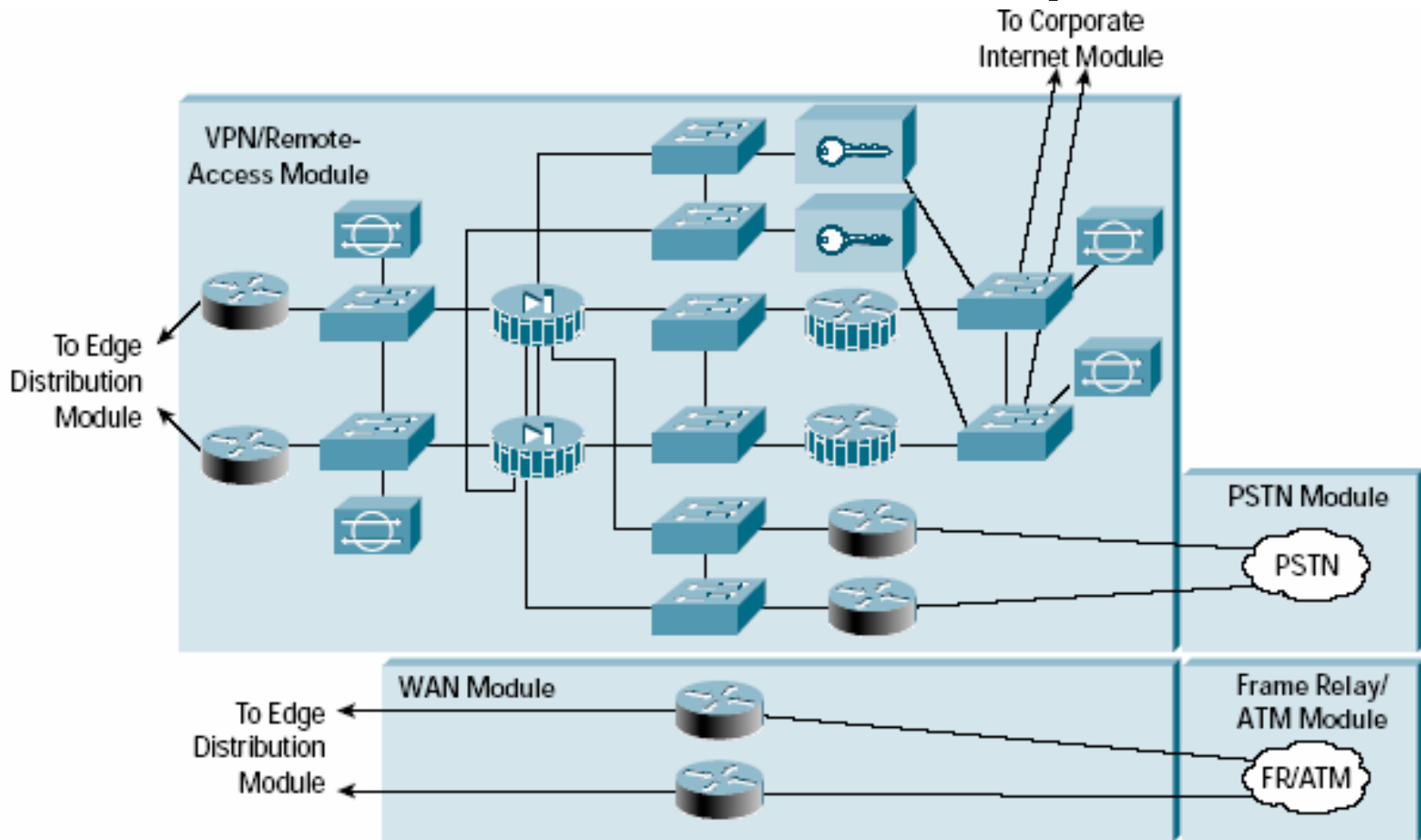
Edge Distribution Module



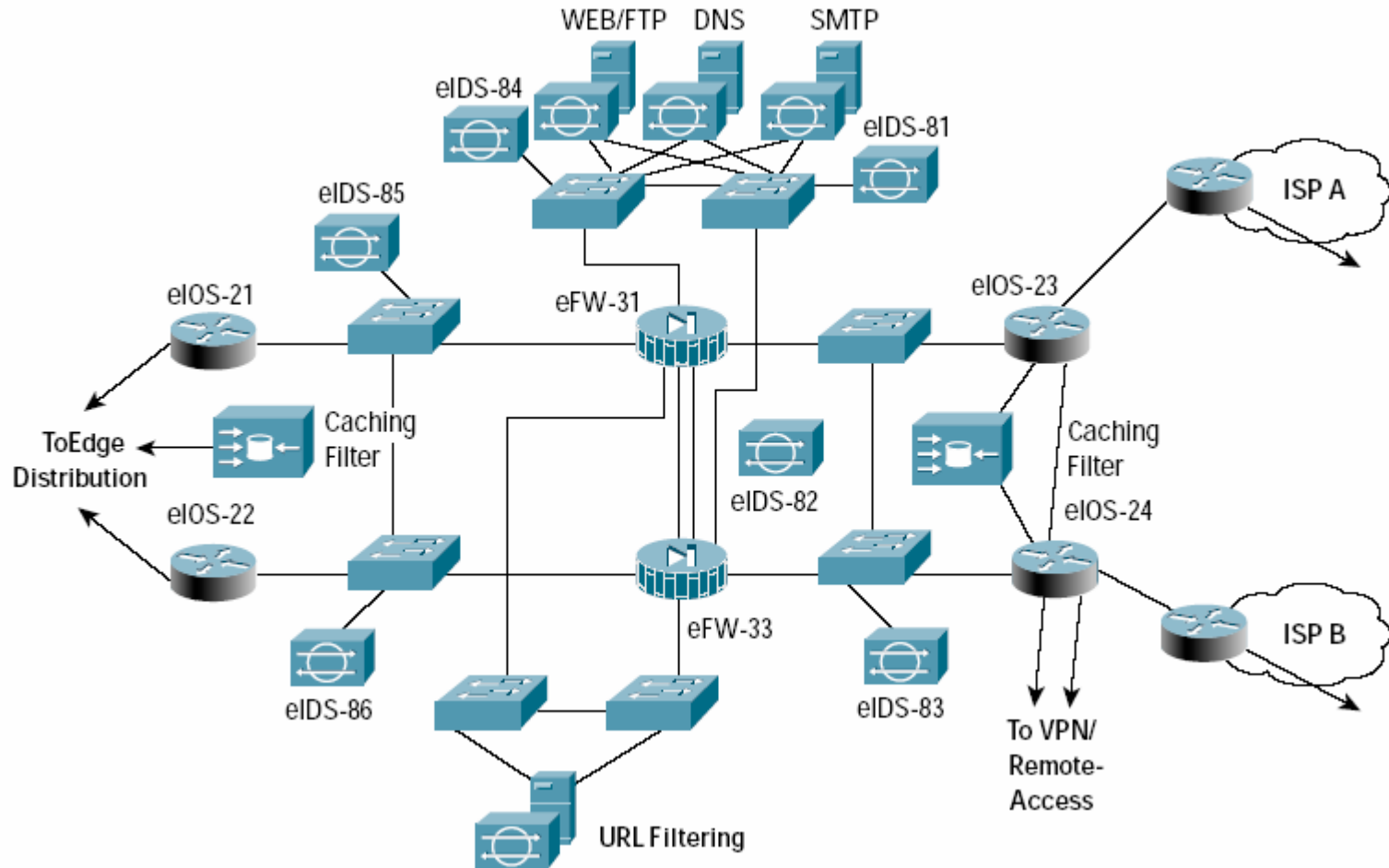
Second portion of architecture



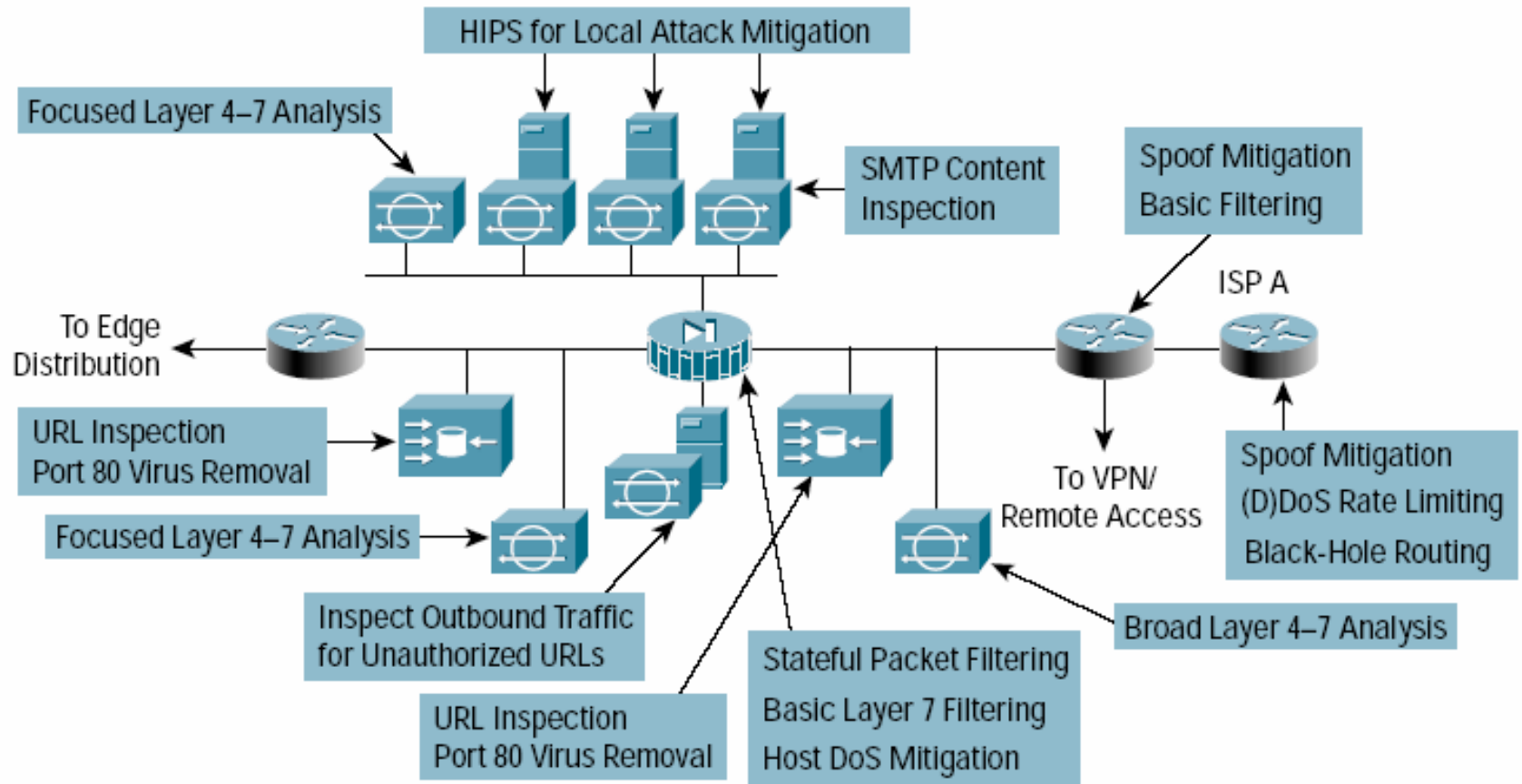
More of the second portion



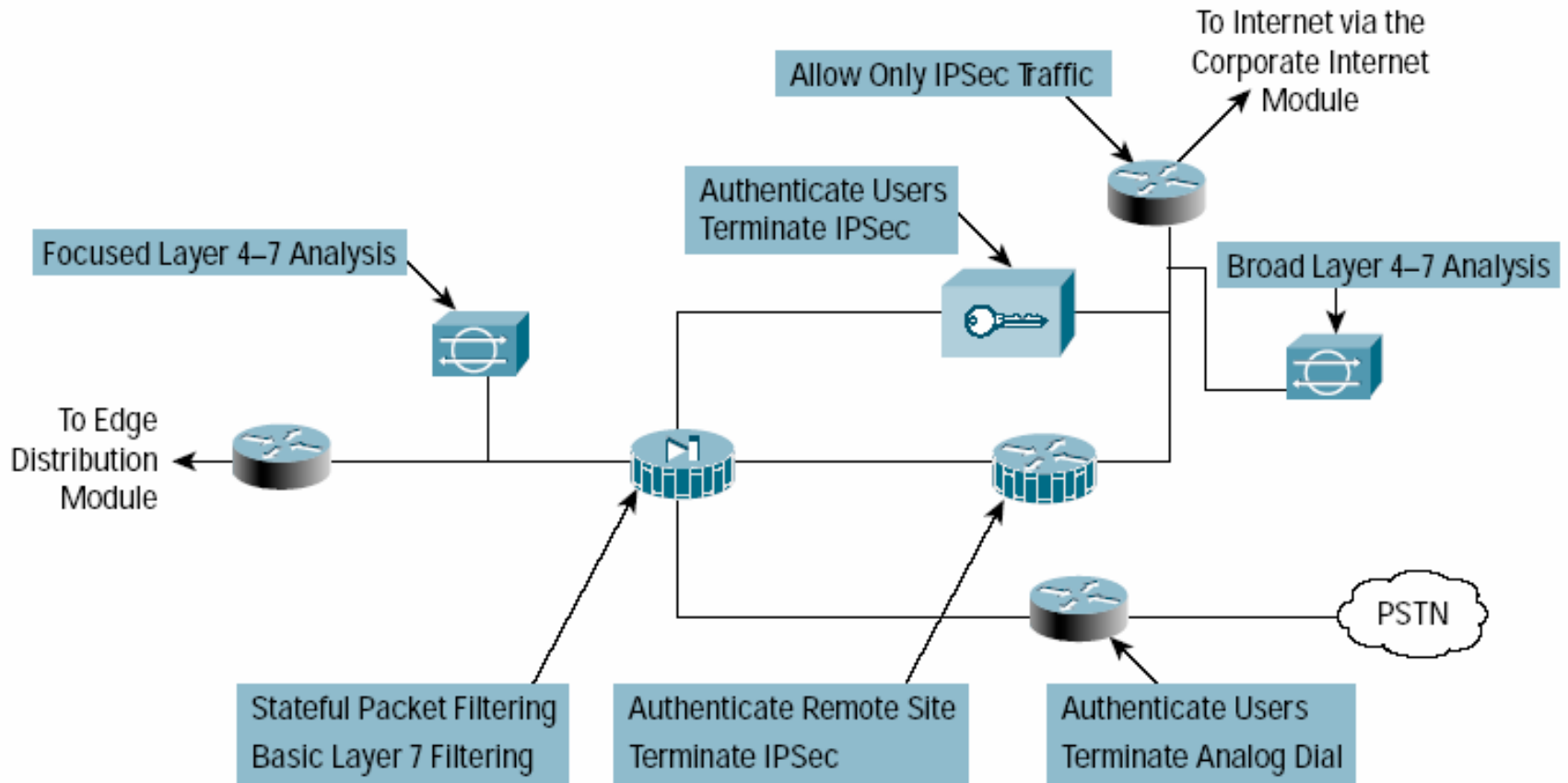
Corporate Internet Module



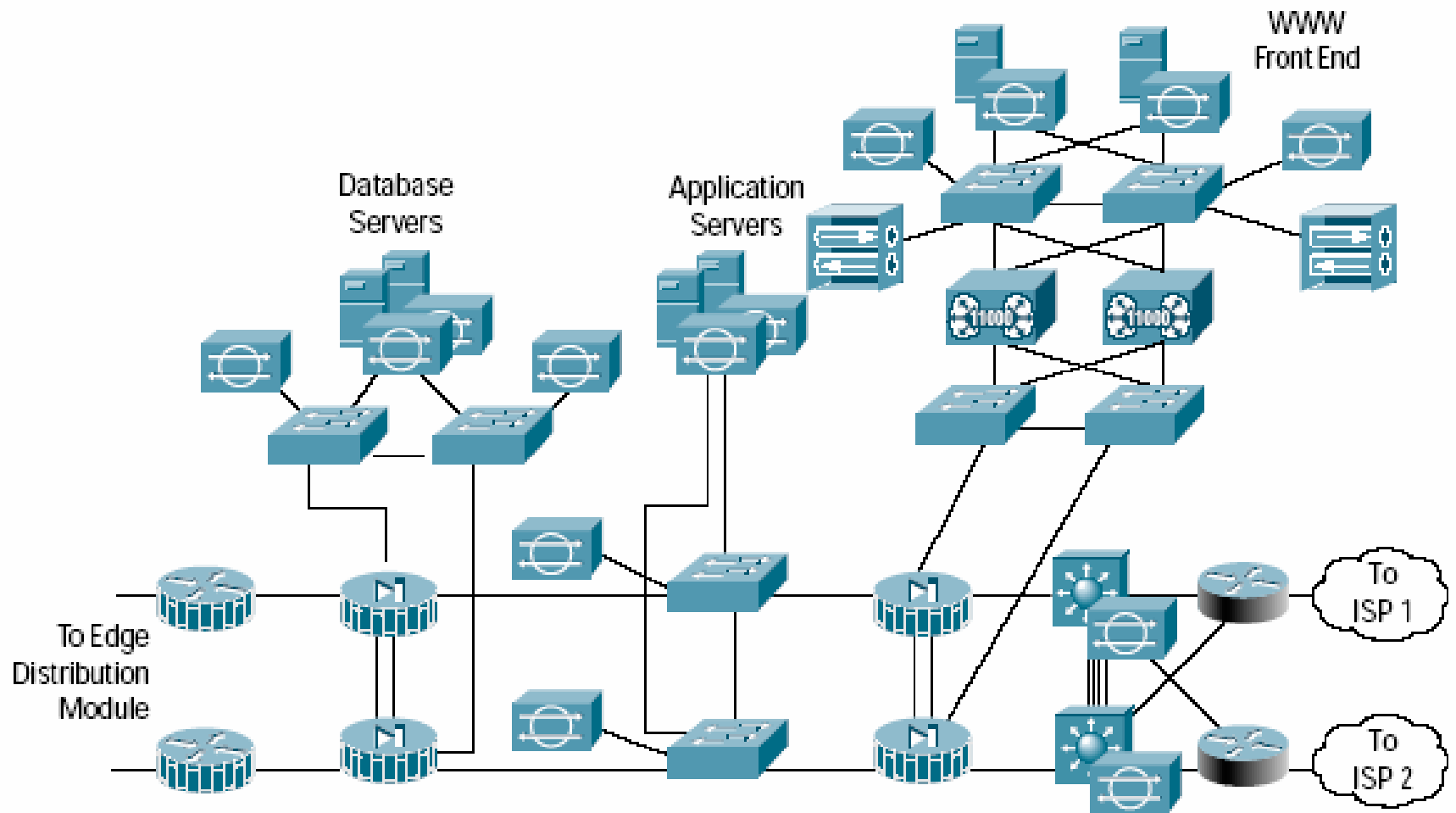
Corporate Internet – Another View



VPN/Remote Access Module



E-Commerce Module



E-Commerce Module, another view

