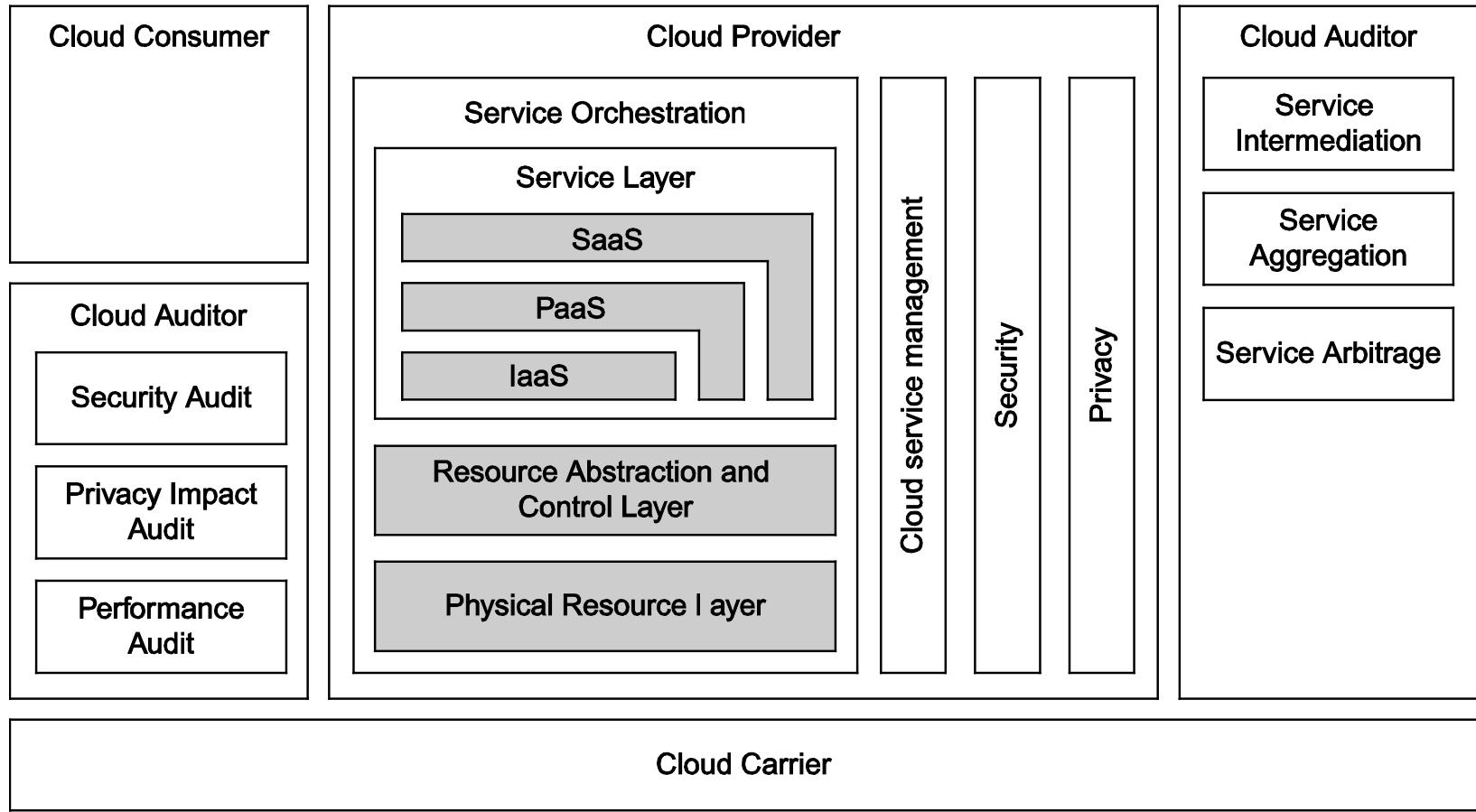


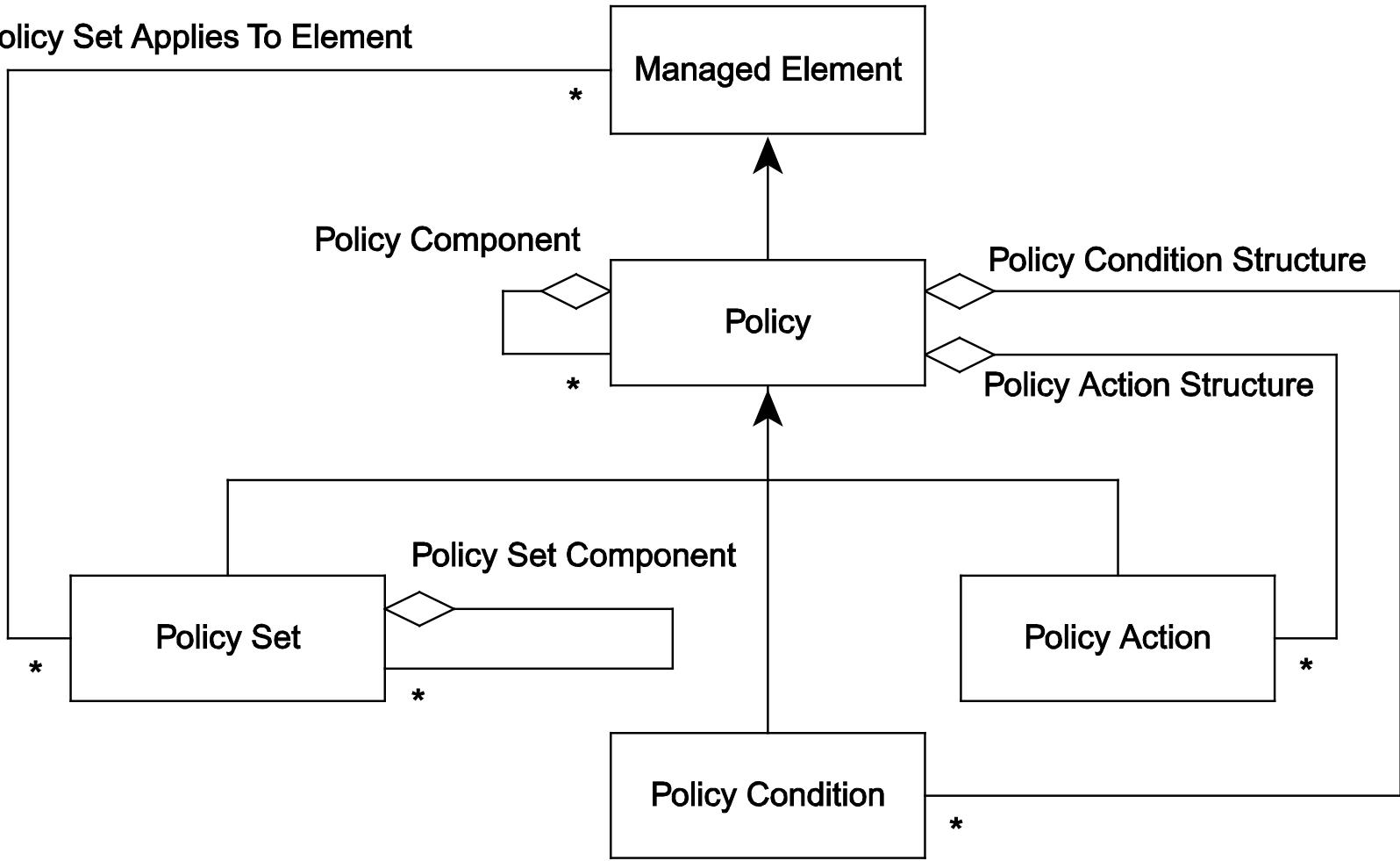
Chapter 23

Policy-driven System Management

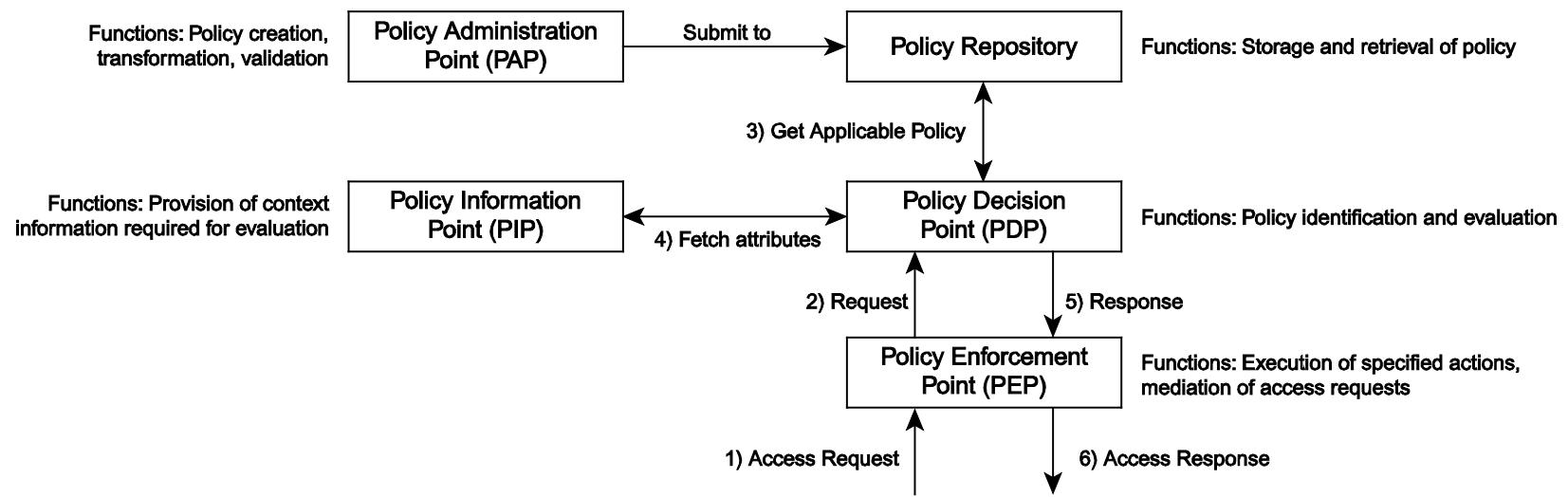


f23-01-9780123943972

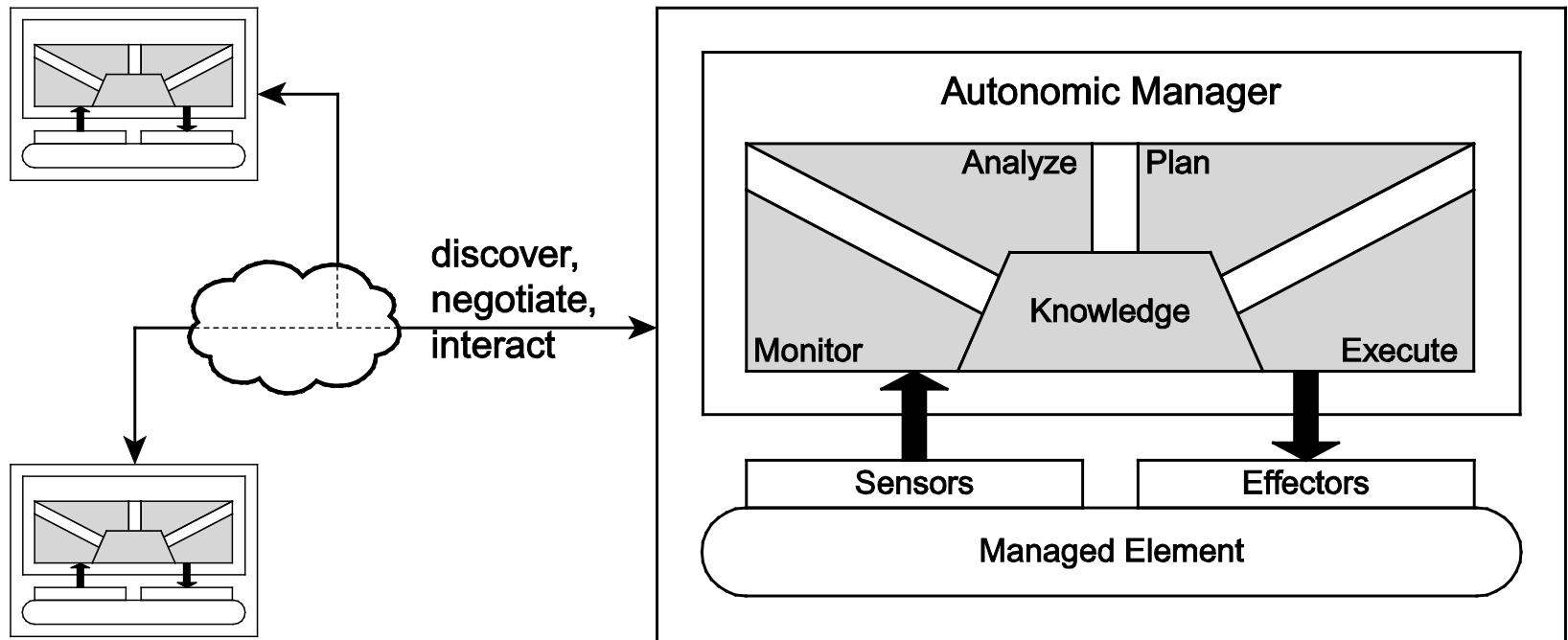
Policy Set Applies To Element



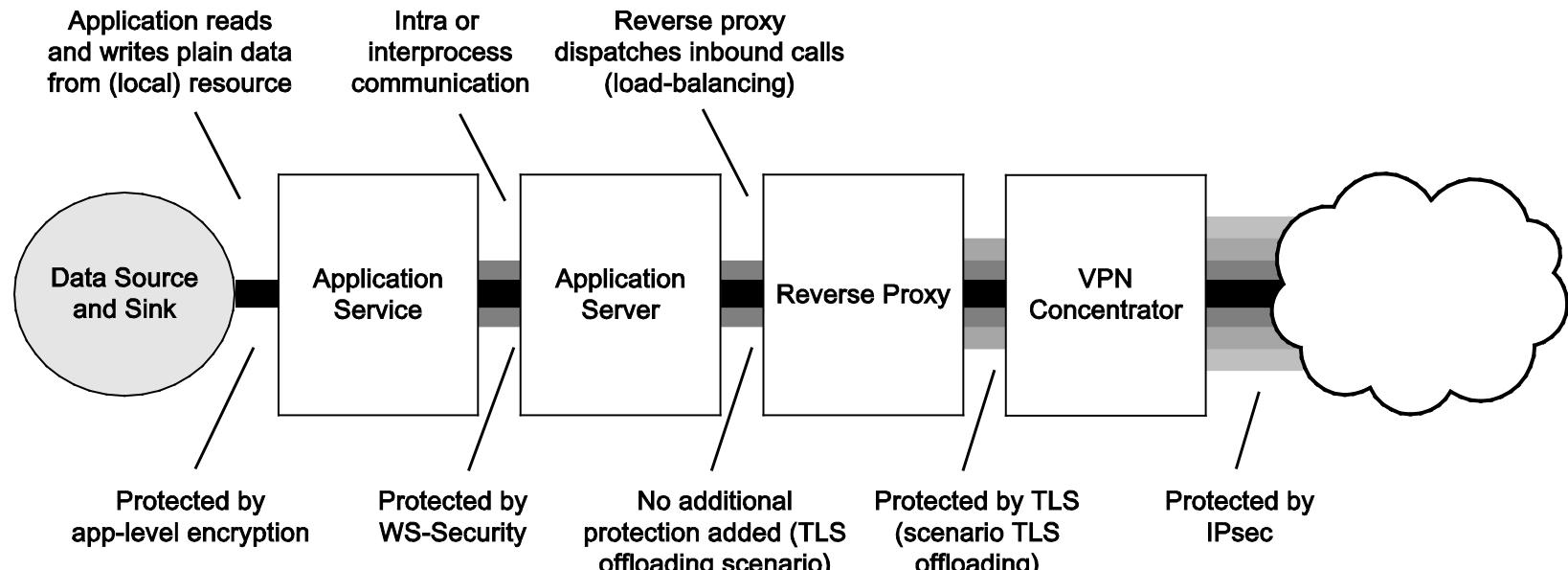
f23-02-9780123943972



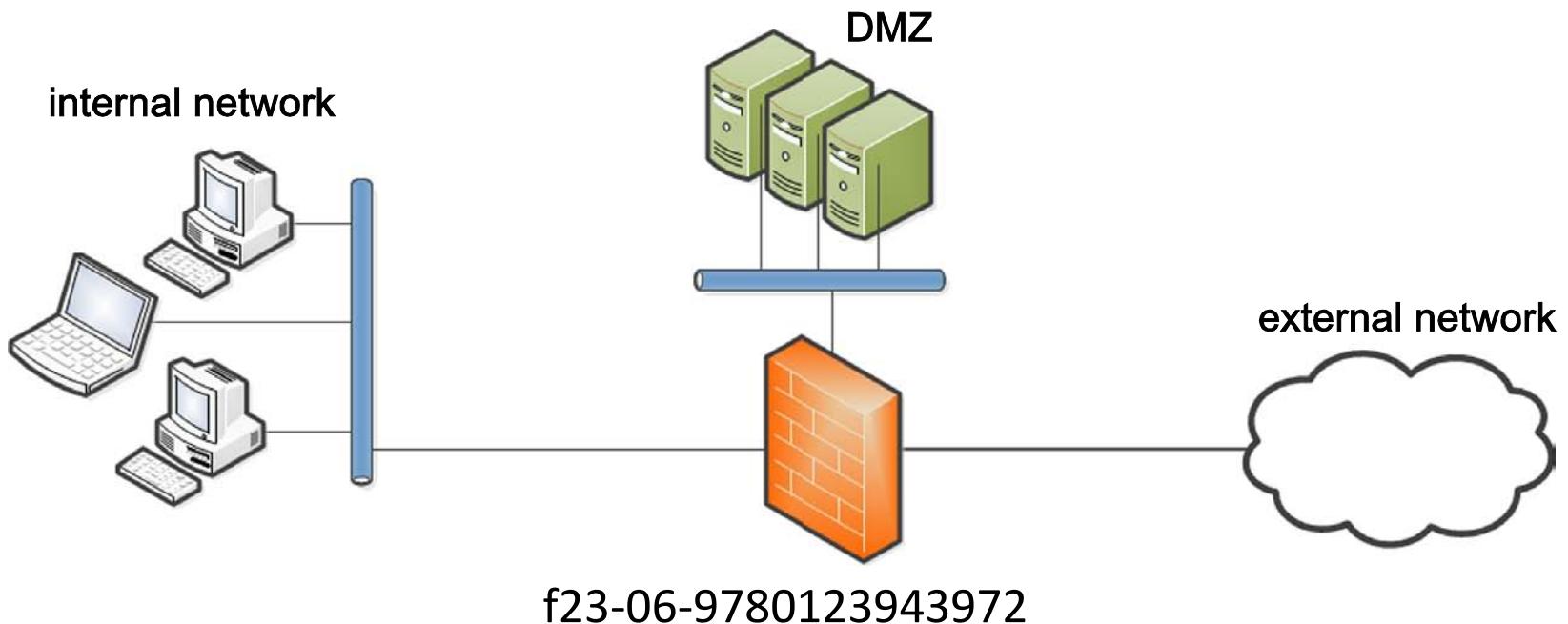
f23-03-9780123943972

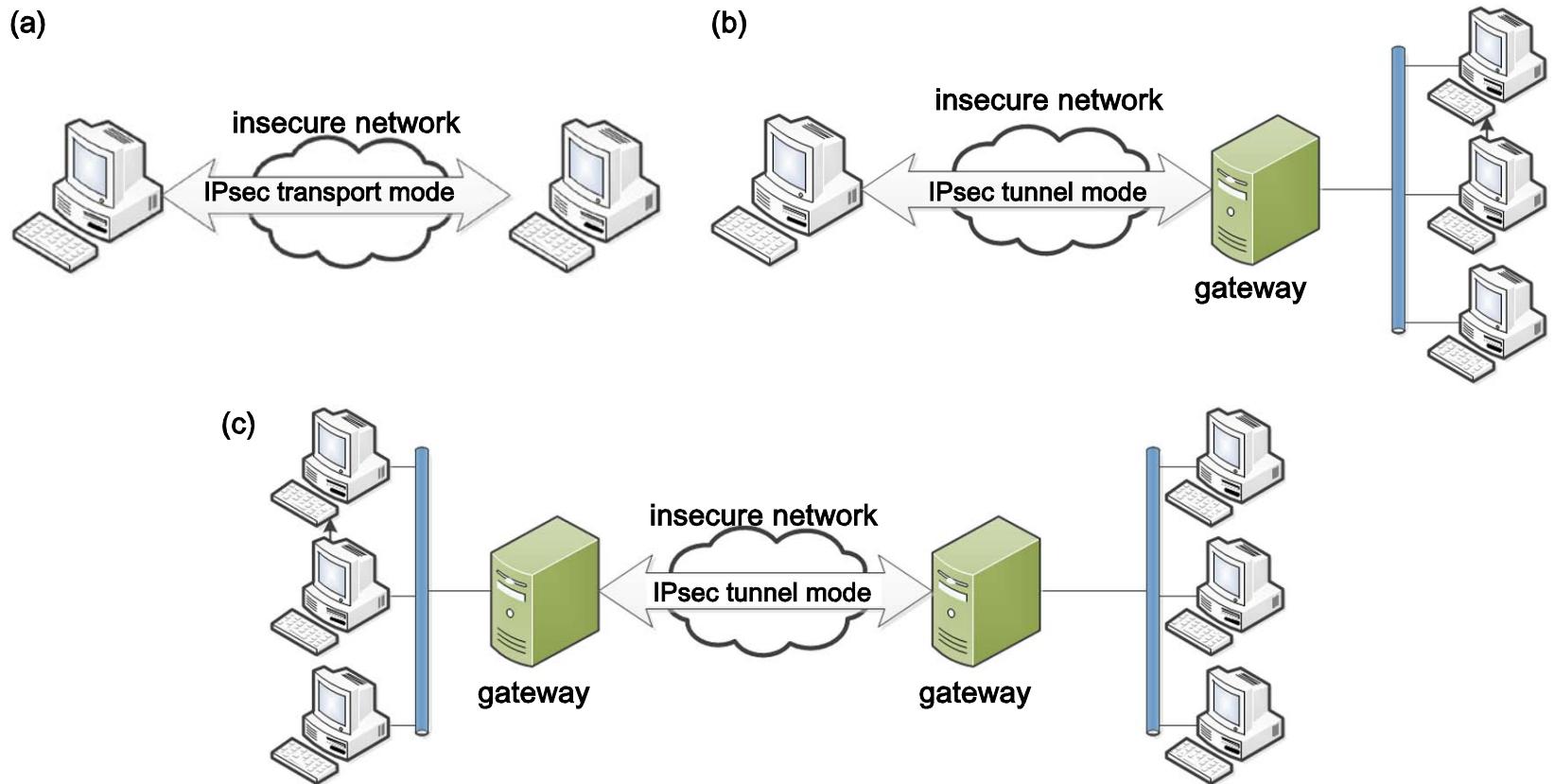


f23-04-9780123943972

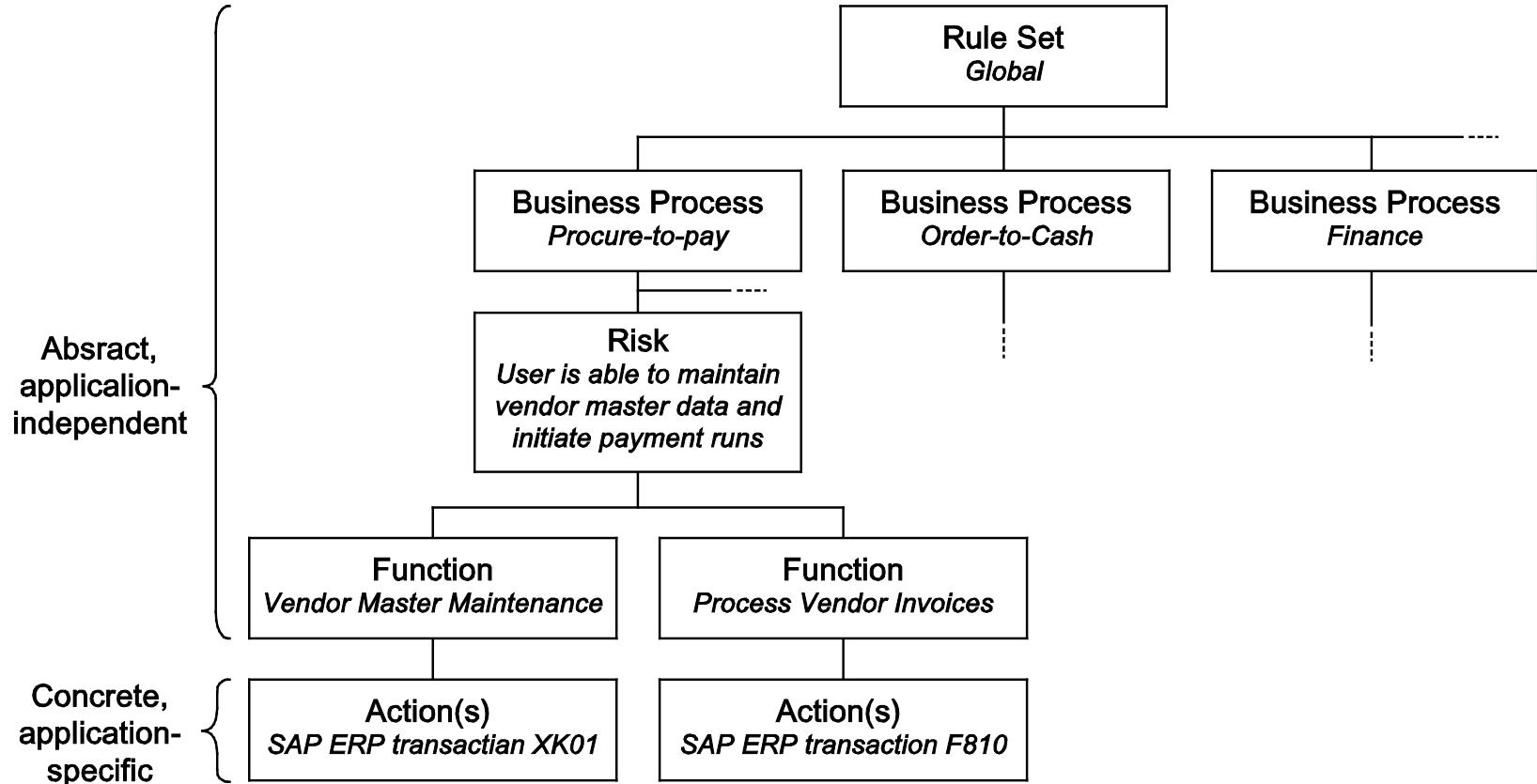


f23-05-9780123943972





f23-07-9780123943972



f23-08-9780123943972

Group Policy Management

File Action View Window Help

Group Policy Management

Forest: corp

Domains

acme.corp

- Default Domain Policy
- GPO_Vintela
- Domain Controllers
- OUAdm
- OUAuth
- Resources
- UserComputers
- Group Policy Objects
- WMI Filters
- Starter GPOs

Sites

- Site-US-Dallas

Group Policy Modeling

Group Policy Results

Default Domain Policy

Data collected on: 26/08/2012 19:46:19

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	5 passwords remembered
Maximum password age	0 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Account Policies/Kerberos Policy

Local Policies/Security Options

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

show all hide

hide

hide

hide

hide

hide

hide

show

show

show

show

show

show

show

f23-09-9780123943972

Cisco ASDM 6.3 for ASA - 10.10.10.1

File View Tools Wizards Window Help

Look For: Go

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

- + Add - Delete Connect
- 10.10.10.1

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Configuration > Firewall > Access Rules

#	Source	Destination	Service	Action	Hits	Logging	Enabled
1	inside (1 incoming rule)						
2	inside IPv6 (1 implicit incoming rule)						
3	outside (0 implicit incoming rules)						
4	outside IPv6 (0 implicit incoming rules)						
5	Global (11 rules)						
1	any	webservers	tcp http tcp https	Permit	0		
2	Remote-2-internal	any	tcp http	Permit	0		
3	Corporate-internal-net	Corporate-finance-net Corporate-hr-net Corporate-rnd-net	ip	Permit	0		
4	Tech-Support	Remote-1-web-server	tcp http	Permit	0	Alerts	
5	Corporate-internal-terminal-server	any	ip	Permit	0		
6	any	Corporate-dns-ext	domain	Permit	0	disabled	
7	any	Corporate-proxy-server	tcp http	Permit	0		
8	any	Corporate-dmz-net	tcp http tcp https tcp smtp	Permit	0		
9	Corporate-mail-server	Internal-net-group	tcp smtp	Permit	0		
10	Internal-net-group	any	ip	Permit	0		
11	any	any	ip	Deny	0		
12	Global IPv6 (1 implicit rule)						

Access Rule Type: IPv4 and IPv6 IPv4 Only IPv6 Only

210.155.35.2 ————— [] ————— 192.168.2.2
 http ————— [] ————— Permit

Apply Reset Advanced...

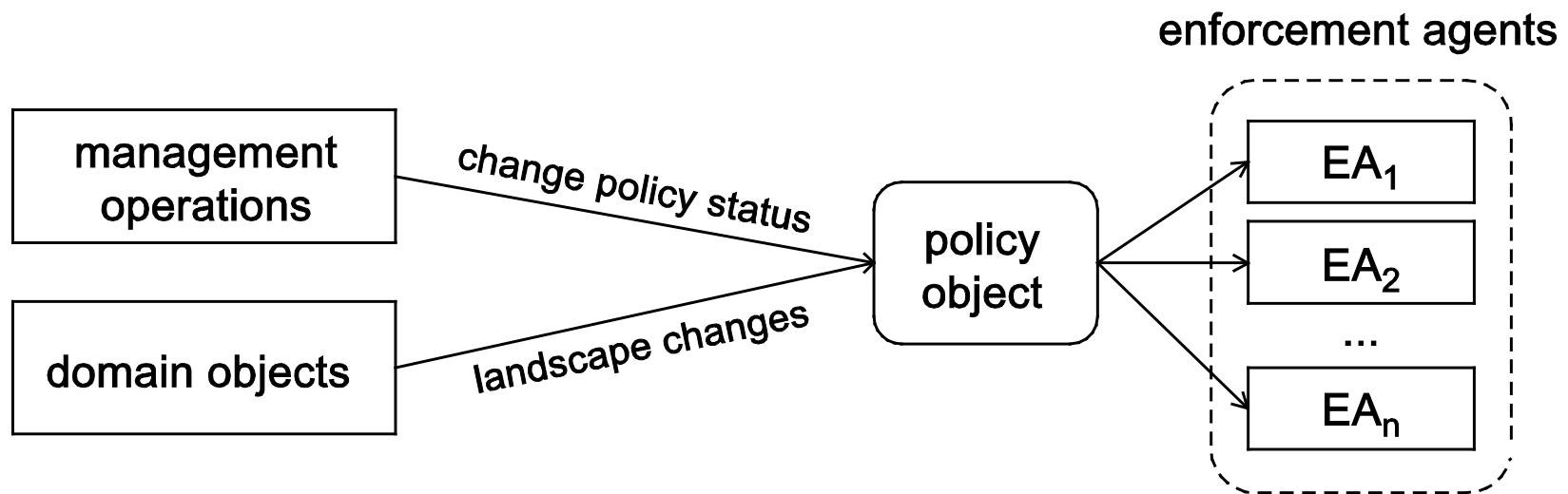
Running configuration successfully saved to flash memory.

<admin> | 15 | 3/4/10 6:55:12 PM UTC

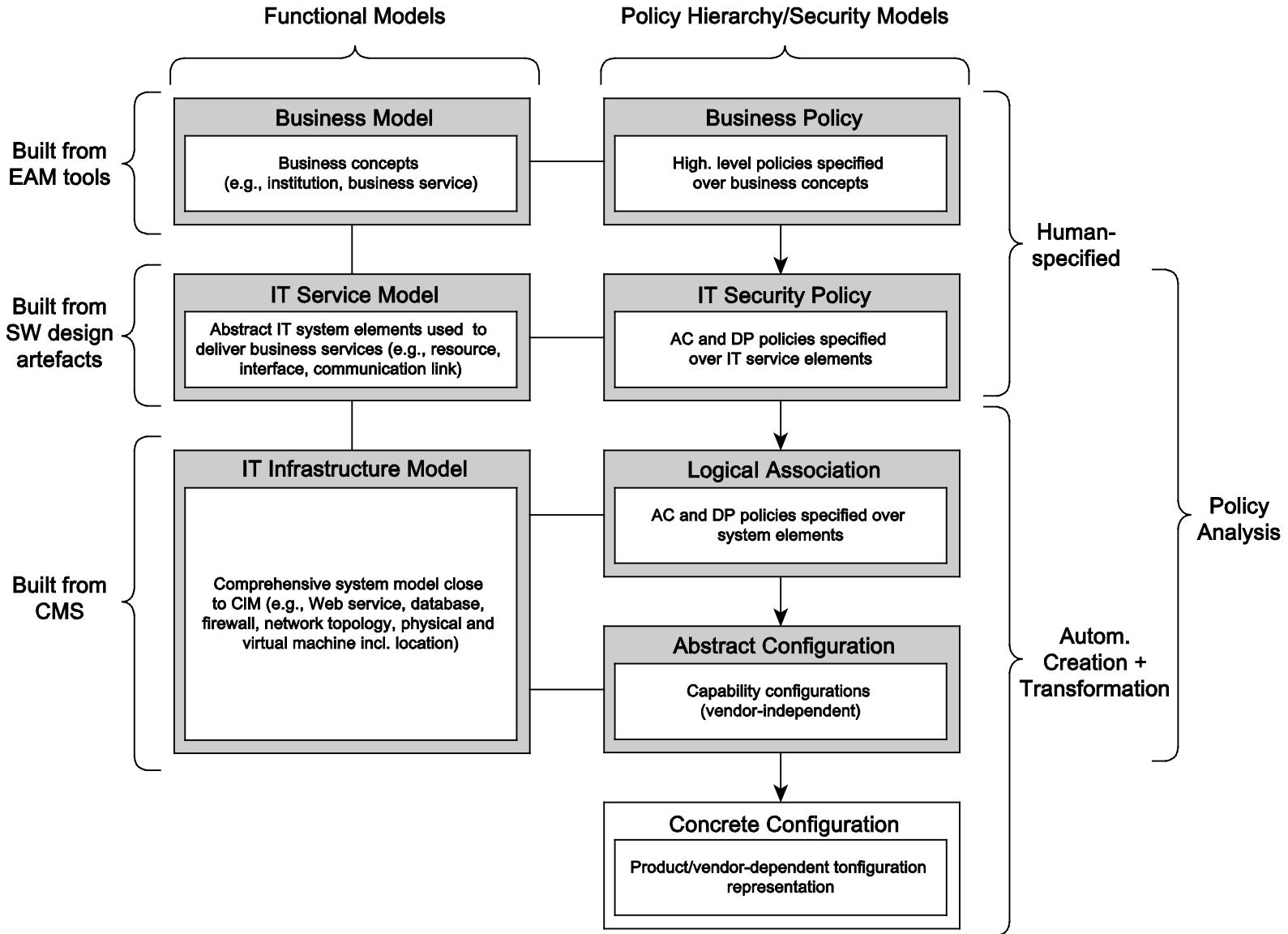
Addresses

- + Add - Edit Delete Where Used
- Filter: Filter Clear
- Name
- IP4 Network Objects
- Corporate-dmz-net
Corporate-dns-ext
Corporate-finance-net
Corporate-hr-net
Corporate-internal-net
Corporate-internal-terminal-server
Corporate-mail-server
Corporate-proxy-server
Corporate-rnd-net
Corporate-dns-ext
Public-IP-Remote-1
Public-IP-Remote-2
Public-IP-Remote-3
Public-IP-Remote-4
Public-IP-Remote-5
Public_IP_ISP1
Remote-1-internal
Remote-1-web-server
Remote-2-internal
Remote-3-internal
Remote-4-internal
Remote-5-internal
Tech-Support
- www_server1
www_server2
www_server3

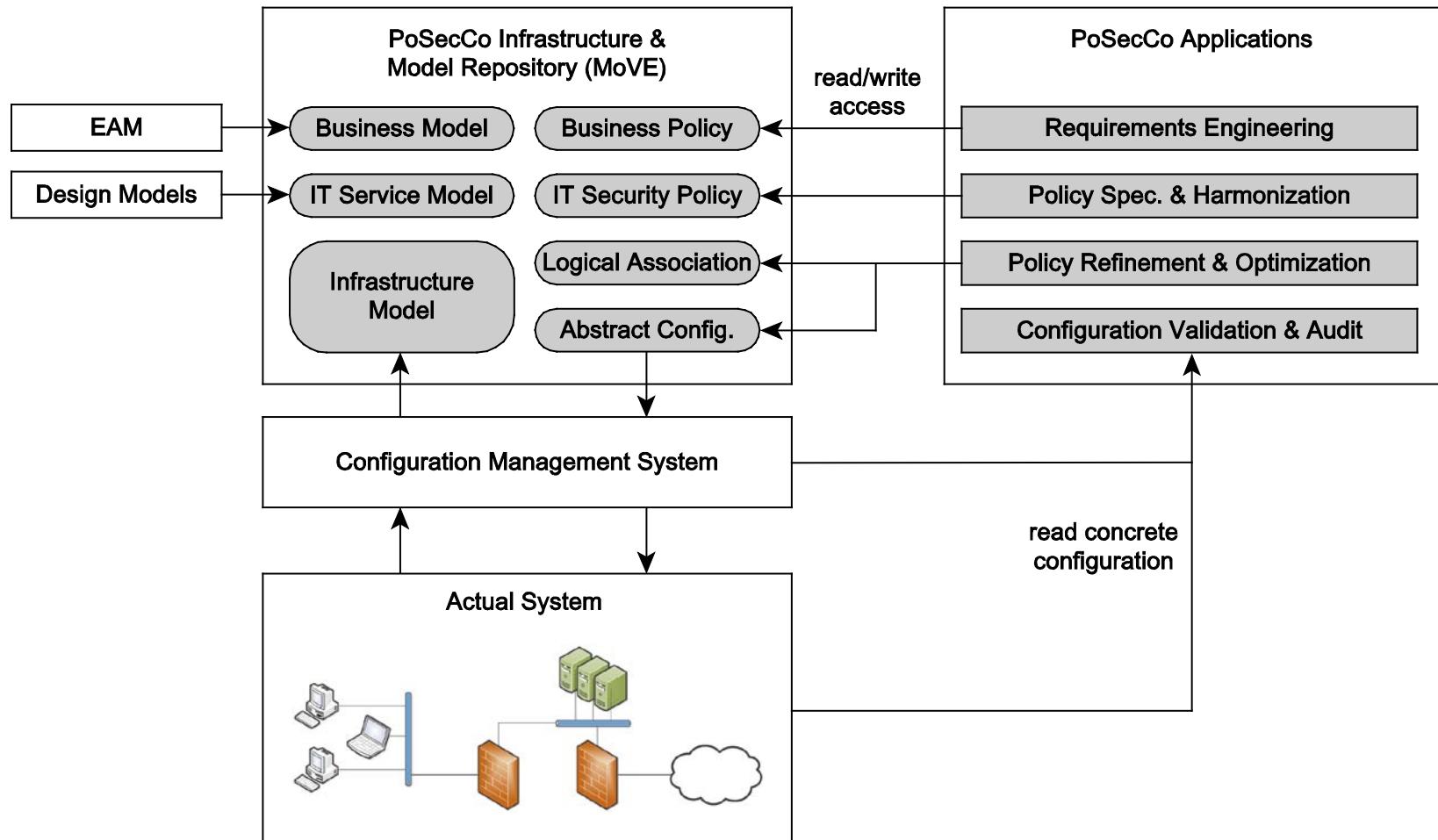
f23-10-9780123943972



f23-11-9780123943972



f23-12-9780123943972



f23-13-9780123943972