

ICAT 2002 4 16

MPSEC

,

{jhyang,heejo}@ahnlab.com

MPSEC

*

1)

- / , Server,

PC

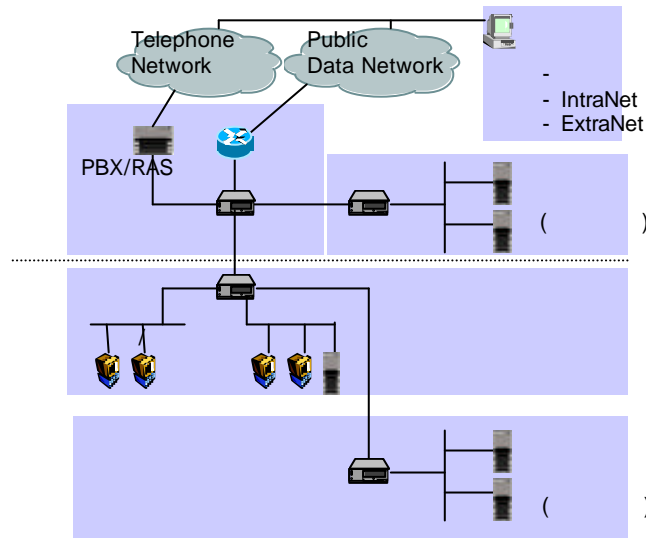
가 Vulnerability

(Distributed Environment)

2)

- ,
- ,
-

(Multi-Vendor, Multi-Platform)



O(100~1000) PC
O(10~100)
O(10~30)



1)

(Manageability)

(Gateway, PC, Server)

-
-

,

,

,

2)

(Automation)

-
-

가

가

가

3)

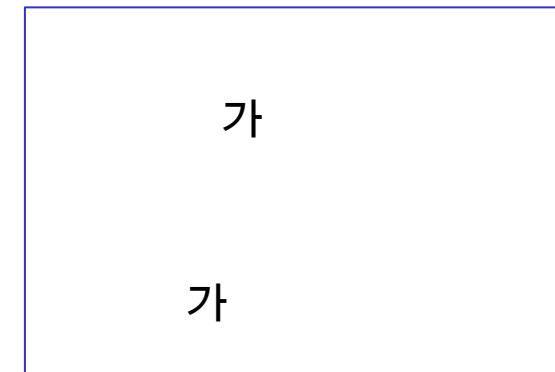
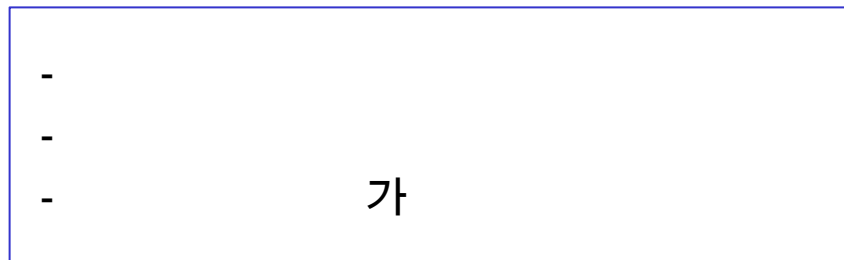
(Controllability)

-

가

가

,





가

ESM

ESM : Enterprise Security Management,

ESM

: , , , ...
: AV, VPN, Firewall, IDS, PKI, ...
: , / , , ...

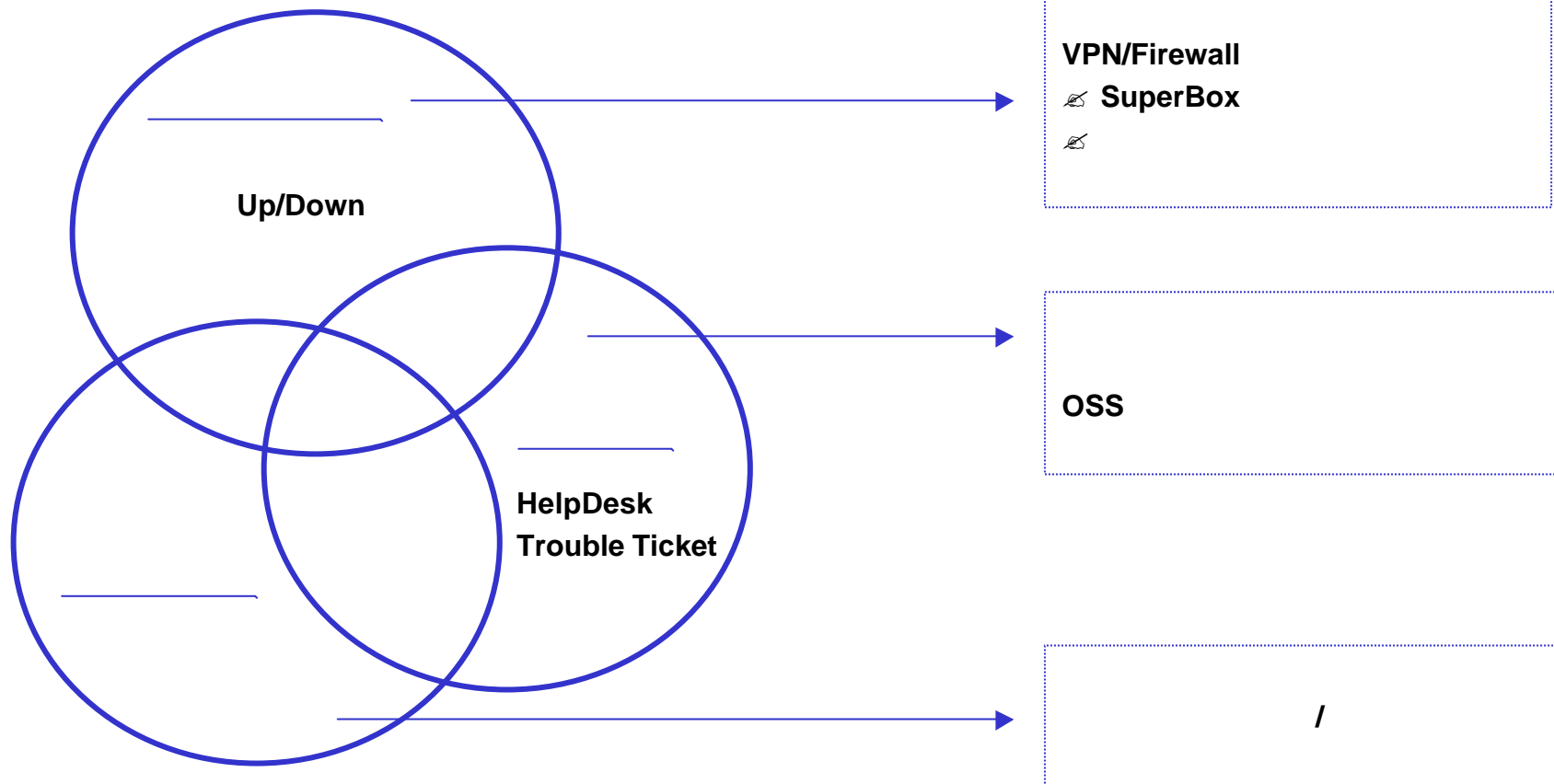
가

NMS	(SNMP agent)
SMS	(SMS agent)

Tivoli Secureway
OPSEC , SDK, ...

IETF, DMTF, ...

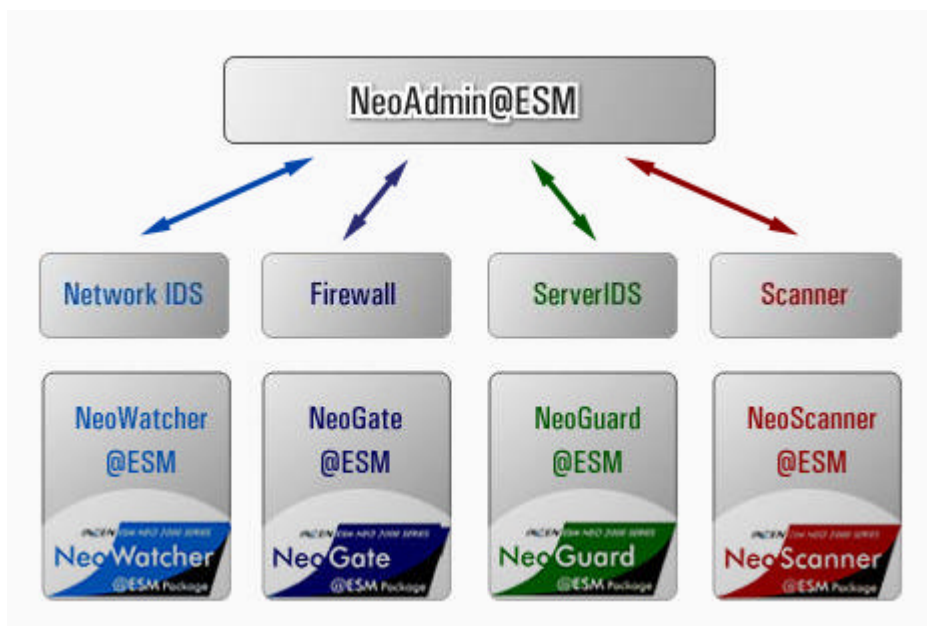
	SMS	.	Tivoli Secureway, DMS,
	NMS	.	..
	OSS	.	..
		.	Insen ESM
		One-Stop .	SPiDER1, secuiesm
		Extranet .	..
	OPSEC		OPSEC Alliance
	IETF	, IPSec	IP Security Working Group
		Network QoS, IPSec	IPSP



-
-

가

() ESM



: [NeoAdmin@ESM](http://www.inzen.com/kor/products/esm/family.asp) <http://www.inzen.com/kor/products/esm/family.asp>

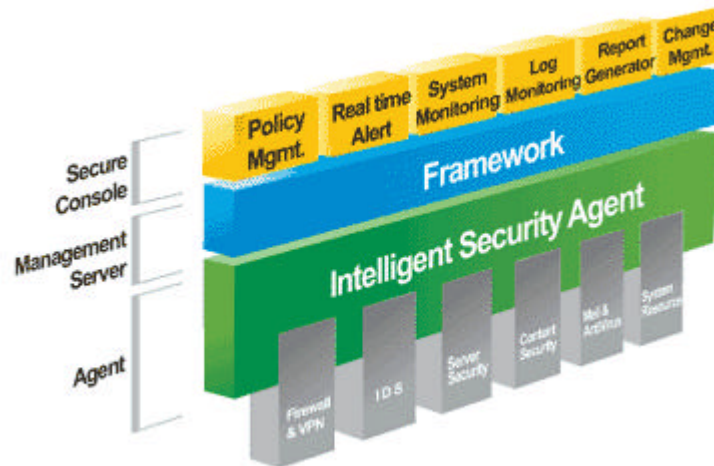
•

, ,

()

SPiDER-1

Secui secuiESM ()
Tivoli RiskManager



: SPiDER-1 <http://www.igloosec.co.kr>

Tivoli Secureway

-
-
-

Tivoli

Adaptor



: Tivoli Secureway http://korea.tivoli.com/product/security/s_1121.html

Open Platform for SECurity

OPSEC은 ,
/VPN Inspection Module Policy
Management
가 .
, 300 가 .

OPSEC SDK

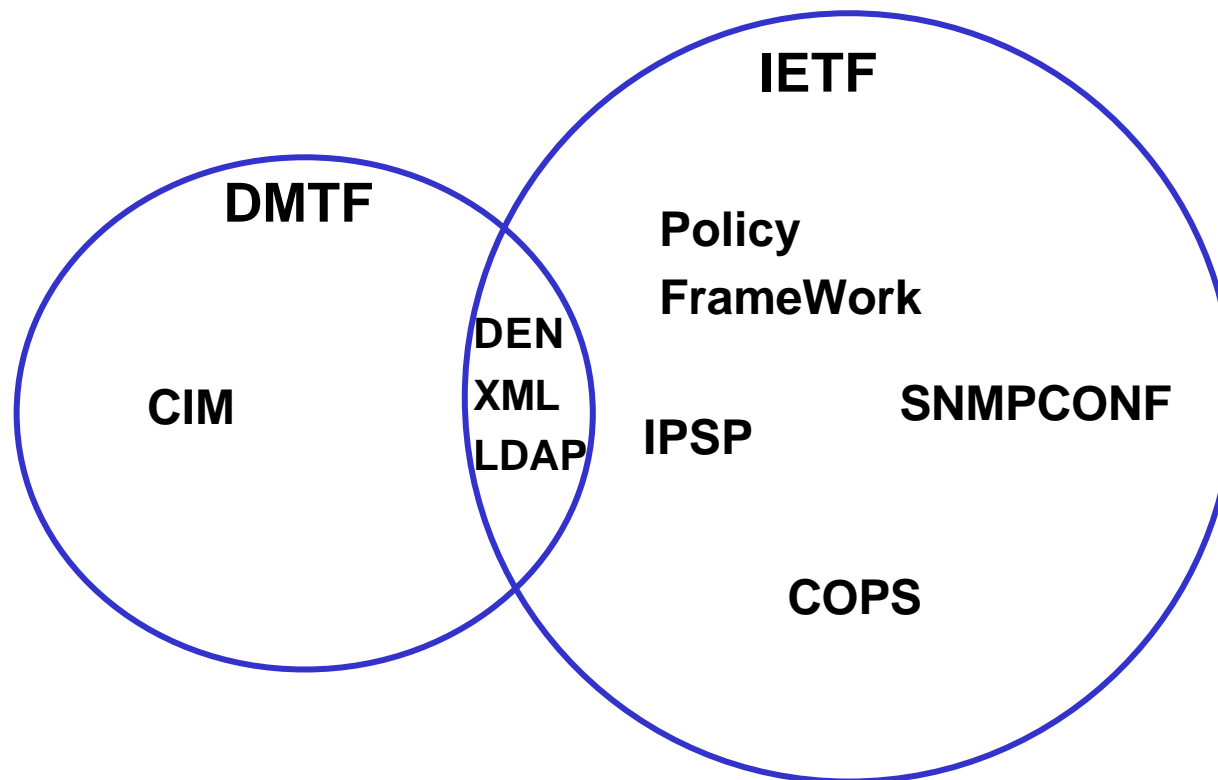
- CVP (Content Vectoring Protocol)
- UFP (URL Filtering Protocol)
- SAM (Suspicious Activity Monitoring)
- LEA (Log Export API) / ELA (Event Logging API)
- AMON (Application Monitoring API)
- OMI (Object Management Interface)
- CPMI (CheckPoint Management Interface)

IETF Activities

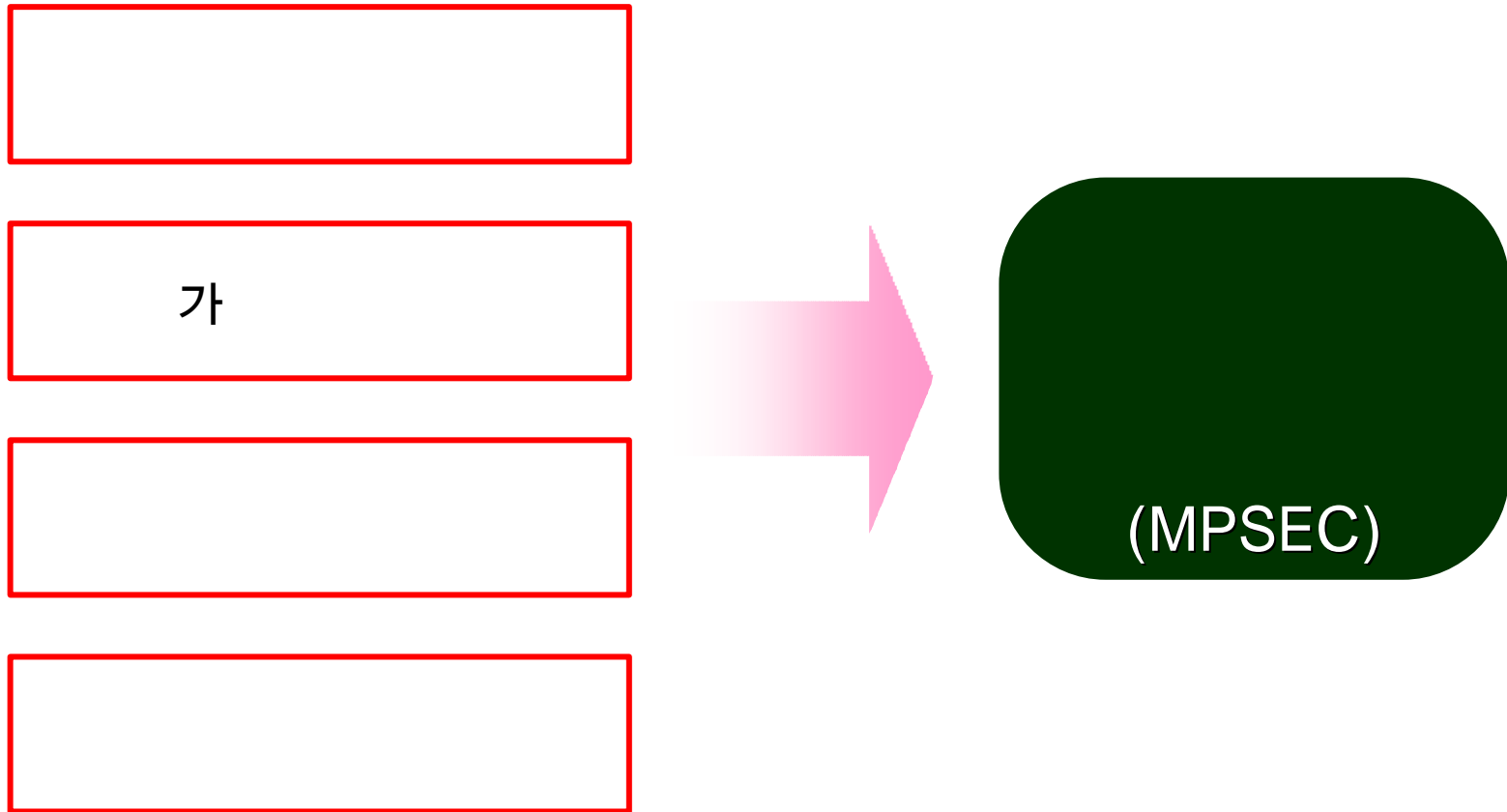
, IPSec

IPSec

(IPSP – IP Security Policy WorkingGroup)



- MPSEC



:



1) Security Device/Application

Directory Server

2) , Security

:



- 1) , . Agent가
- 2) , .

:

Data Oriented (Not Task Oriented)

1) Task , 가 Task

.

2) Policy Task가 Directory (LDAP, DB) ,
Task .

MPSEC

- MPSEC

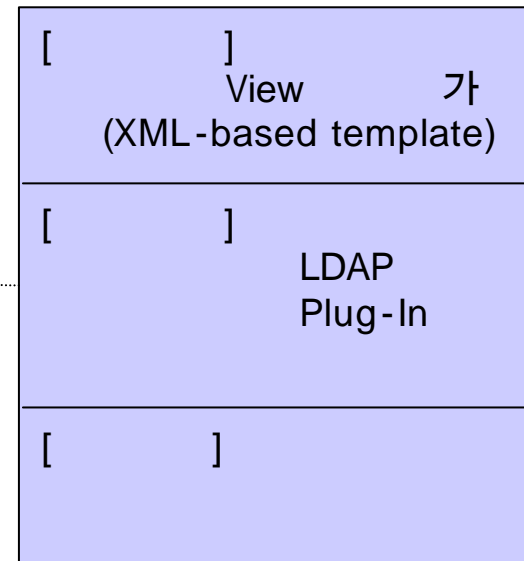
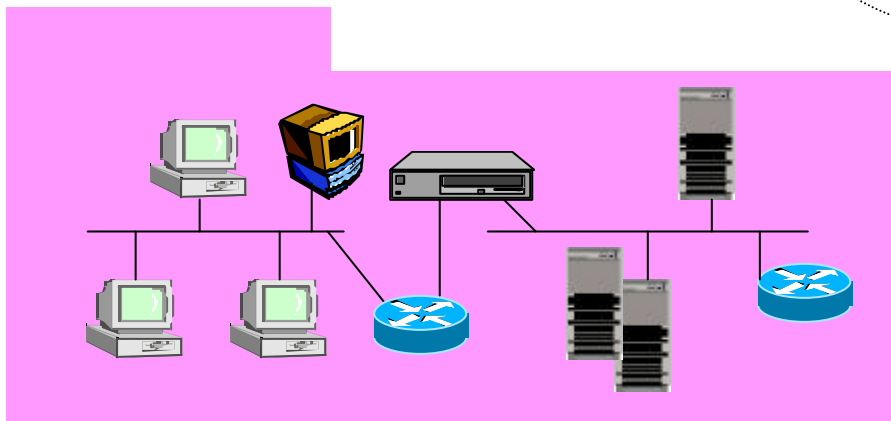
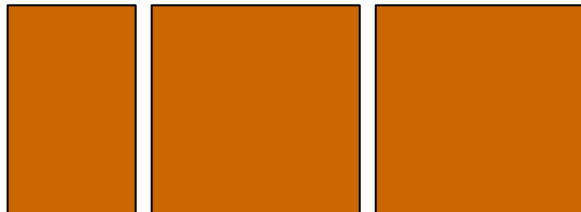
- MPSEC plug-in
- /view

가
가

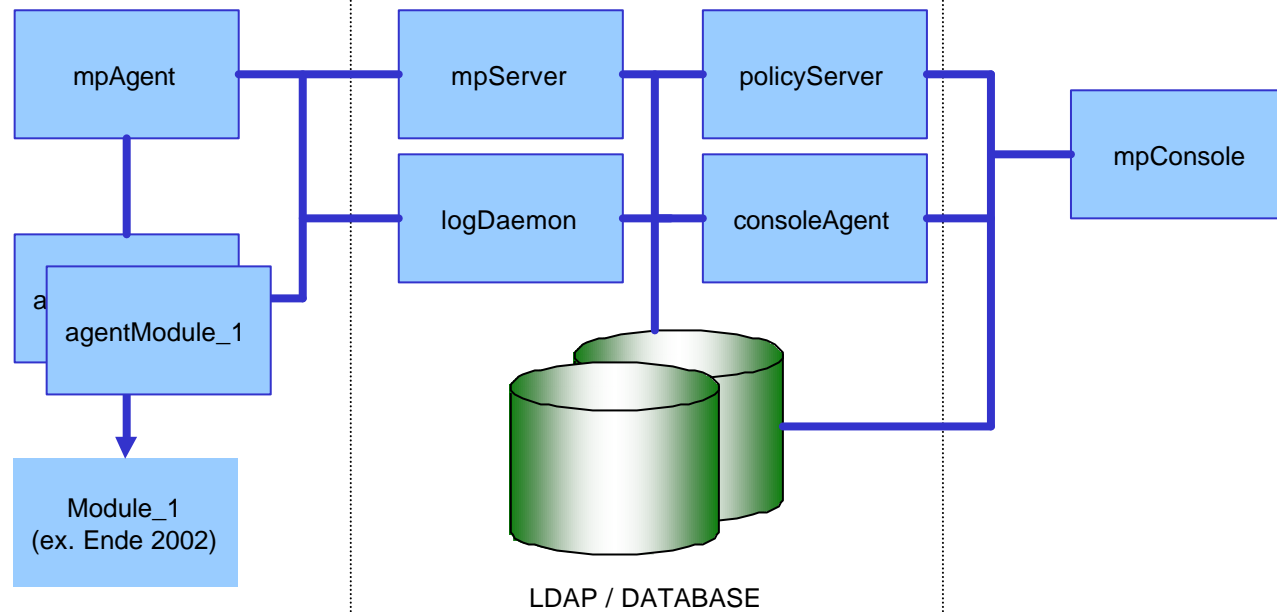
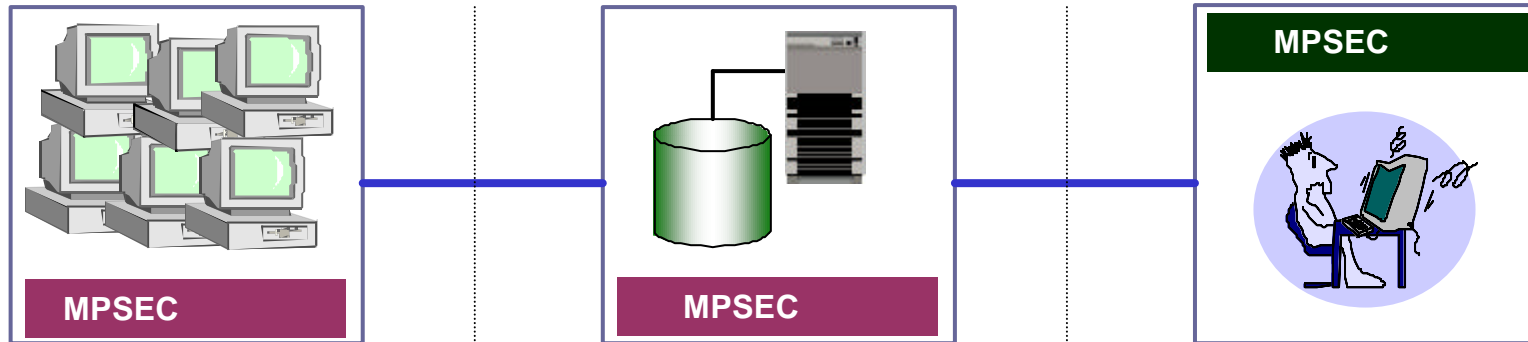
MPSEC

/ , () , ,
/ / , ,

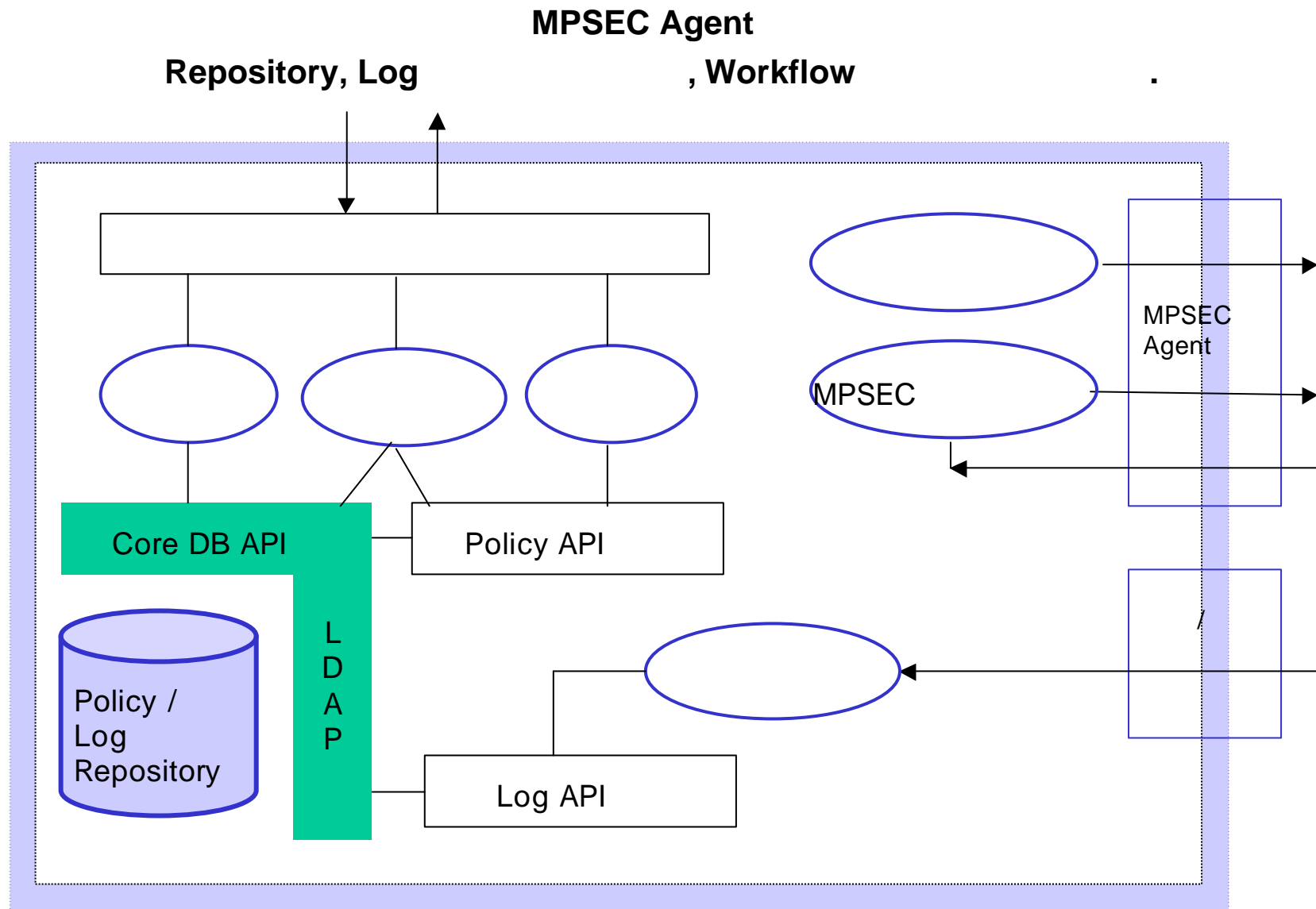
가



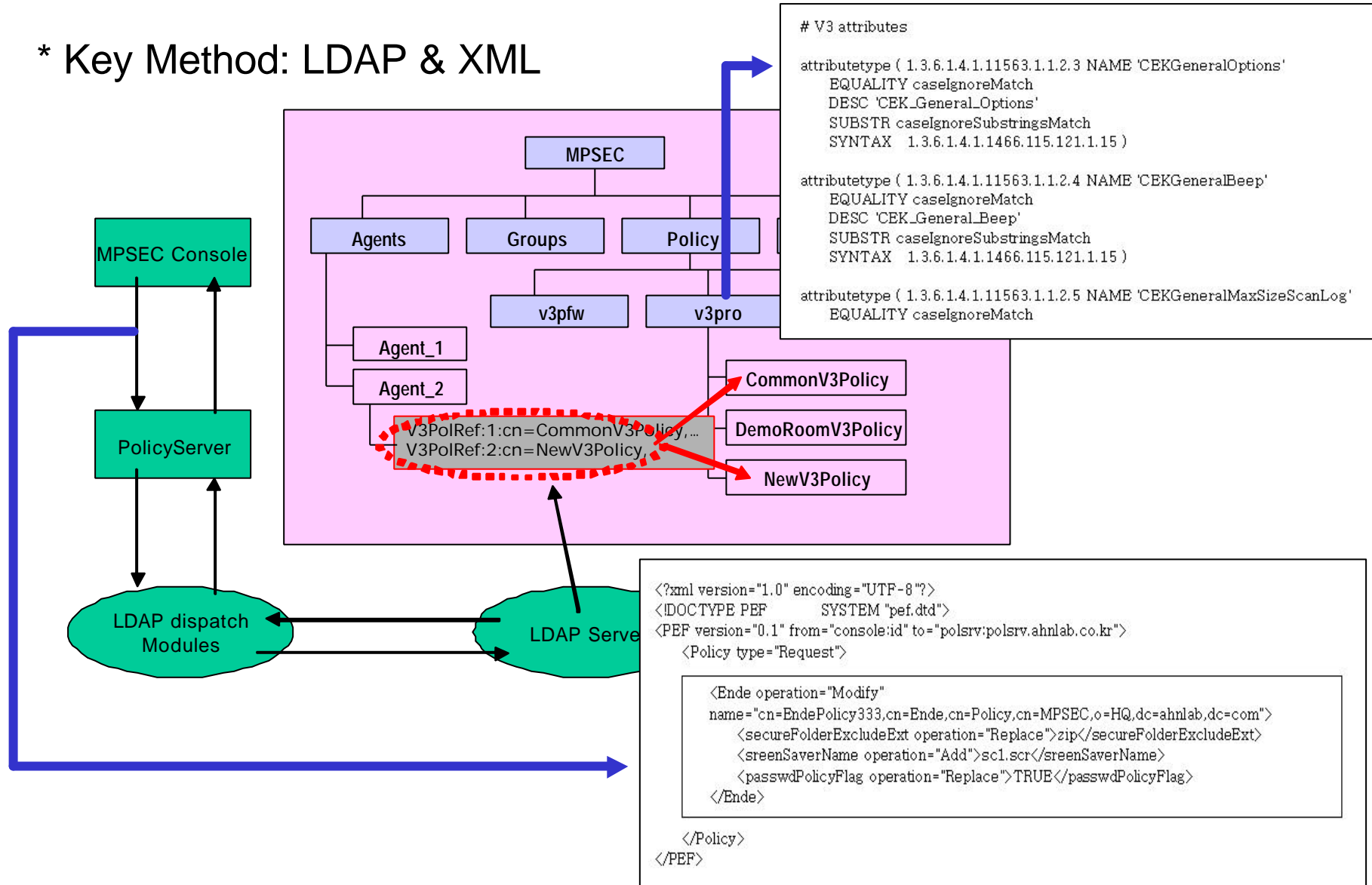
MPSEC



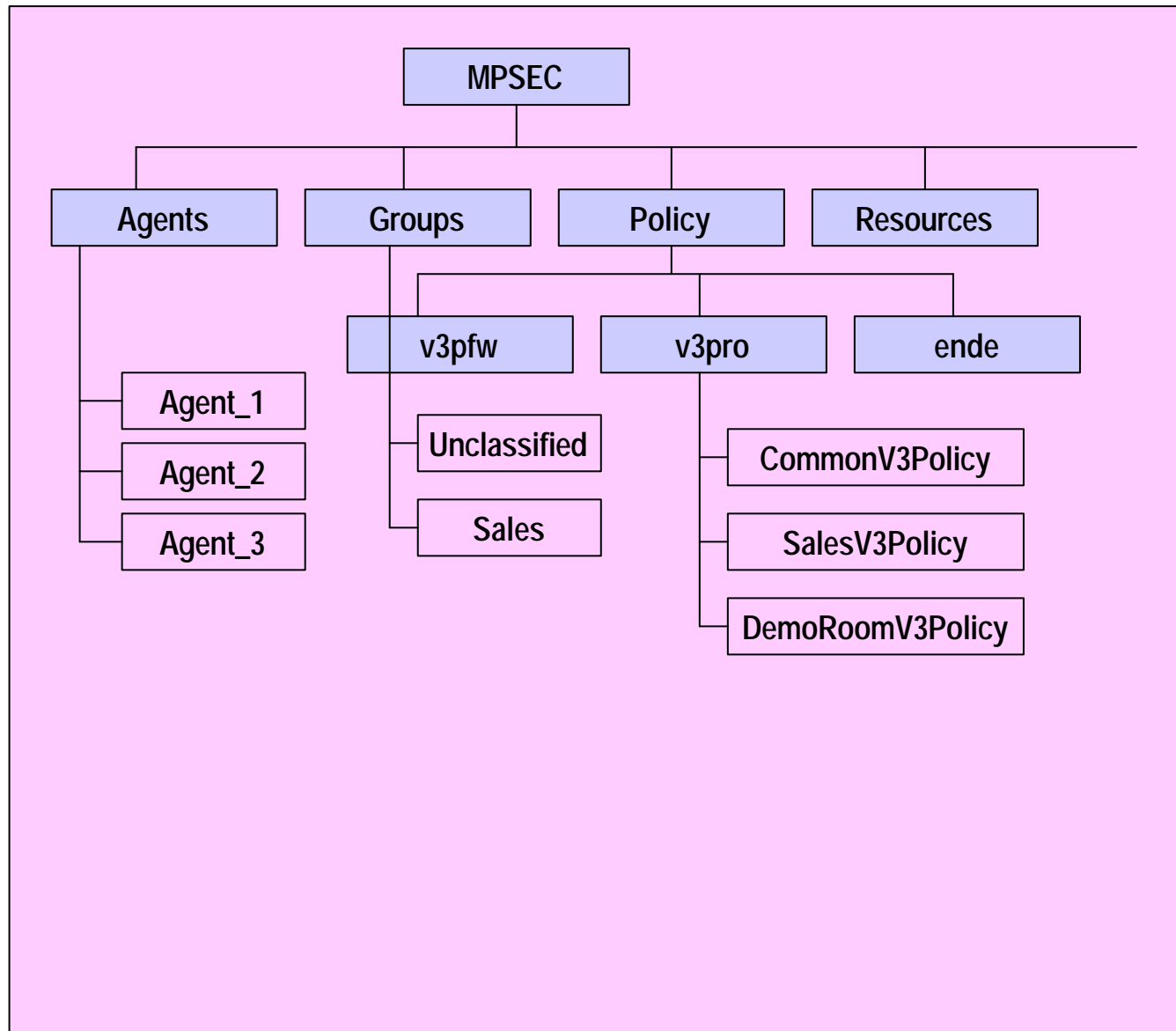
MPSEC



* Key Method: LDAP & XML



: LDAP – Policy Repository



LDAP

Agents

Groups

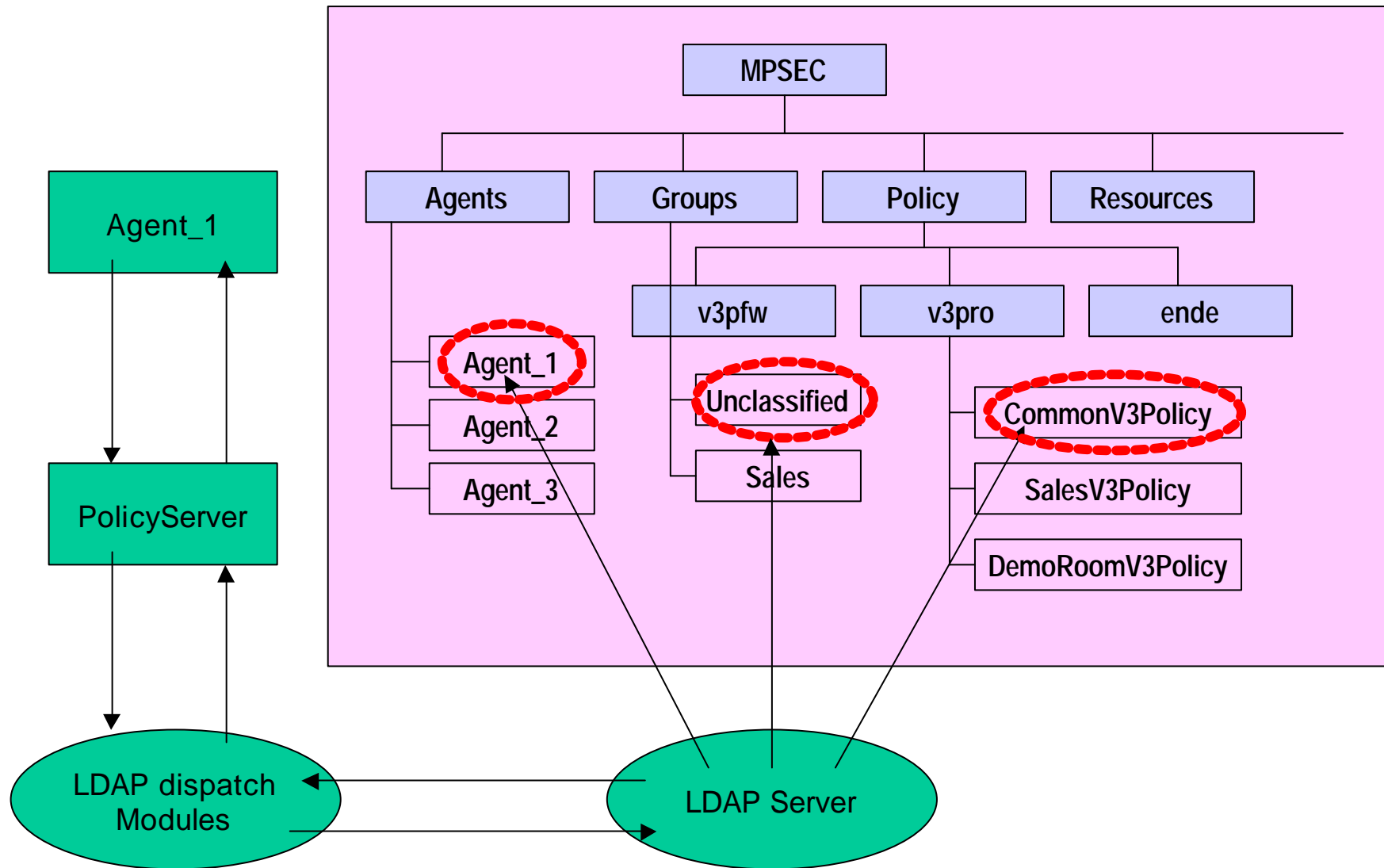
Policies

Resources

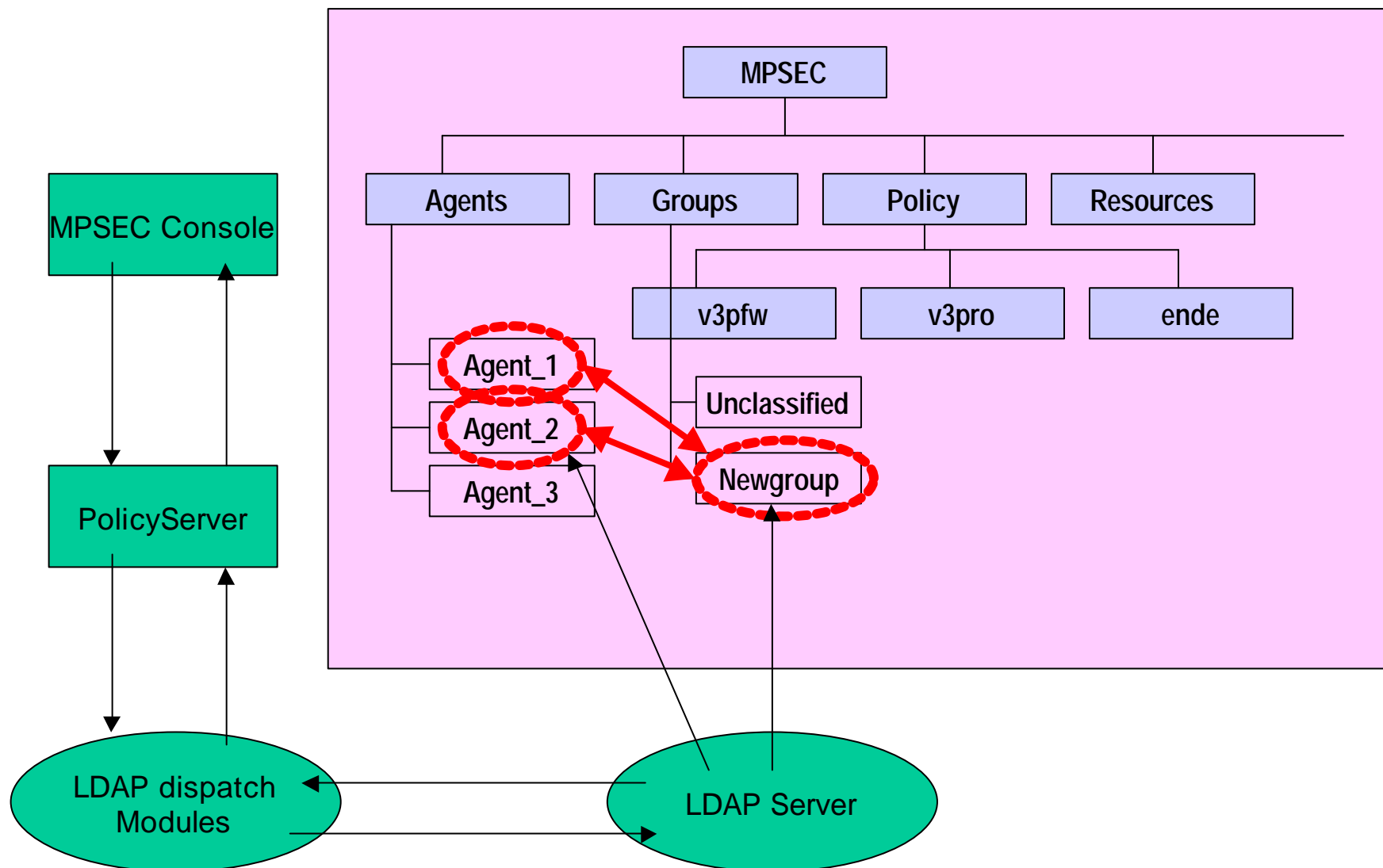
Entities

.

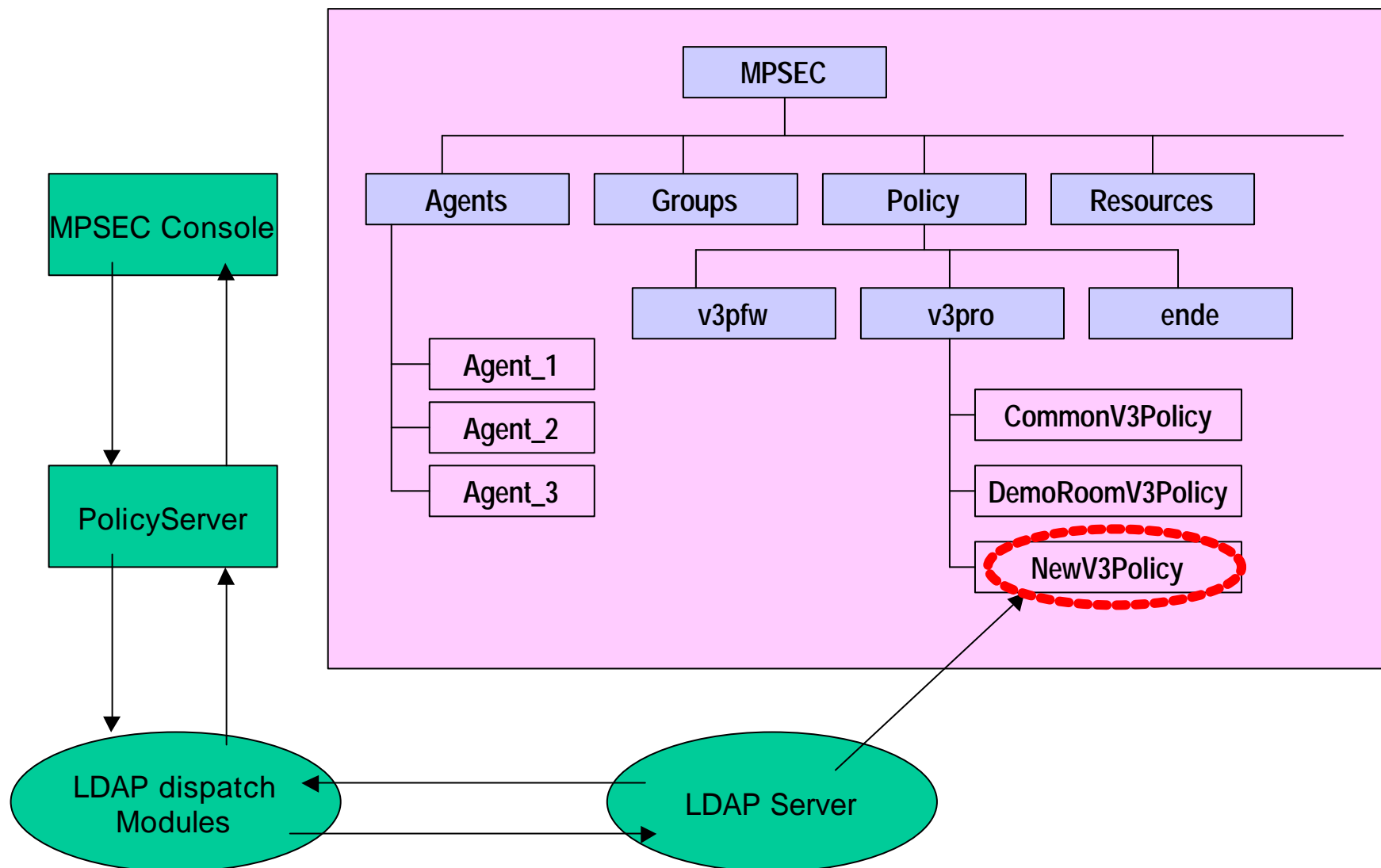
: Agent



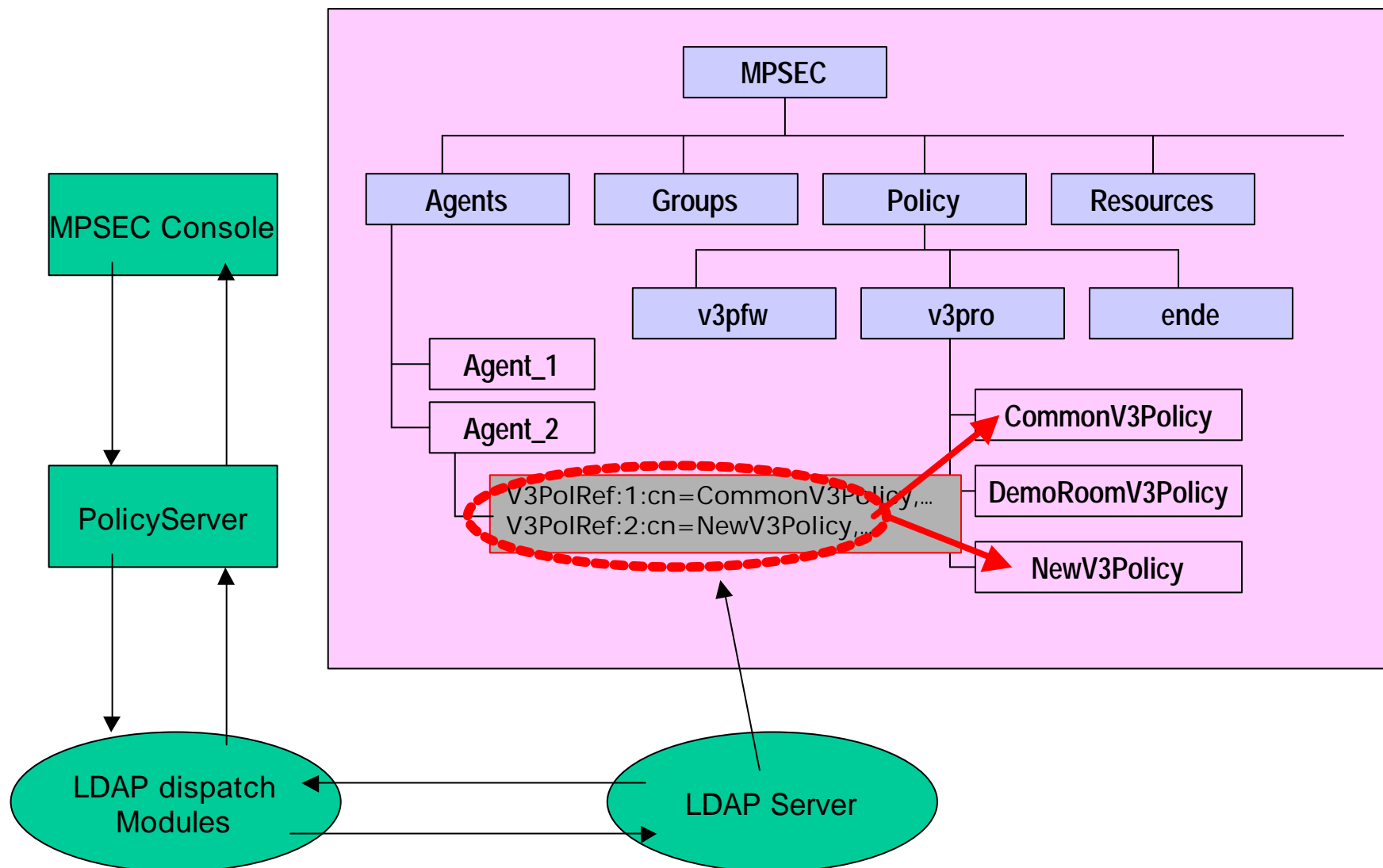
:



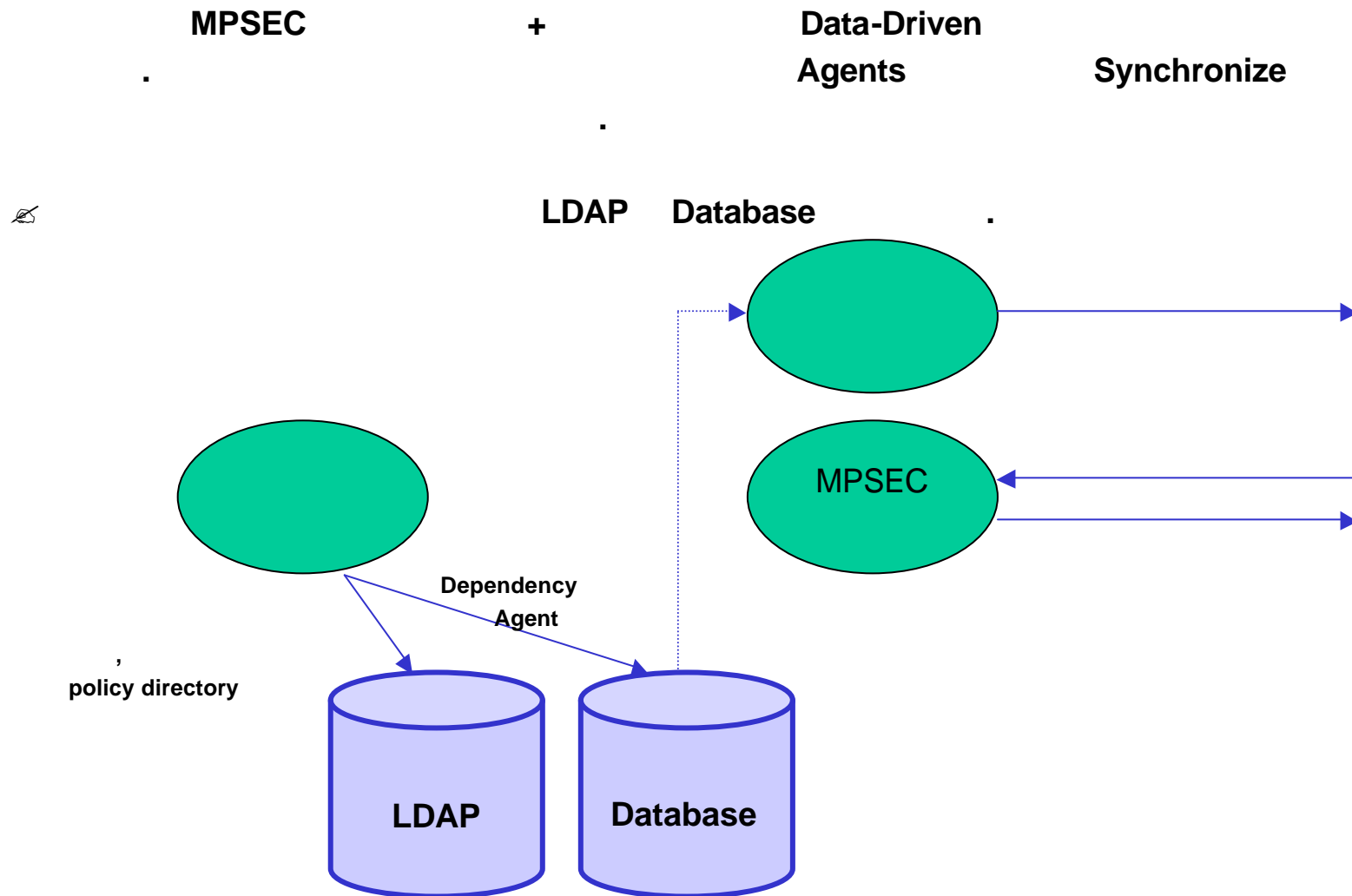
:



:



- MPSEC

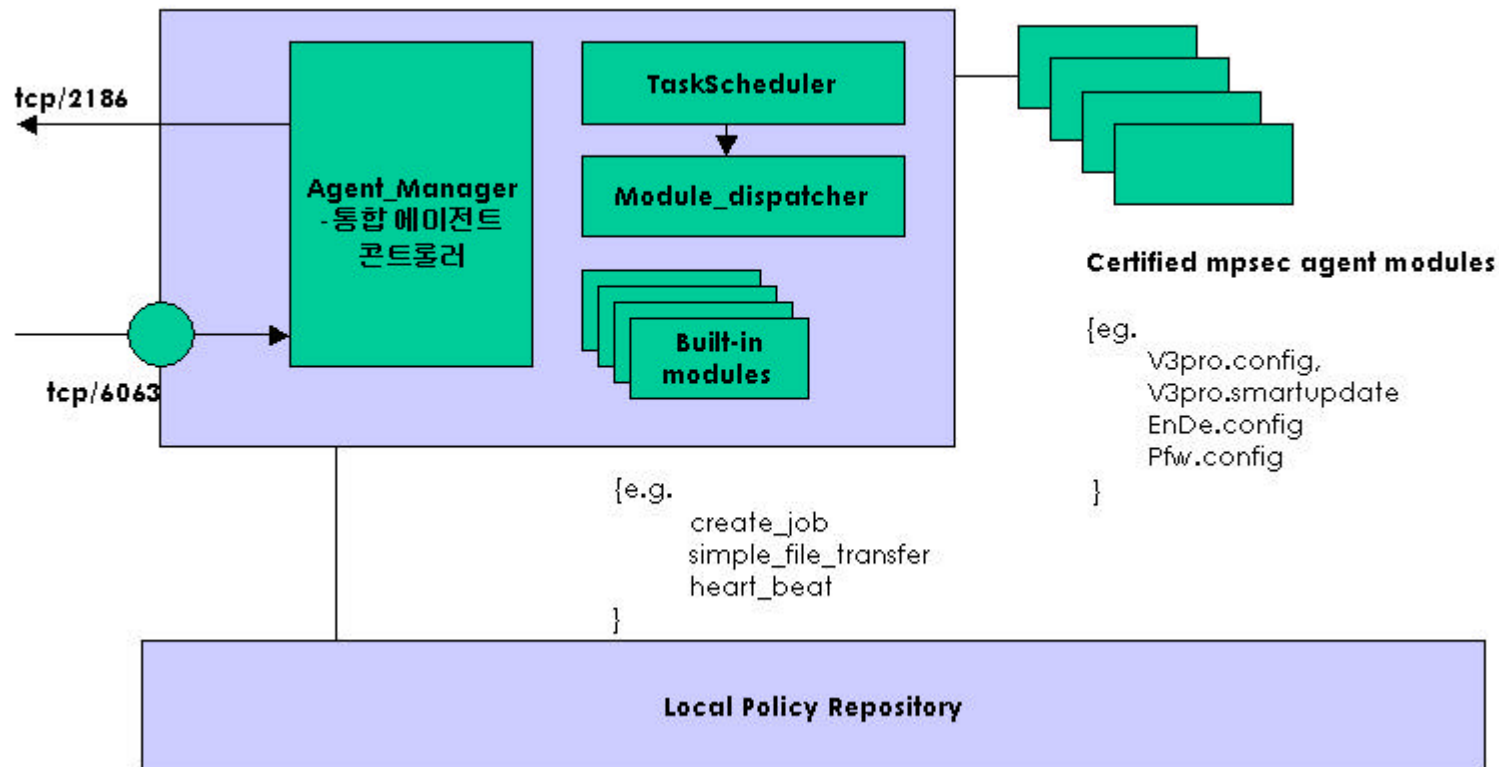


MPSEC

- MPSEC Agent
MPSEC agent module

Application/

가
가



MPSEC

MPSEC

MPSEC

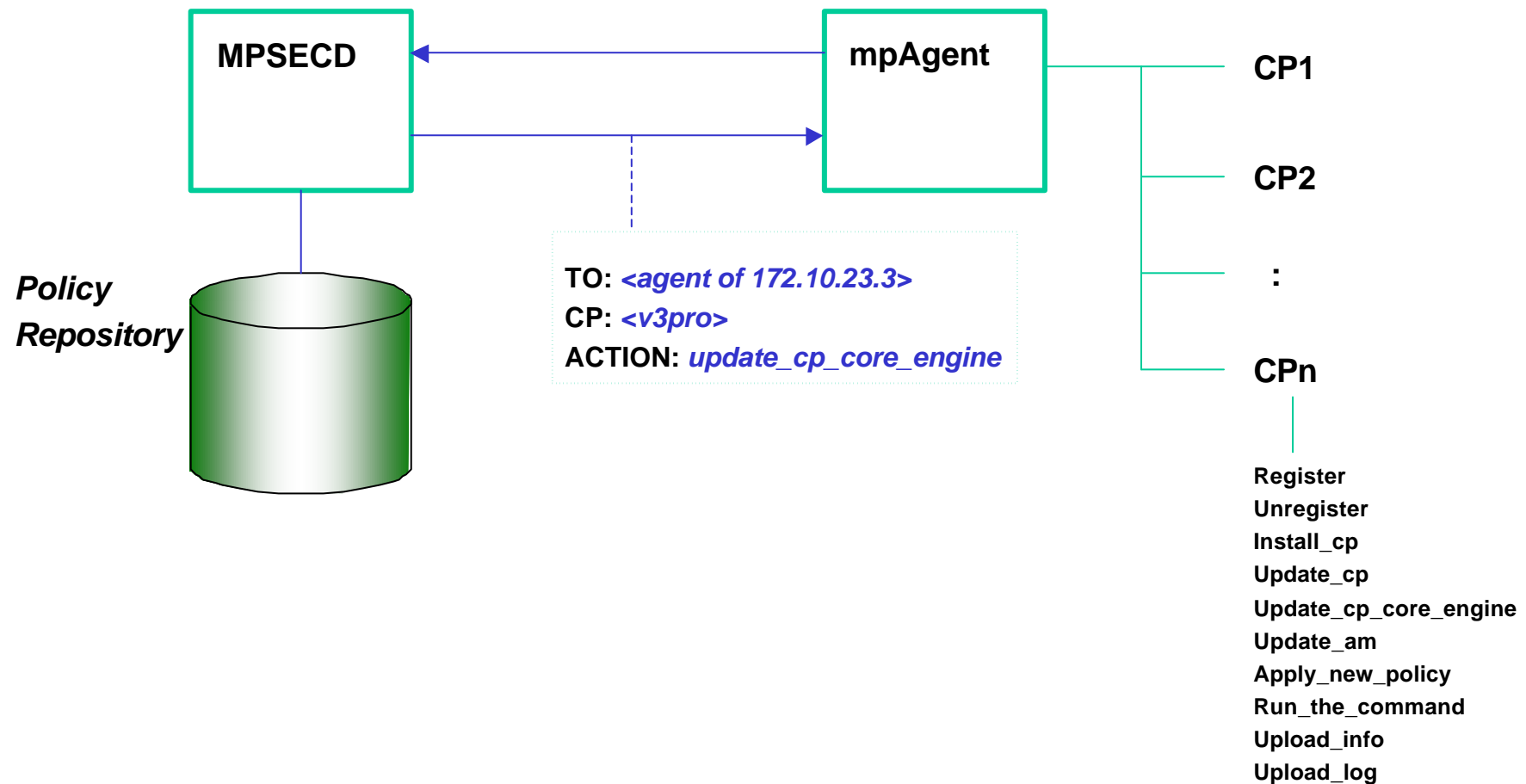
Agent

logical operation

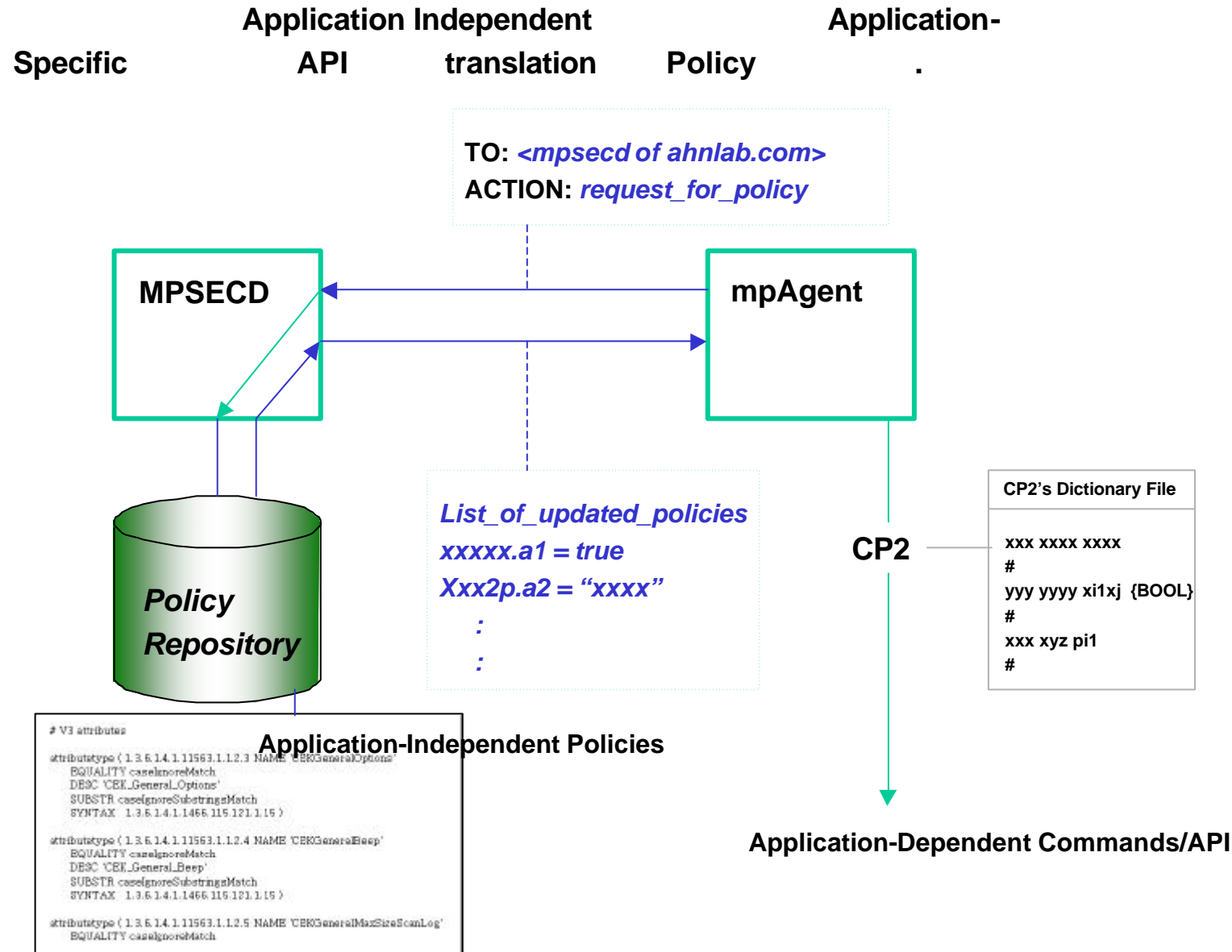
CP(Client Product)

Method

Call



: Client-Side Action

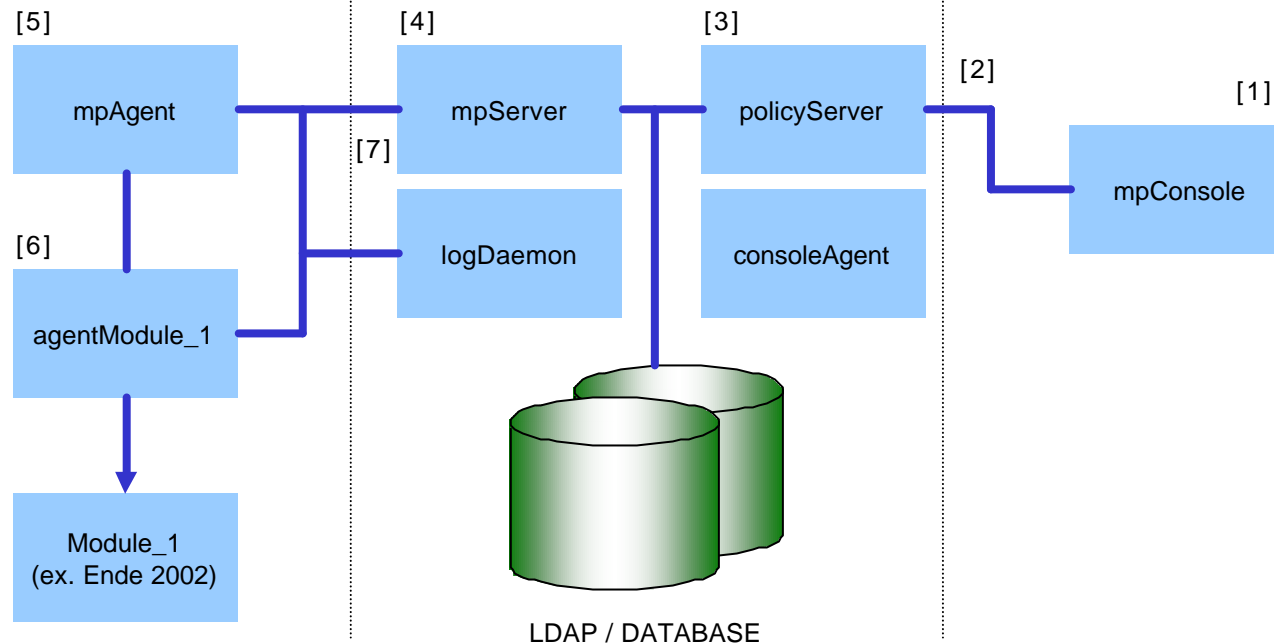


[5] mpAgent mpServer
taskScheduler
invoke .
[6] invoke (ende2002.enforce)
MPSEC API mpServer
updatePolicy .
- client
mpServer logDaemon
[7] mpServer
Green

[3] policyServer XML
LDAP
Agent MPSEC Agent
Yellow
[4] mpServer Yellow
SYNC mpAgent
enforcement module
addTask now ende2002.enforcement

[1] MpConsole Group1
EnDe 2002
45 14
[2] mpConsole policyServer Group1
XML

```
<policyUpdateRequest>
  <application> ende2002 </>
  <passwordTTL> 14 days </>
</policyUpdateRequest>
```



Firewall, IDS

1) PC

2)

3)

1)

2)

1)

2)

가

