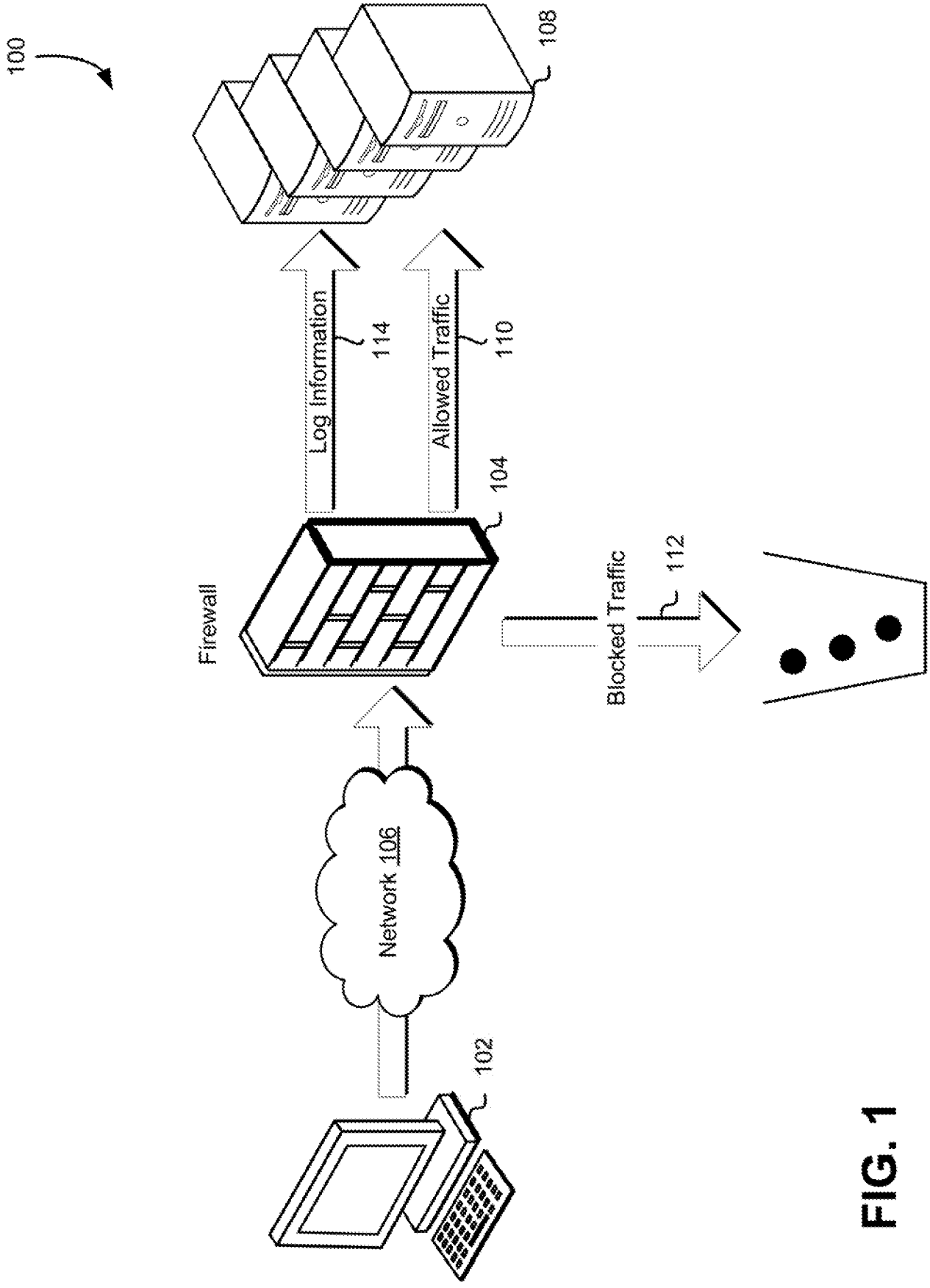
100
108
Log Information
114
Allowed Traffic
110
104
Firewall
Blocked Traffic
112
Network 106
102

FIG. 1

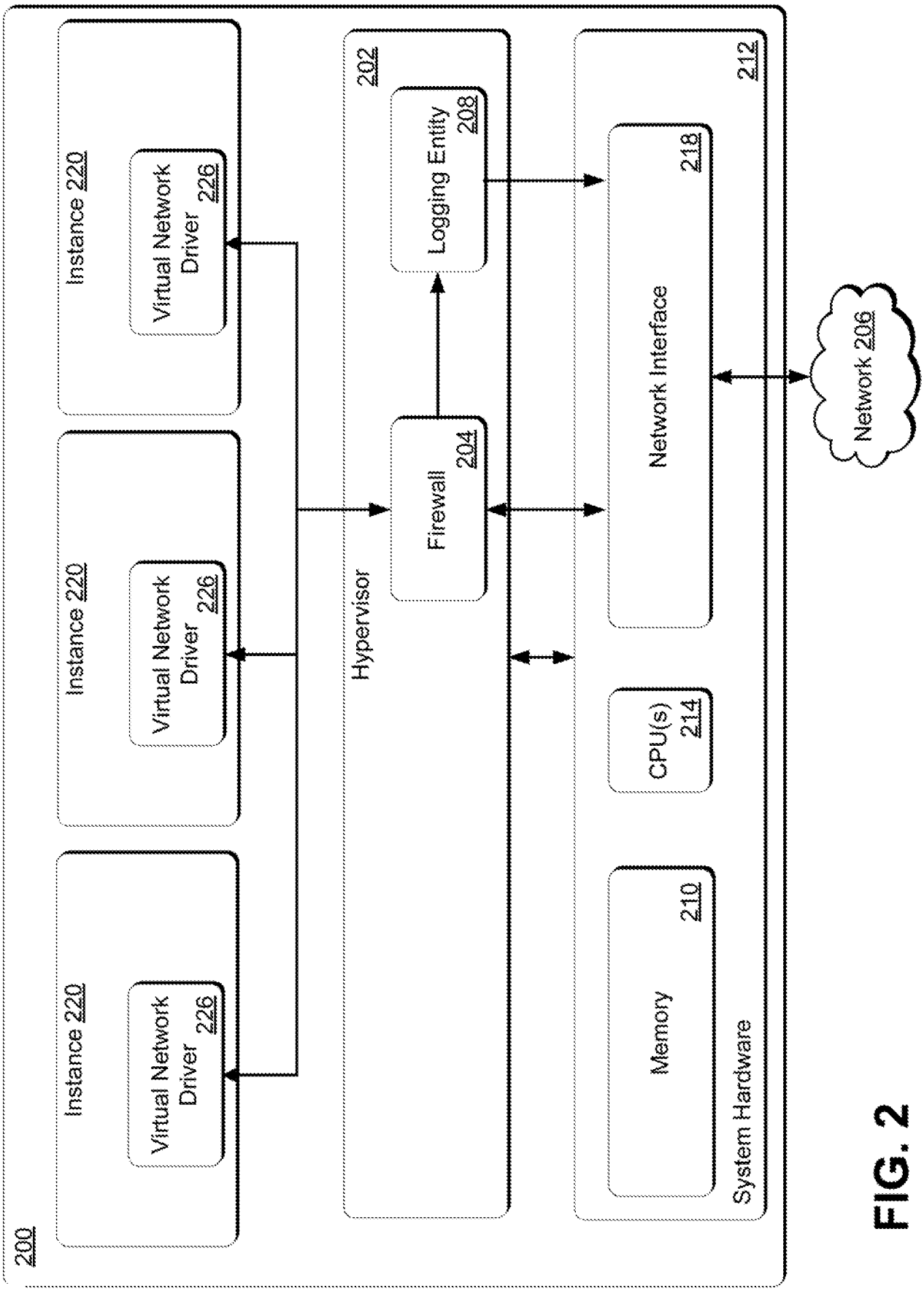
200
Instance 220
Virtual Network Driver 226
Instance 220
Virtual Network Driver 226
Instance 220
Virtual Network Driver 226
Hypervisor
202
Firewall 204
Logging Entity 208
System Hardware
212
Memory 210
CPU(s) 214
Network Interface 218
Network 206

FIG. 2

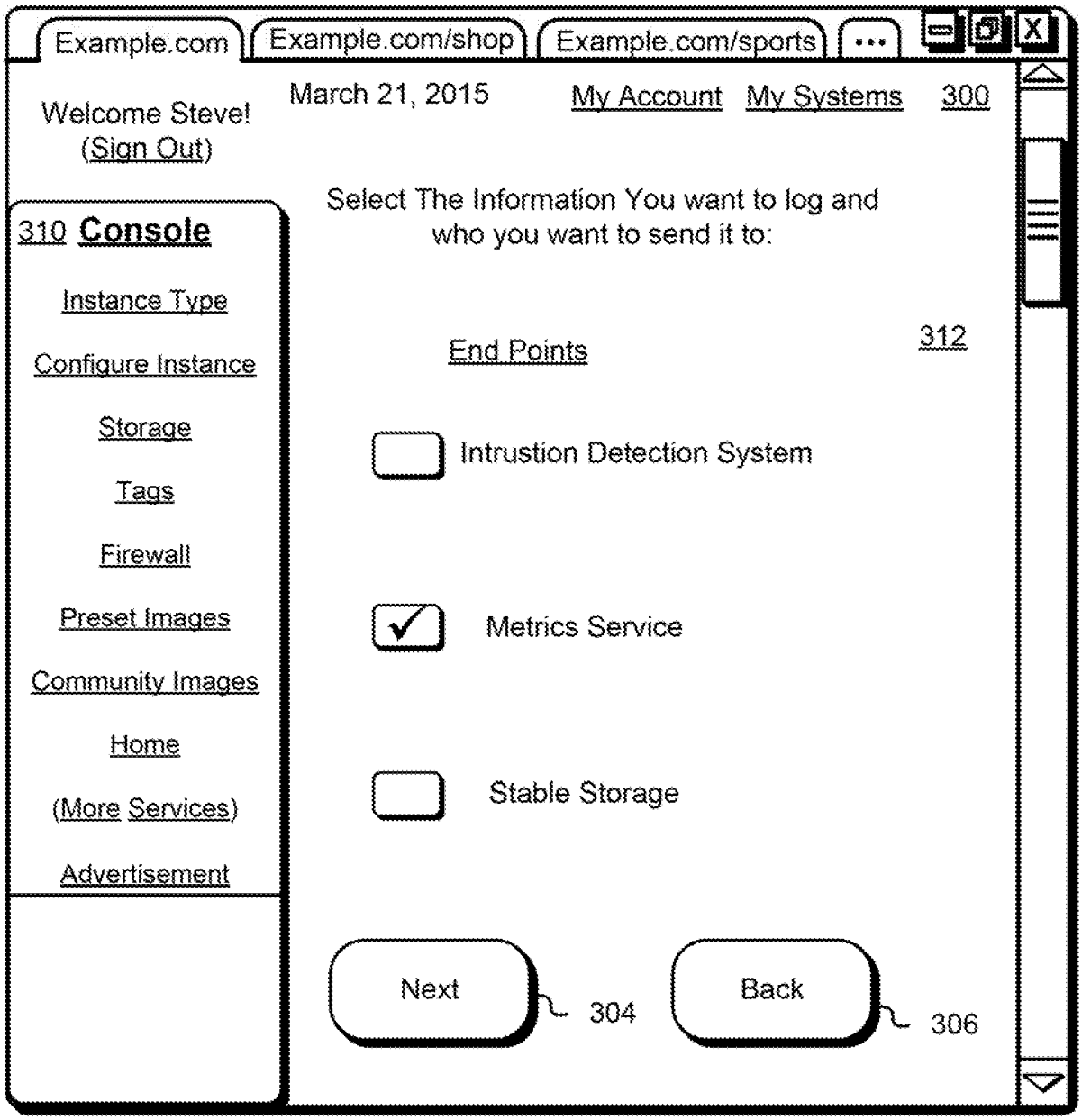
Example.com
Example.com/shop
Example.com/sports
Welcome Steve!
(Sign Out)
March 21, 2015
My Account
My Systems
300
310 Console
Instance Type
Configure Instance
Storage
Tags
Firewall
Preset Images
Community Images
Home
(More Services)
Advertisement
Select The Information You want to log and who you want to send it to:
End Points
312
Intrustion Detection System
Metrics Service
Stable Storage
Next
304
Back
306

FIG. 3

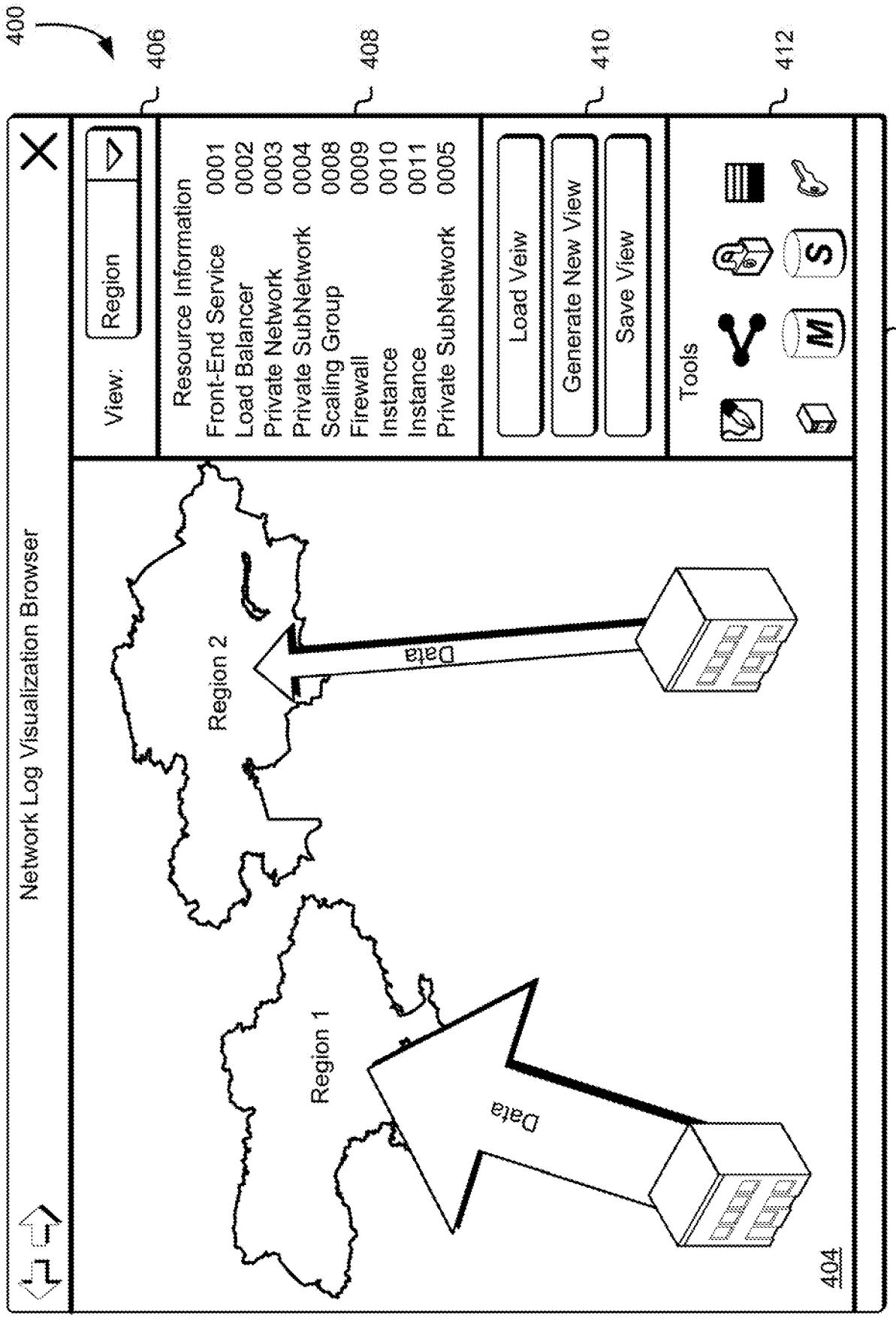
400
406
408
410
412
402
404
Network Log Visualization Browser
View:
Region
Resource Information
Front-End Service 0001
Load Balancer 0002
Private Network 0003
Private SubNetwork 0004
Scaling Group 0008
Firewall 0009
Instance 0010
Instance 0011
Private SubNetwork 0005
Load Veiw
Generate New View
Save View
Tools
Region 1
Region 2
Data
Data

FIG. 4

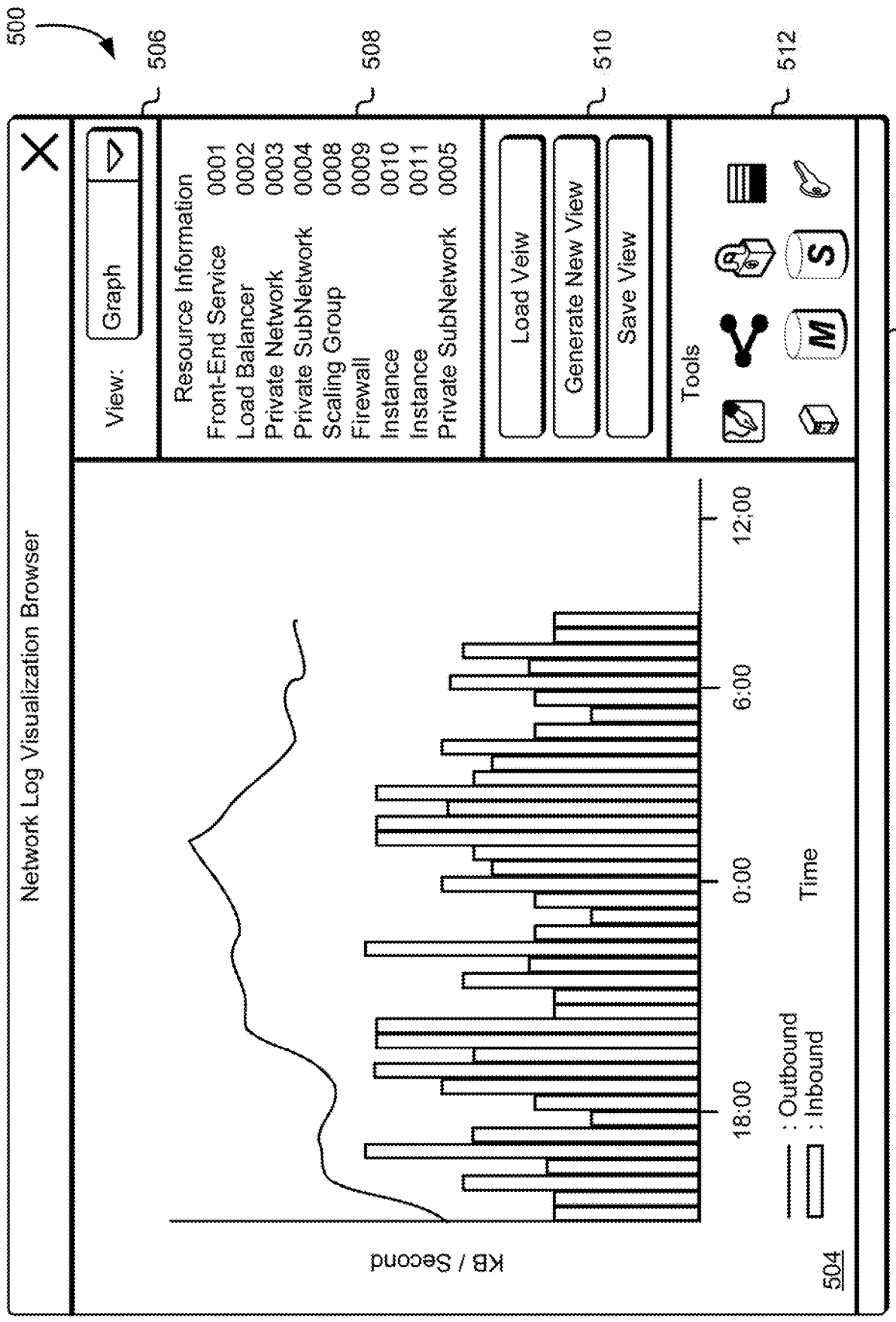
500
506
508
510
512
502
Network Log Visualization Browser
View:
Graph
Resource Information
Front-End Service 0001
Load Balancer 0002
Private Network 0003
Private SubNetwork 0004
Scaling Group 0008
Firewall 0009
Instance 0010
Instance 0011
Private SubNetwork 0005
Load Veiw
Generate New View
Save View
Tools
KB / Second
18:00
0:00
6:00
12:00
Time
: Outbound
: Inbound
504

FIG. 5

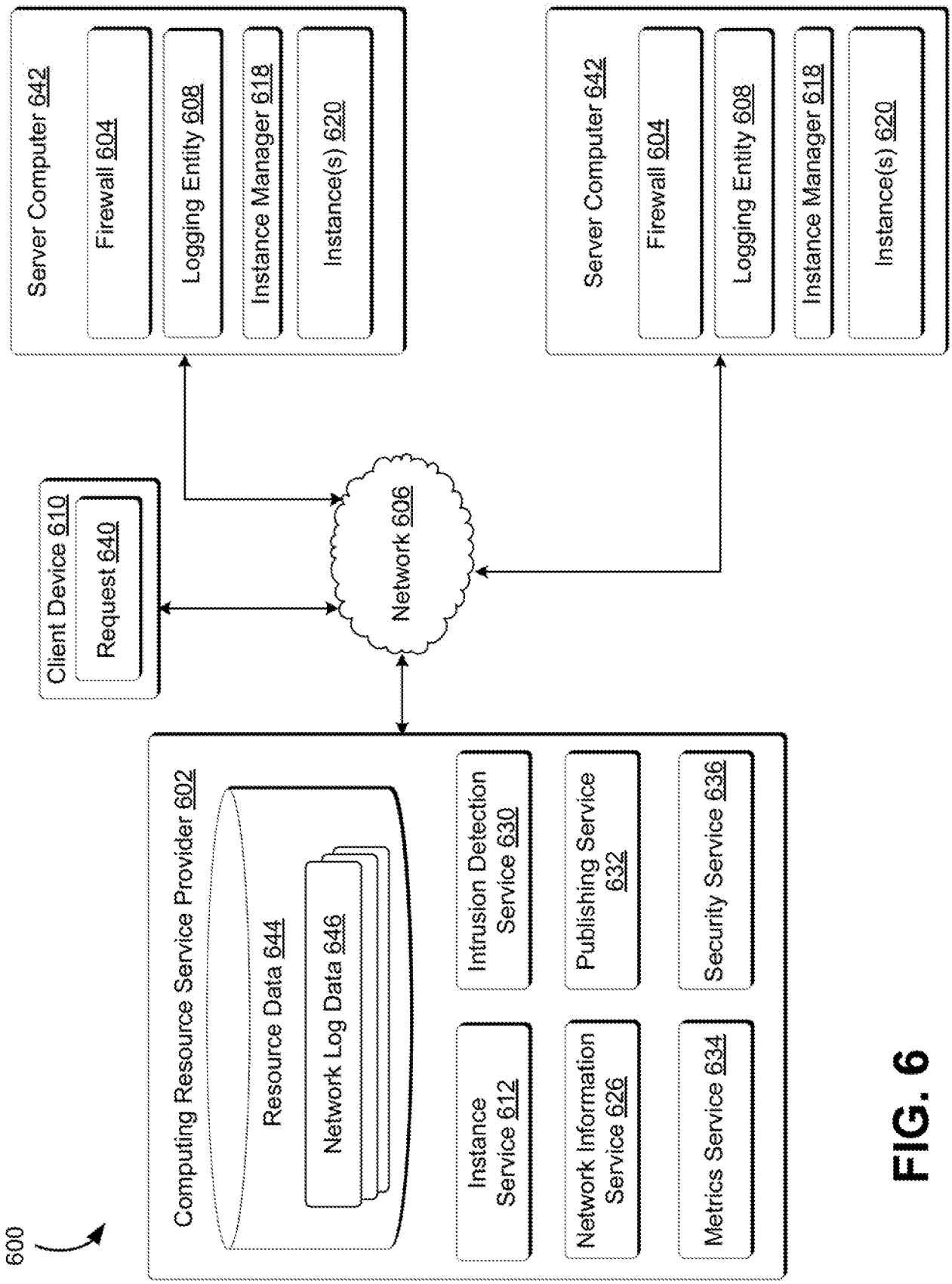
600
Computing Resource Service Provider 602
Resource Data 644
Network Log Data 646
Instance Service 612
Intrusion Detection Service 630
Publishing Service 632
Security Service 636
Network Information Service 626
Metrics Service 634
Network 606
Client Device 610
Request 640
Server Computer 642
Firewall 604
Logging Entity 608
Instance Manager 618
Instance(s) 620
Server Computer 642
Firewall 604
Logging Entity 608
Instance Manager 618
Instance(s) 620

FIG. 6

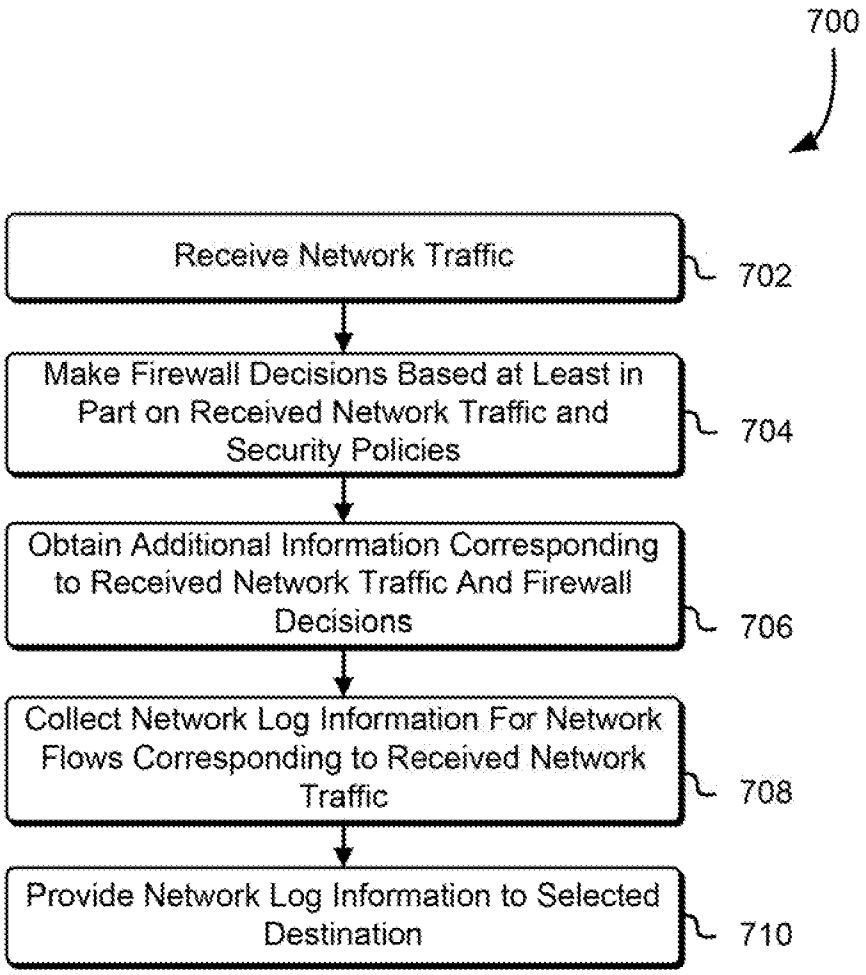
700
Receive Network Traffic
702
Make Firewall Decisions Based at Least in Part on Received Network Traffic and Security Policies
704
Obtain Additional Information Corresponding to Received Network Traffic And Firewall Decisions
706
Collect Network Log Information For Network Flows Corresponding to Received Network Traffic
708
Provide Network Log Information to Selected Destination
710

FIG. 7

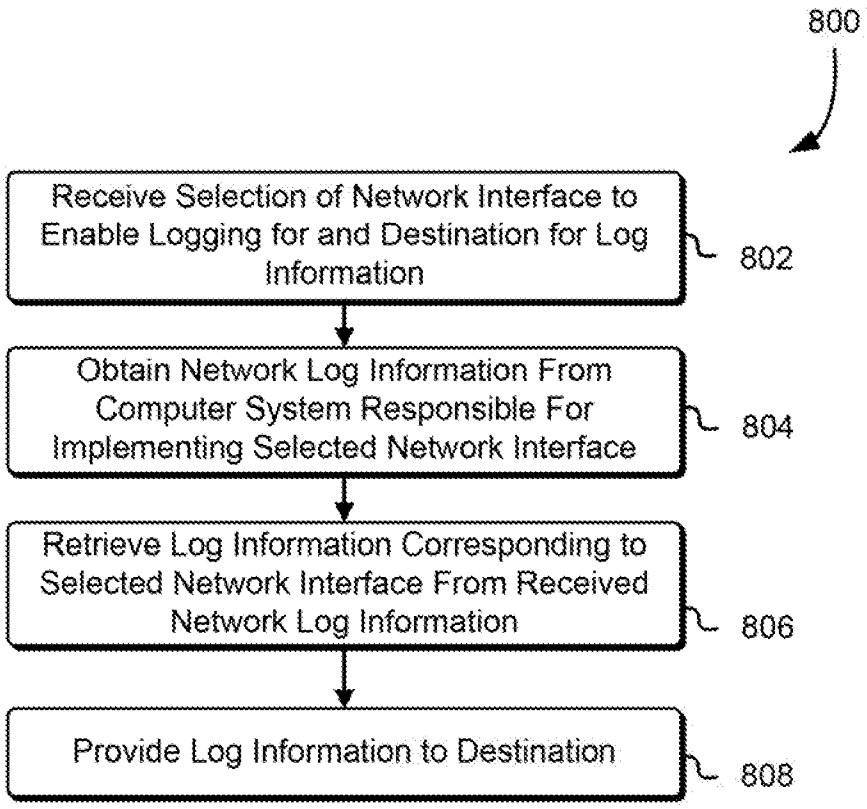
800
Receive Selection of Network Interface to Enable Logging for and Destination for Log Information
802
Obtain Network Log Information From Computer System Responsible For Implementing Selected Network Interface
804
Retrieve Log Information Corresponding to Selected Network Interface From Received Network Log Information
806
Provide Log Information to Destination
808

FIG. 8

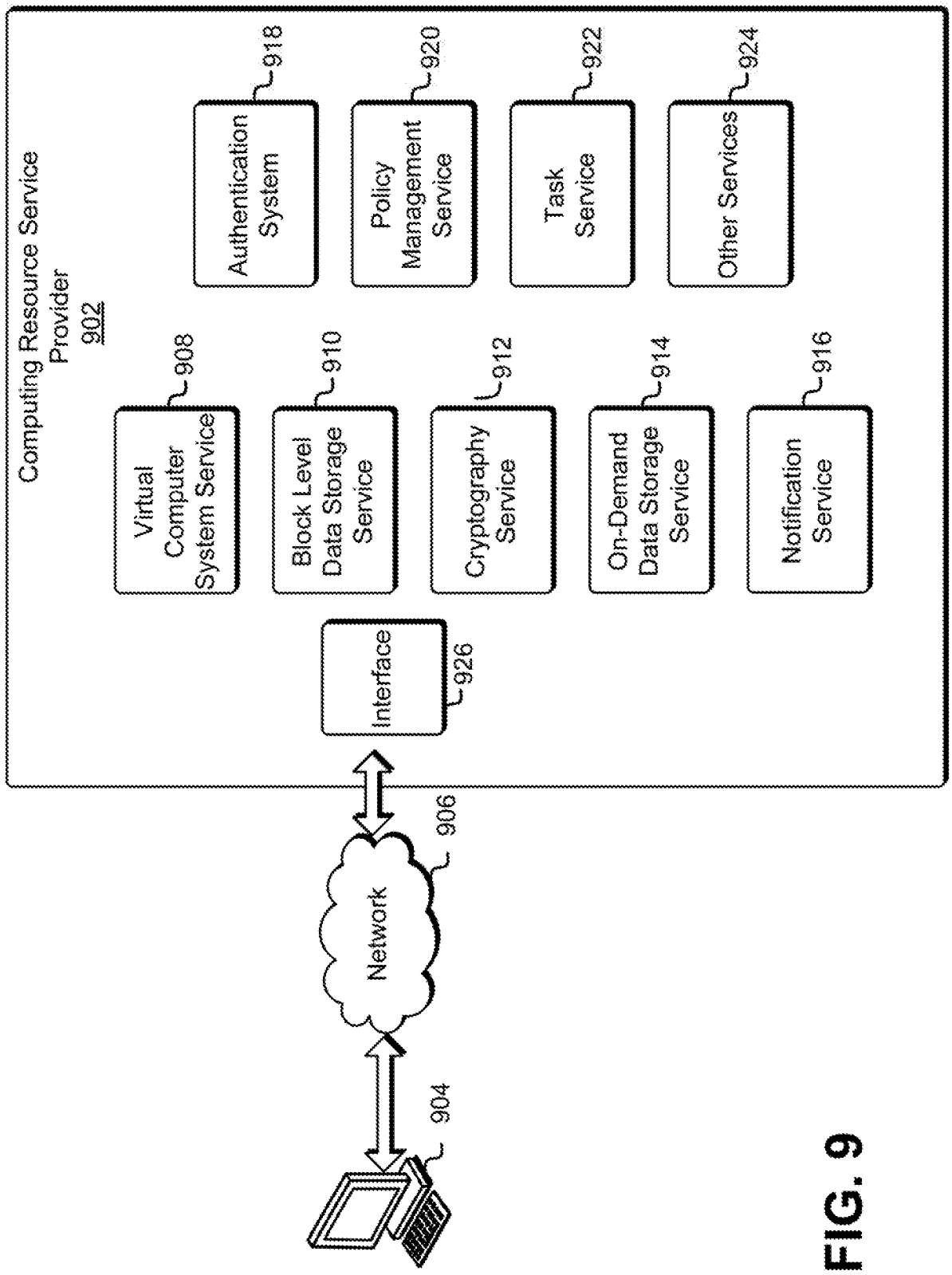
Computing Resource Service Provider
902
Virtual Computer System Service
908
Block Level Data Storage Service
910
Cryptography Service
912
On-Demand Data Storage Service
914
Notification Service
916
Authentication System
918
Policy Management Service
920
Task Service
922
Other Services
924
Interface
926
Network
906
904

FIG. 9

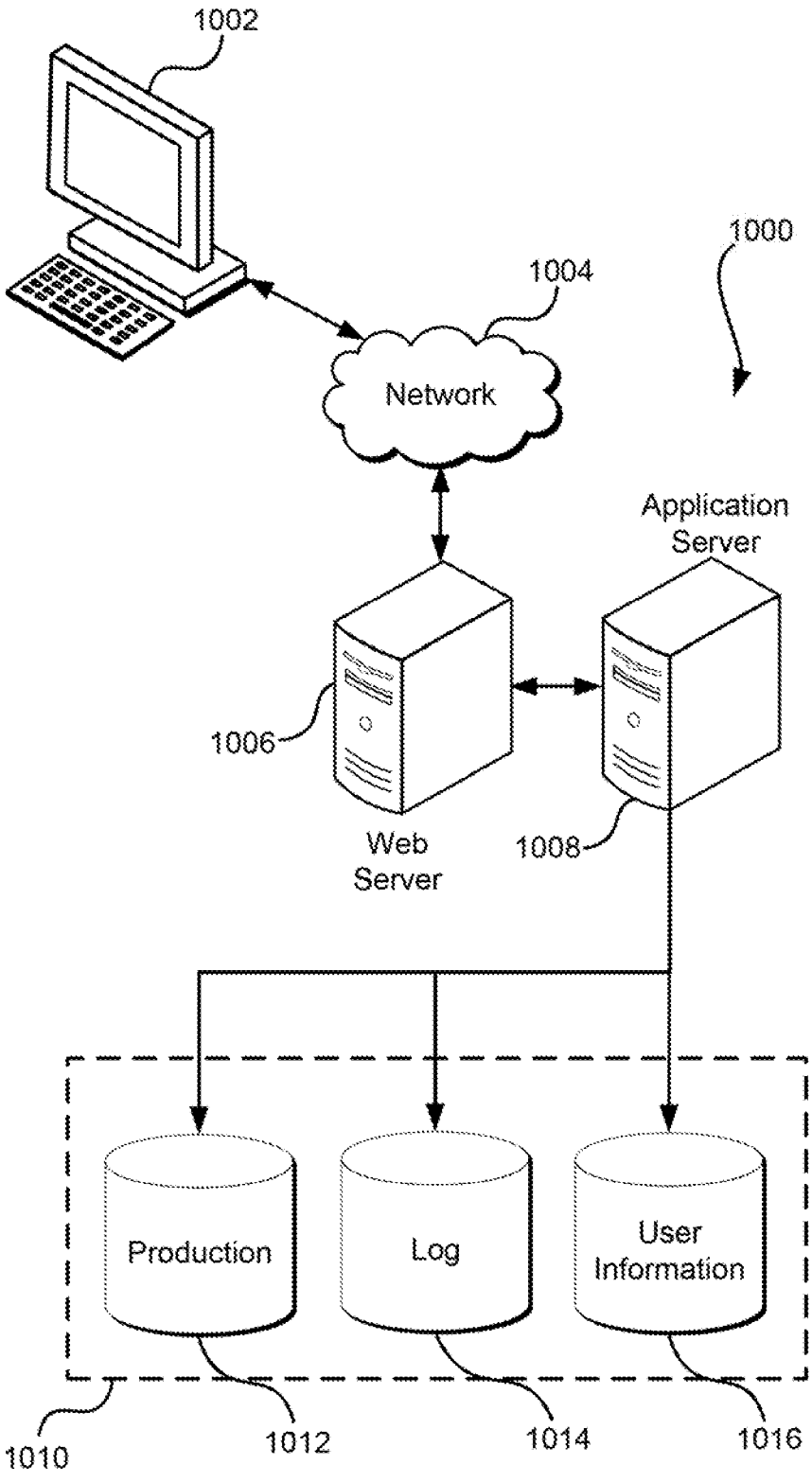
1002
1000
1004
Network
Application
Server
1006
Web
Server
1008
Production
Log
User
Information
1010
1012
1014
1016

FIG. 10

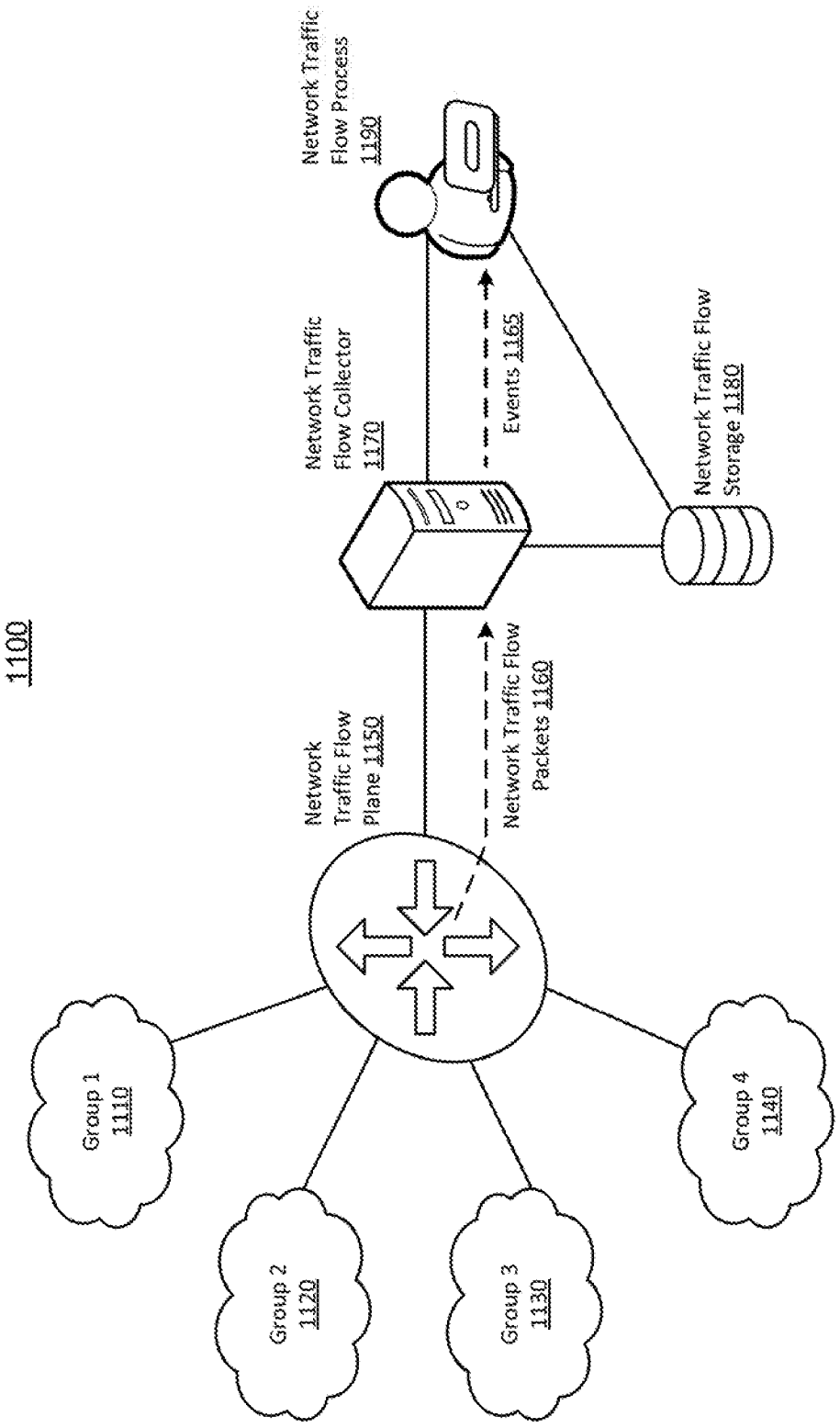
1100
Network Traffic Flow Process 1190
Network Traffic Flow Collector 1170
Events 1165
Network Traffic Flow Storage 1180
Network Traffic Flow Plane 1150
Network Traffic Flow Packets 1160
Group 1 1110
Group 2 1120
Group 3 1130
Group 4 1140

FIG. 11

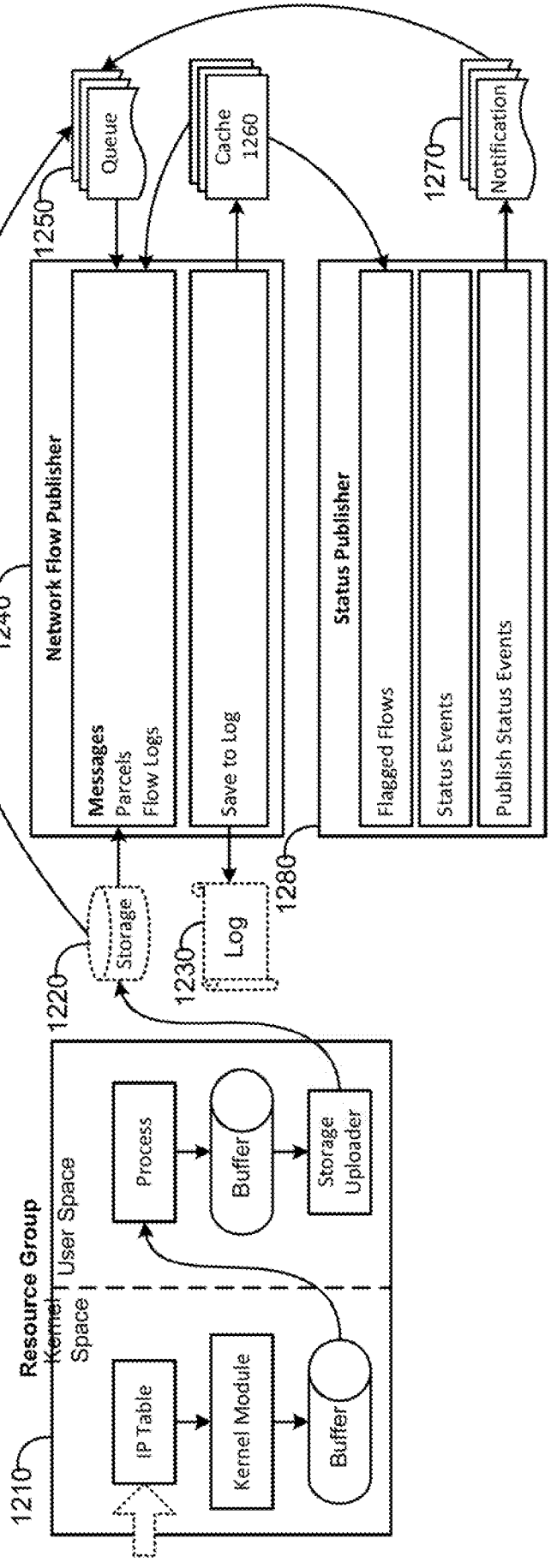
Queue
Cache
1260
Notification
1270
1250
Network Flow Publisher
Messages
Parcels
Flow Logs
Save to Log
Status Publisher
Flagged Flows
Status Events
Publish Status Events
1240
1280
Storage
Log
1230
1220
Resource Group
Kernel Space
User Space
IP Table
Kernel Module
Buffer
Process
Buffer
Storage Uploader
1210

FIG. 12

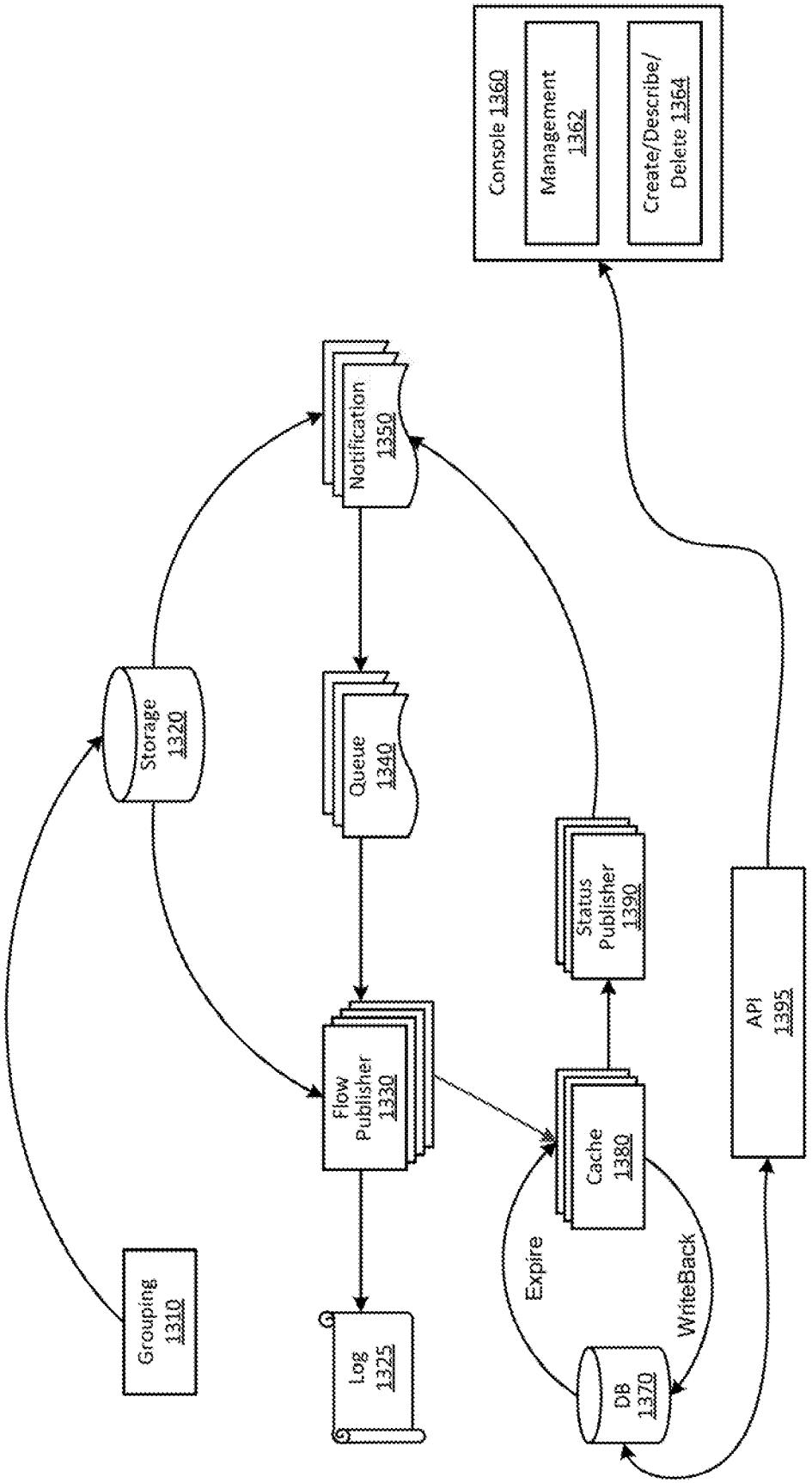
Console 1360
Management 1362
Create/Describe/ Delete 1364
Notification 1350
Storage 1320
Queue 1340
Status Publisher 1390
API 1395
Flow Publisher 1330
Cache 1380
Grouping 1310
Log 1325
Expire
WriteBack
DB 1370

FIG. 13

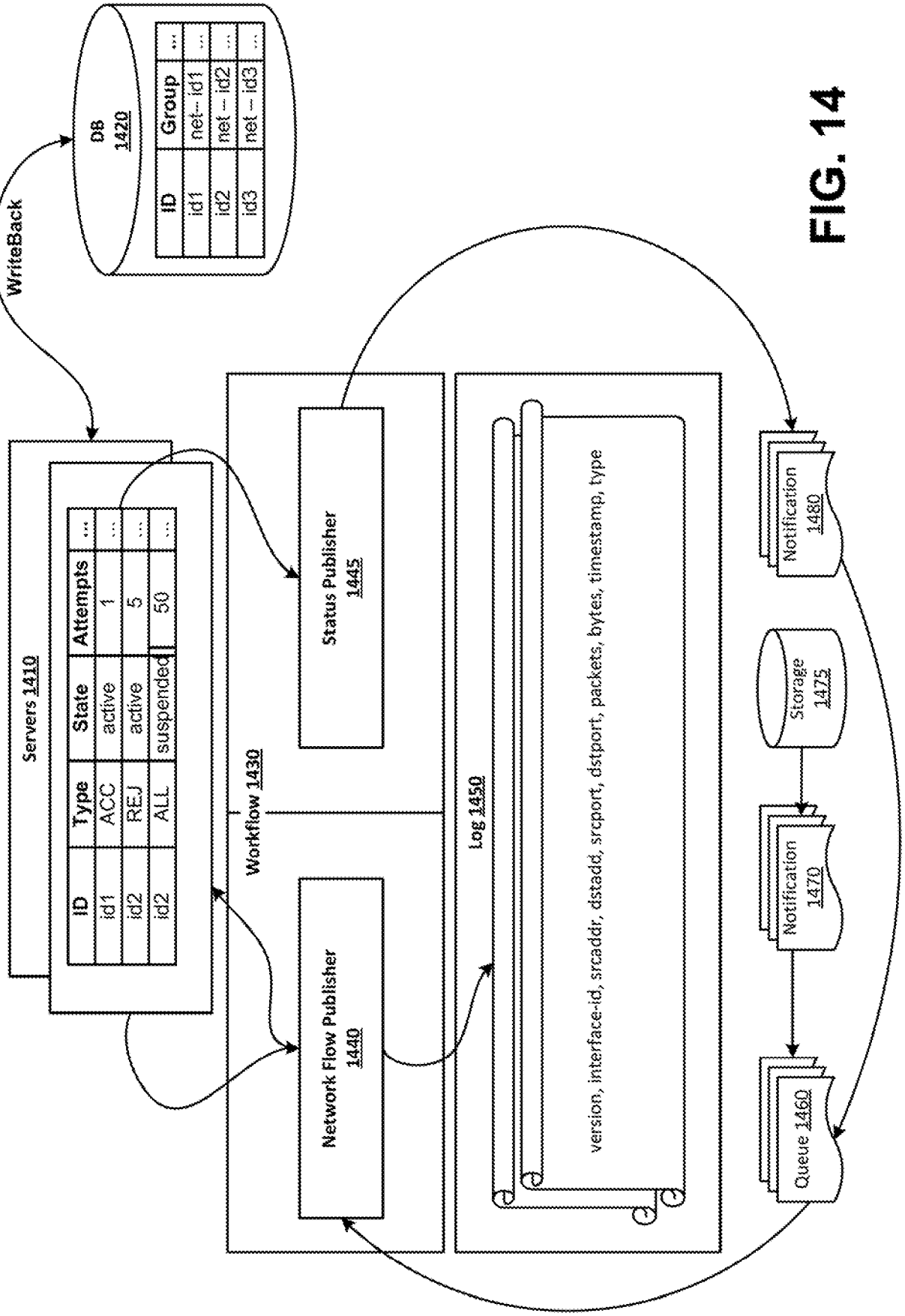
DB
1420
ID
Group
id1
net-- id1
id2
net -- id2
id3
net -- id3
WriteBack
Servers 1410
ID
Type
State
Attempts
id1
ACC
active
1
id2
REJ
active
5
id2
ALL
suspended
50
Workflow 1430
Status Publisher
1445
Network Flow Publisher
1440
Log 1450
version, interface-id, srcaddr, dstadd, srcport, dstport, packets, bytes, timestamp, type
Notification
1480
Storage
1475
Notification
1470
Queue 1460

FIG. 14

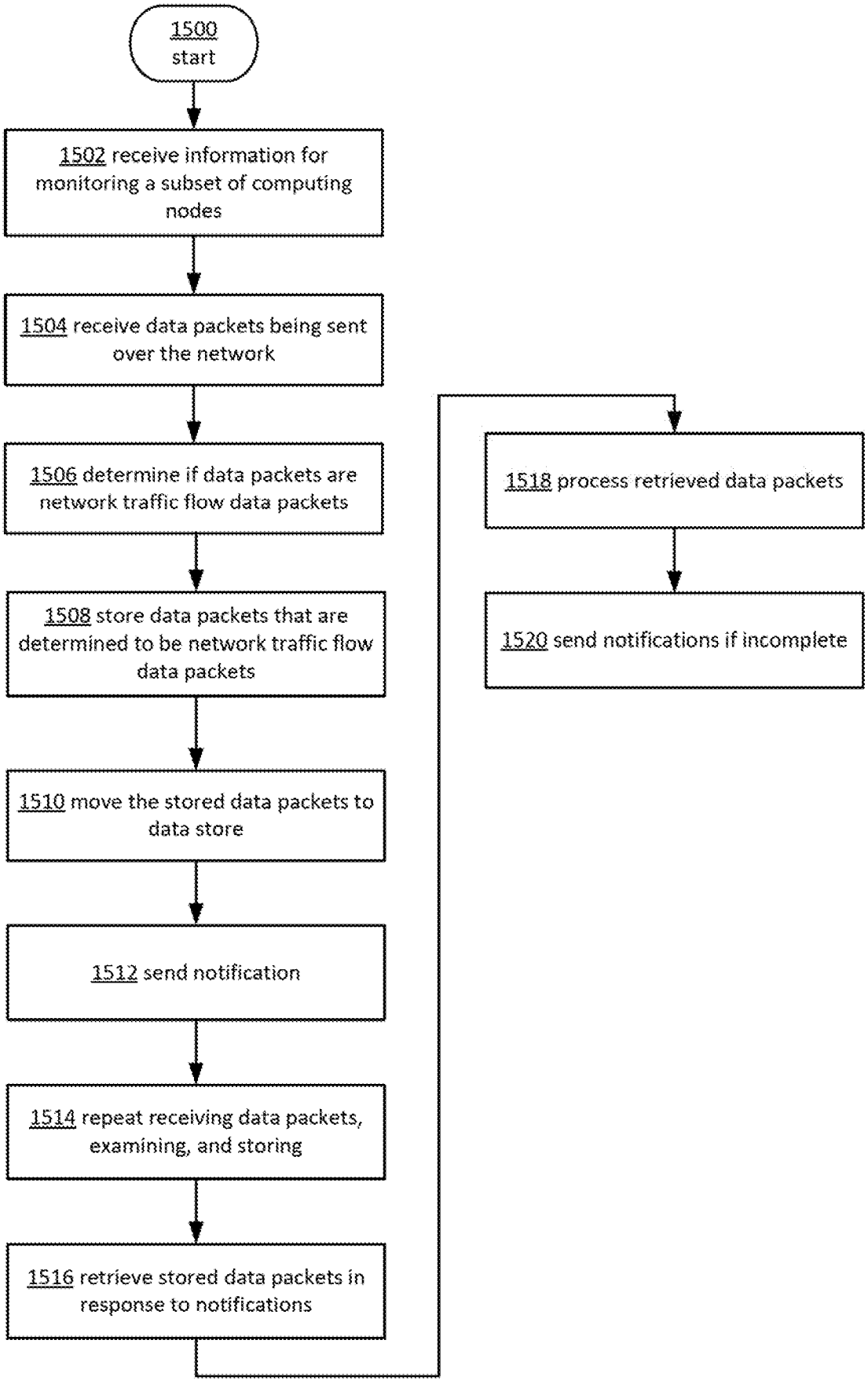
1500 start
1502 receive information for monitoring a subset of computing nodes
1504 receive data packets being sent over the network
1506 determine if data packets are network traffic flow data packets
1508 store data packets that are determined to be network traffic flow data packets
1510 move the stored data packets to data store
1512 send notification
1514 repeat receiving data packets, examining, and storing
1516 retrieve stored data packets in response to notifications
1518 process retrieved data packets
1520 send notifications if incomplete

FIG. 15

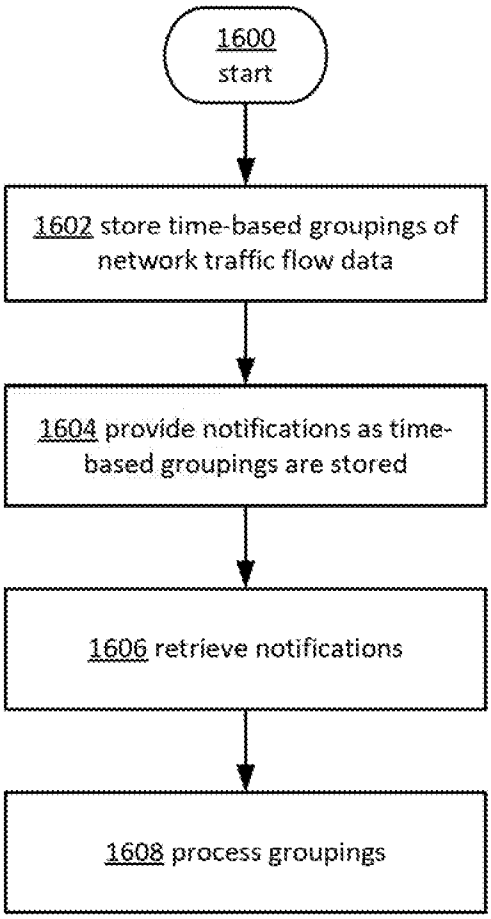
1600
start
1602 store time-based groupings of network traffic flow data
1604 provide notifications as time-based groupings are stored
1606 retrieve notifications
1608 process groupings

FIG. 16

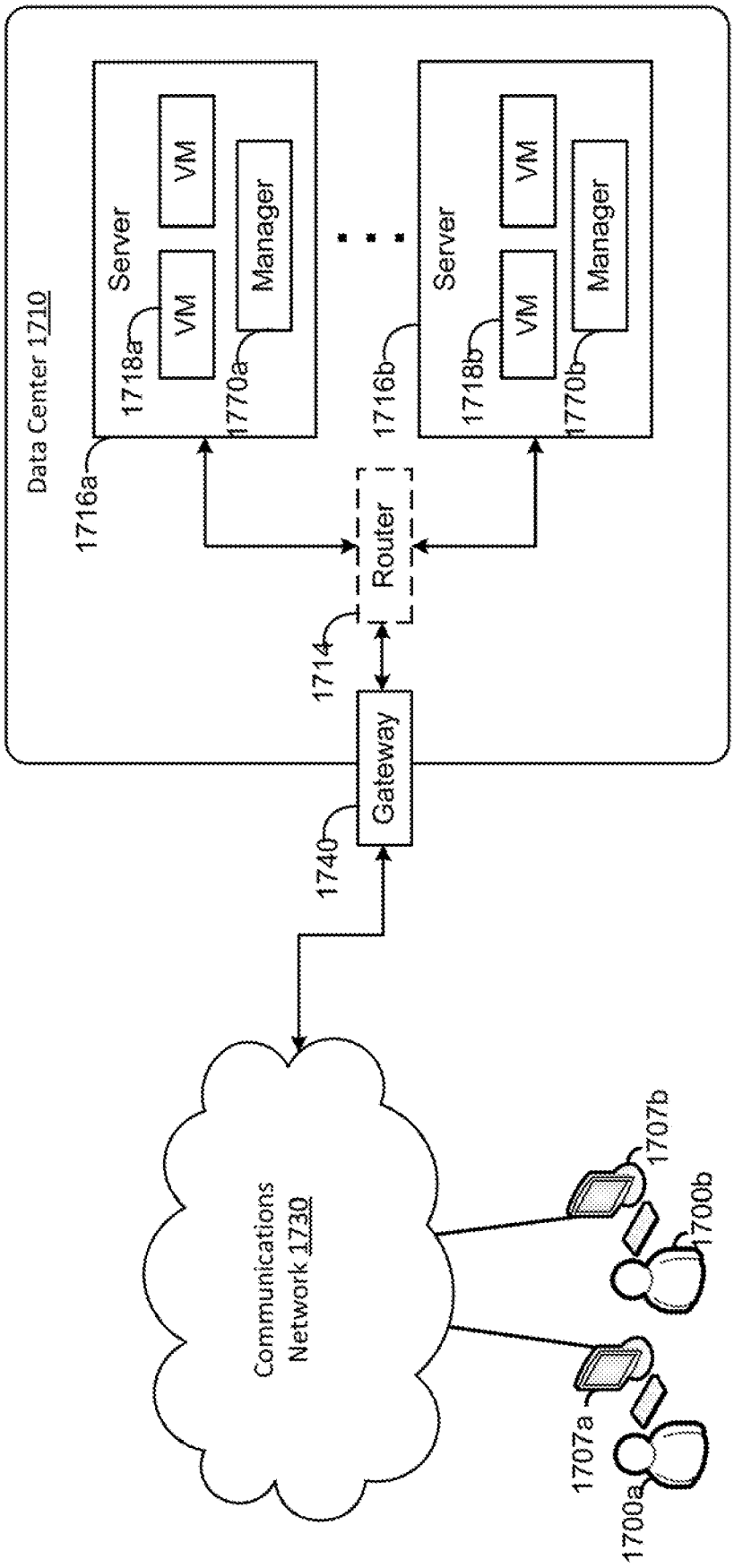
Data Center 1710
1716a
Server
1718a
VM
VM
Manager
1770a
1716b
Server
1718b
VM
VM
Manager
1770b
Router
1714
Gateway
1740
Communications Network 1730
1707a
1700a
1707b
1700b

FIG. 17

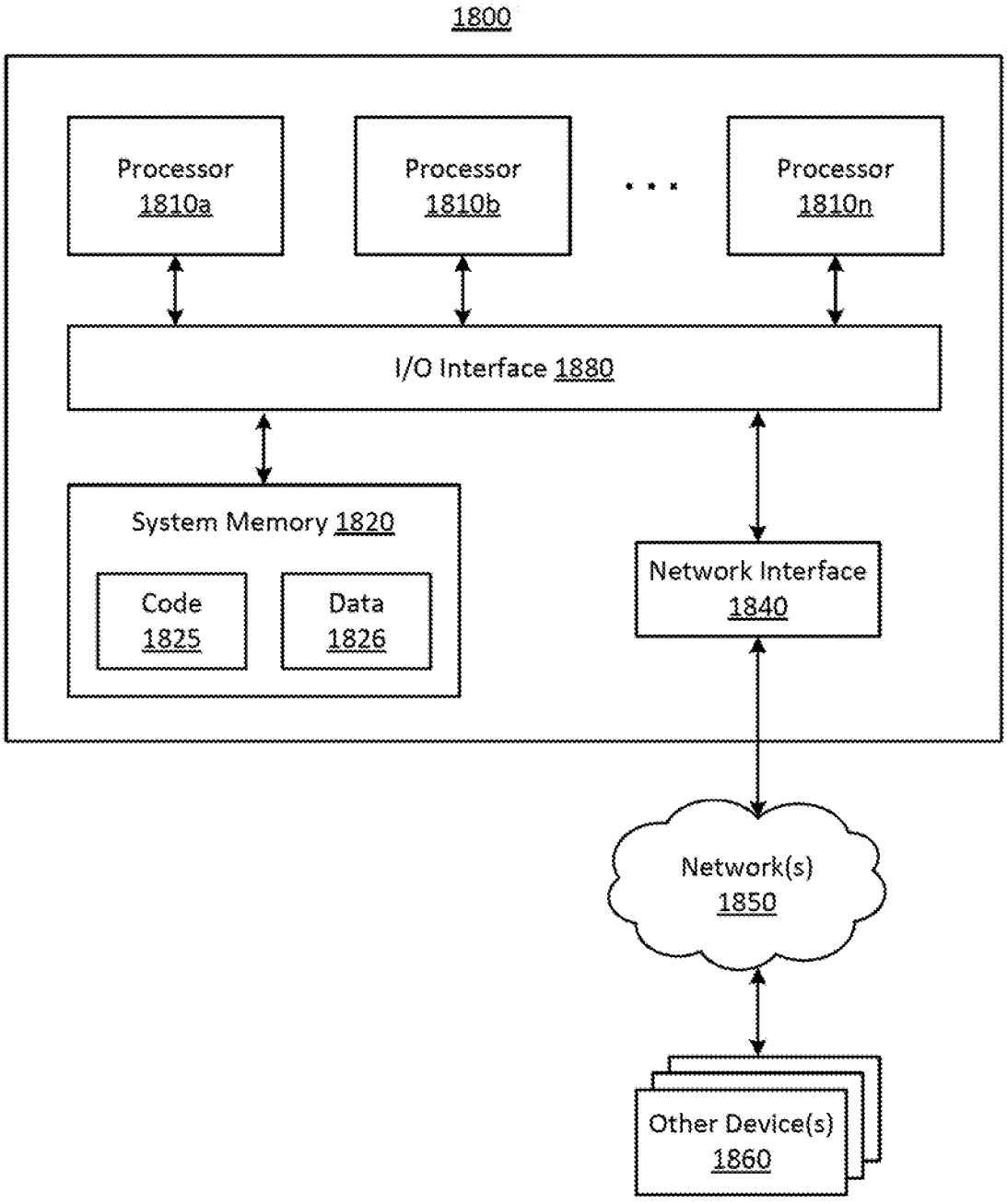
1800
Processor
1810a
Processor
1810b
Processor
1810n
I/O Interface 1880
System Memory 1820
Code
1825
Data
1826
Network Interface
1840
Network(s)
1850
Other Device(s)
1860

FIG. 18

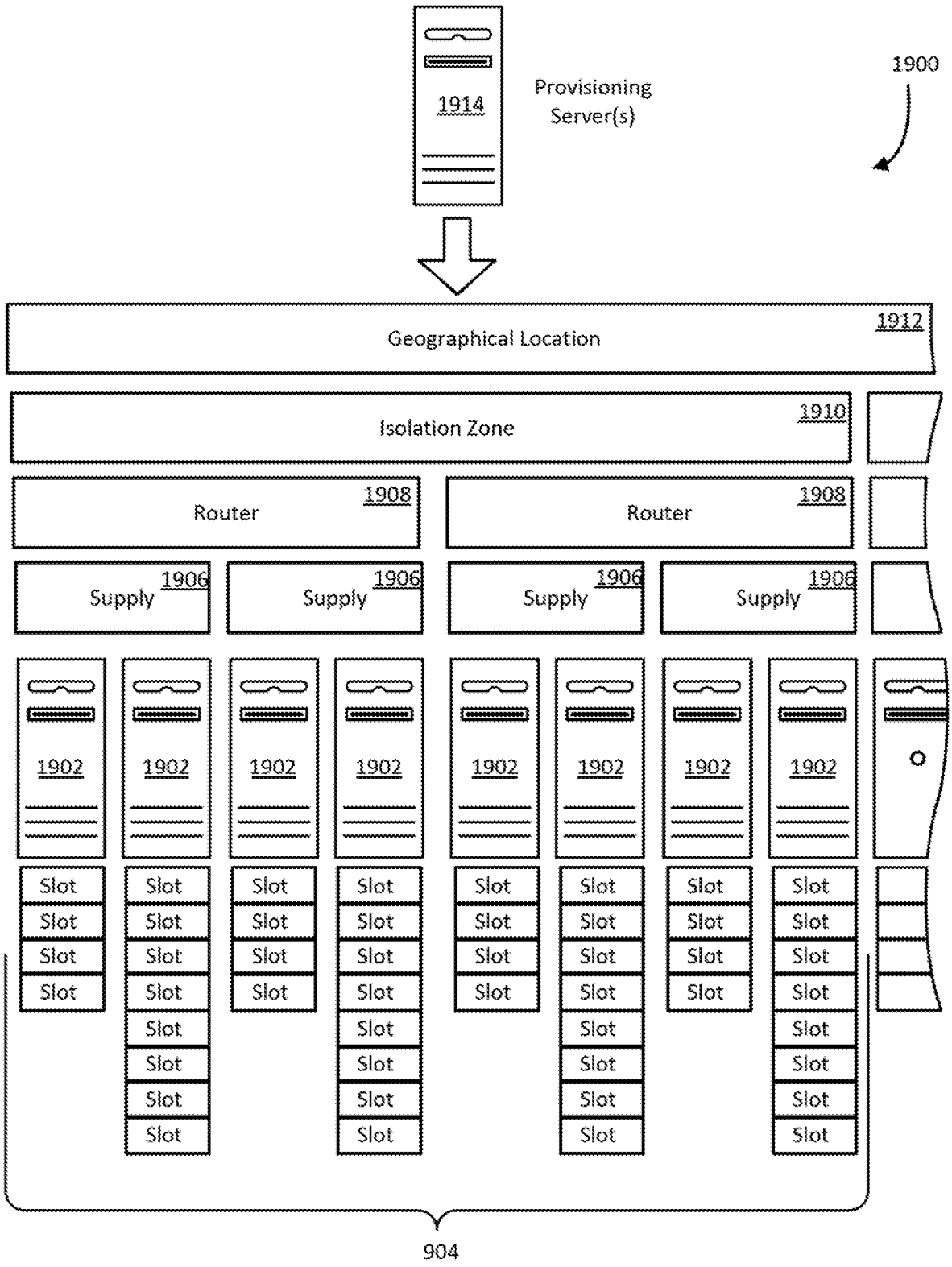
1914
Provisioning Server(s)
1900
Geographical Location
1912
Isolation Zone
1910
Router
1908
Router
1908
Supply
1906
Supply
1906
Supply
1906
Supply
1906
1902
1902
1902
1902
1902
1902
1902
1902
Slot
904

FIG. 19