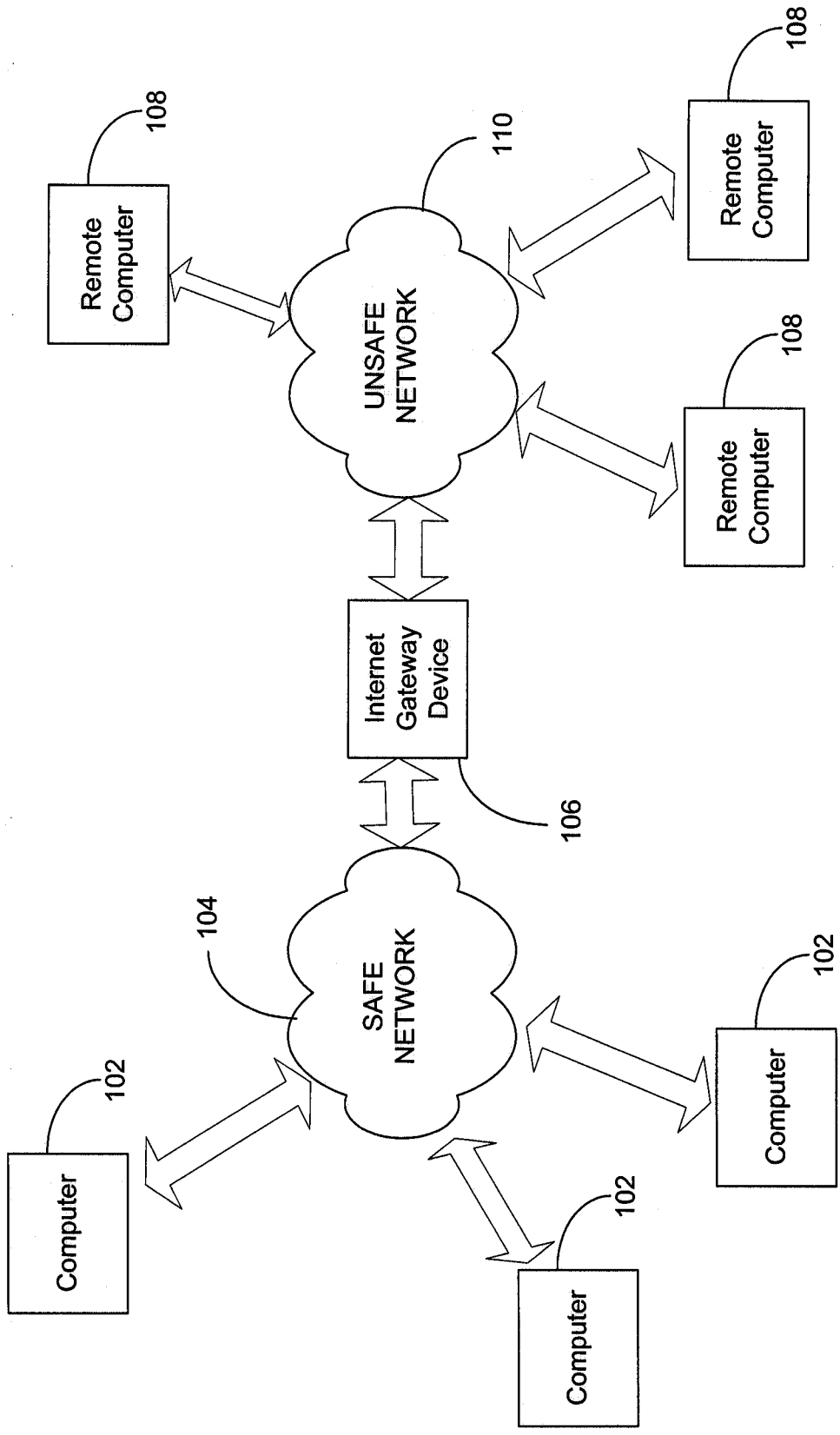

Remote Computer
108
UNSAFE NETWORK
110
Remote Computer
108
Remote Computer
108
Internet Gateway Device
106
SAFE NETWORK
104
Computer
102
Computer
102
Computer
102

FIG. 1

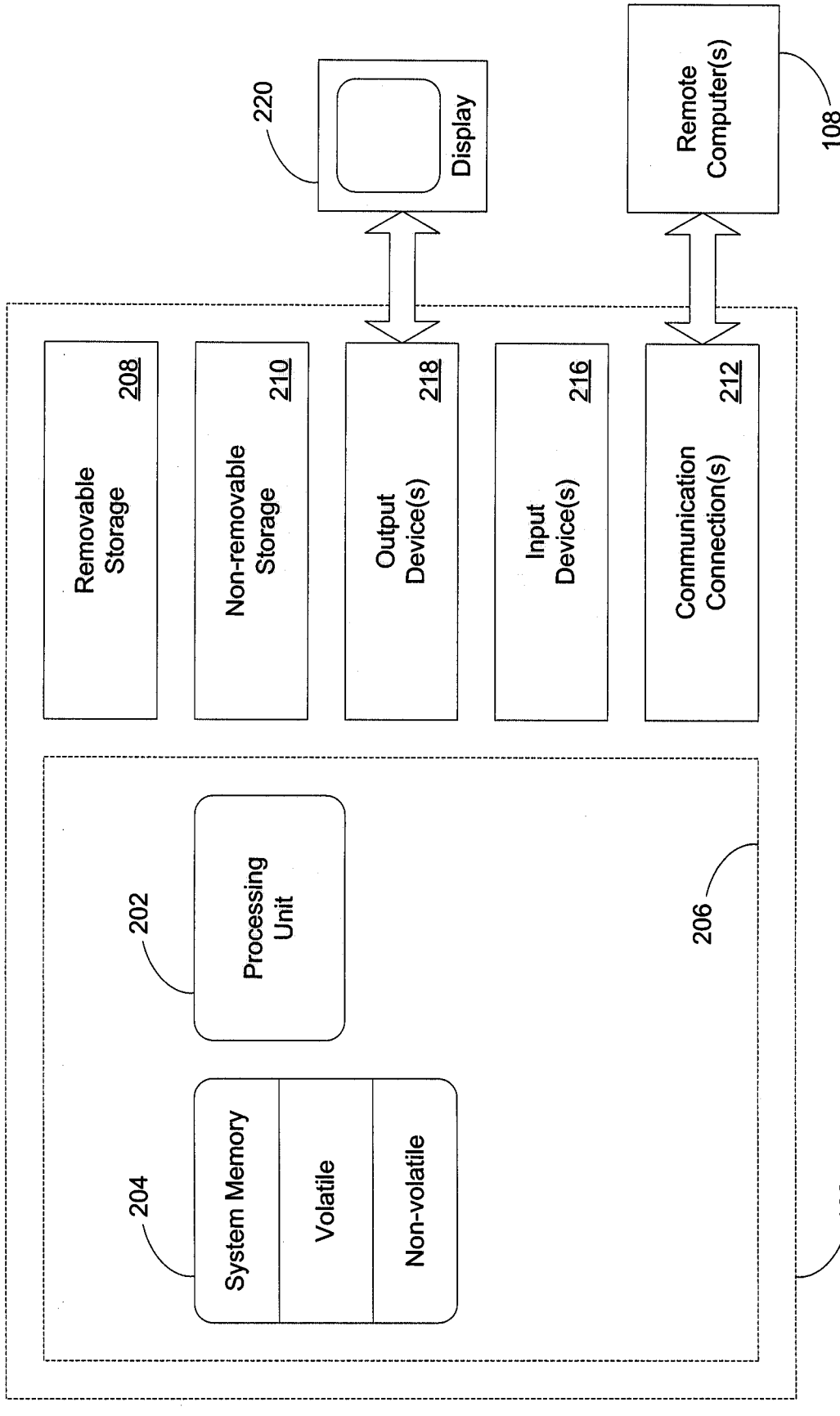

220
Display
Remote Computer(s)
108
Removable Storage 208
Non-removable Storage 210
Output Device(s) 218
Input Device(s) 216
Communication Connection(s) 212
202
Processing Unit
206
204
System Memory
Volatile
Non-volatile
102

FIG. 2

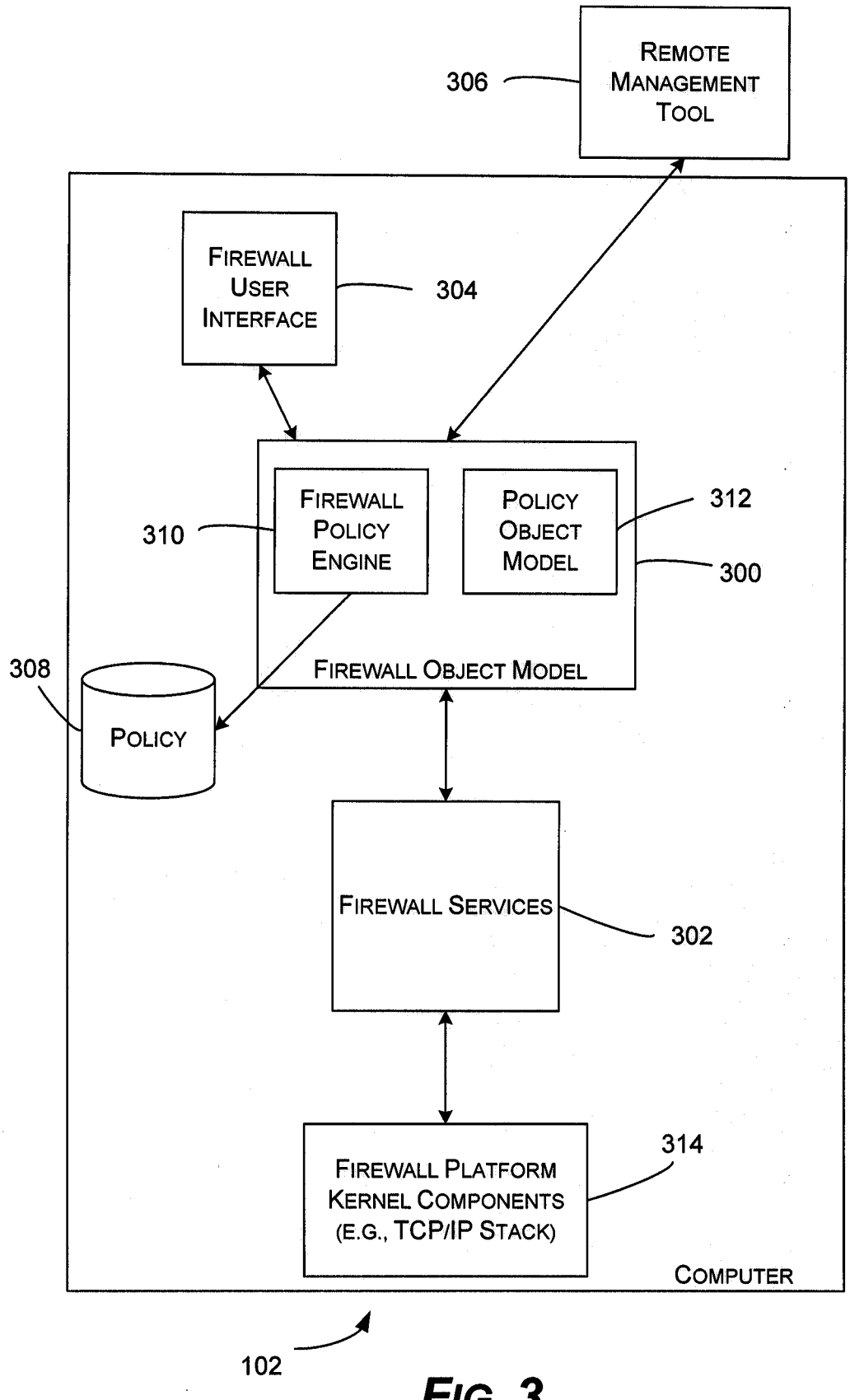

REMOTE MANAGEMENT TOOL
306
FIREWALL USER INTERFACE
304
FIREWALL POLICY ENGINE
310
POLICY OBJECT MODEL
312
300
FIREWALL OBJECT MODEL
308
POLICY
FIREWALL SERVICES
302
FIREWALL PLATFORM KERNEL COMPONENTS (E.G., TCP/IP STACK)
314
COMPUTER
102

FIG. 3

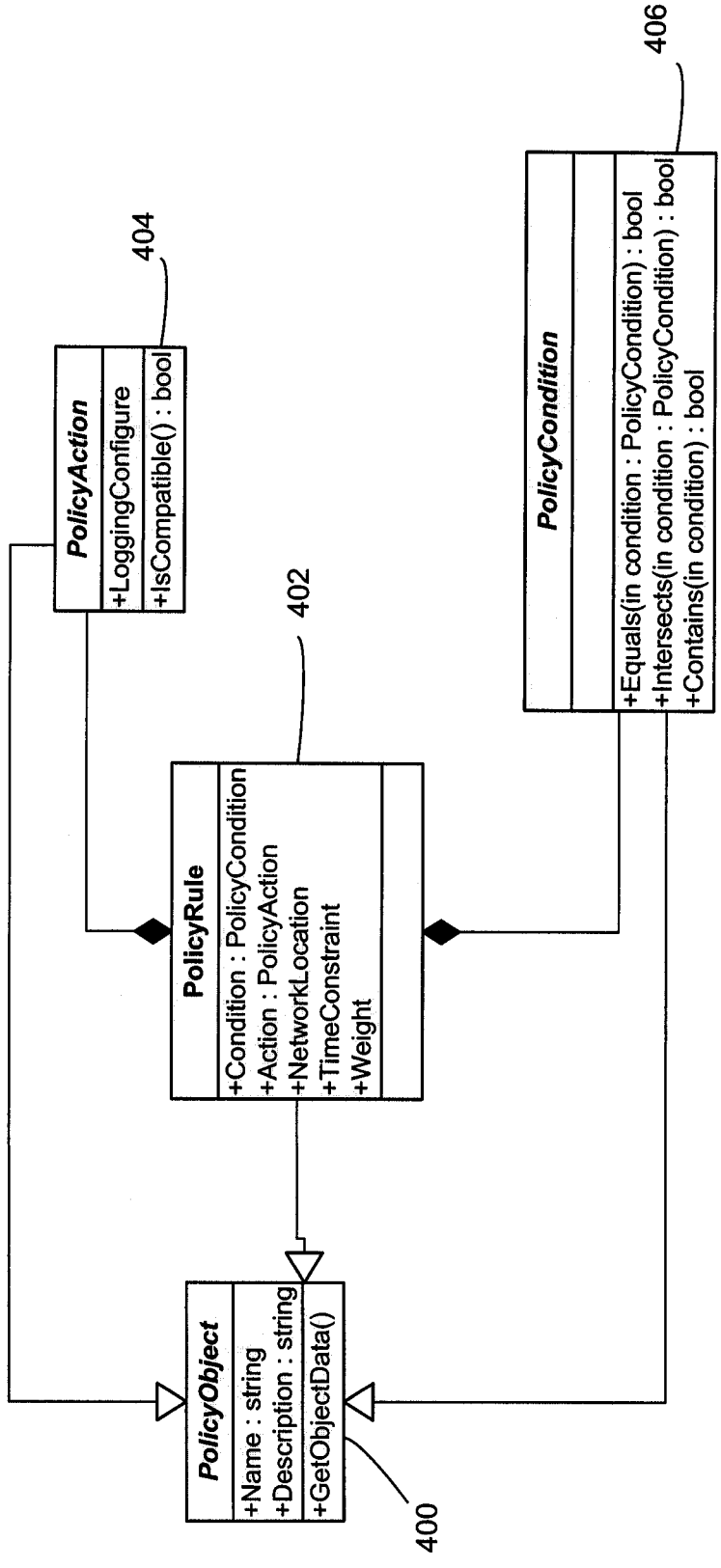

PolicyObject
+Name : string
+Description : string
+GetObjectData()
400
PolicyRule
+Condition : PolicyCondition
+Action : PolicyAction
+NetworkLocation
+TimeConstraint
+Weight
402
PolicyAction
+LoggingConfigure
+IsCompatible() : bool
404
PolicyCondition
+Equals(in condition : PolicyCondition) : bool
+Intersects(in condition : PolicyCondition) : bool
+Contains(in condition) : bool
406

FIG. 4

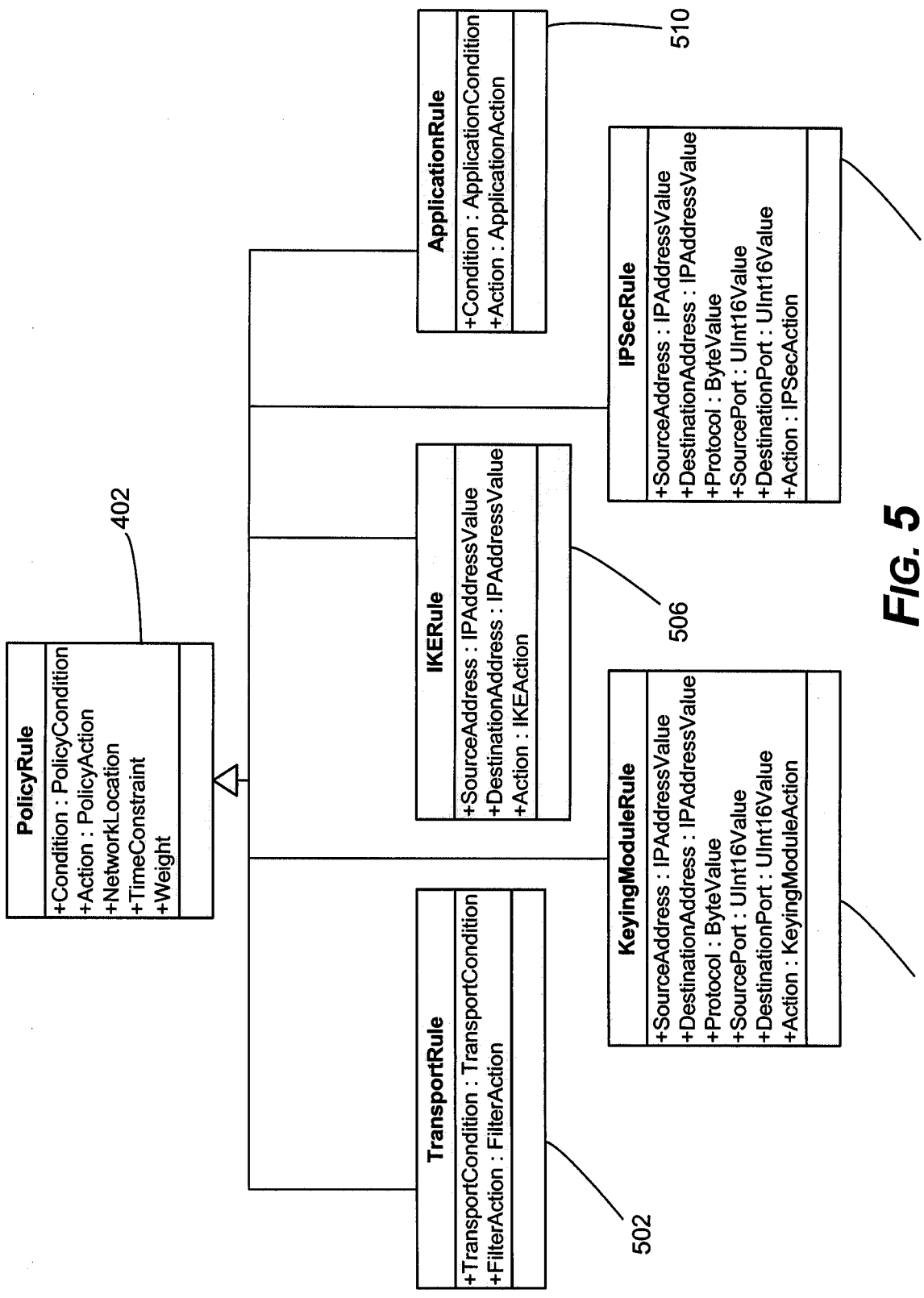

PolicyRule
+Condition : PolicyCondition
+Action : PolicyAction
+NetworkLocation
+TimeConstraint
+Weight
402
TransportRule
+TransportCondition : TransportCondition
+FilterAction : FilterAction
502
IKERule
+SourceAddress : IPAddressValue
+DestinationAddress : IPAddressValue
+Action : IKEAction
506
ApplicationRule
+Condition : ApplicationCondition
+Action : ApplicationAction
510
KeyingModuleRule
+SourceAddress : IPAddressValue
+DestinationAddress : IPAddressValue
+Protocol : ByteValue
+SourcePort : UInt16Value
+DestinationPort : UInt16Value
+Action : KeyingModuleAction
504
IPSecRule
+SourceAddress : IPAddressValue
+DestinationAddress : IPAddressValue
+Protocol : ByteValue
+SourcePort : UInt16Value
+DestinationPort : UInt16Value
+Action : IPSecAction
508

FIG. 5

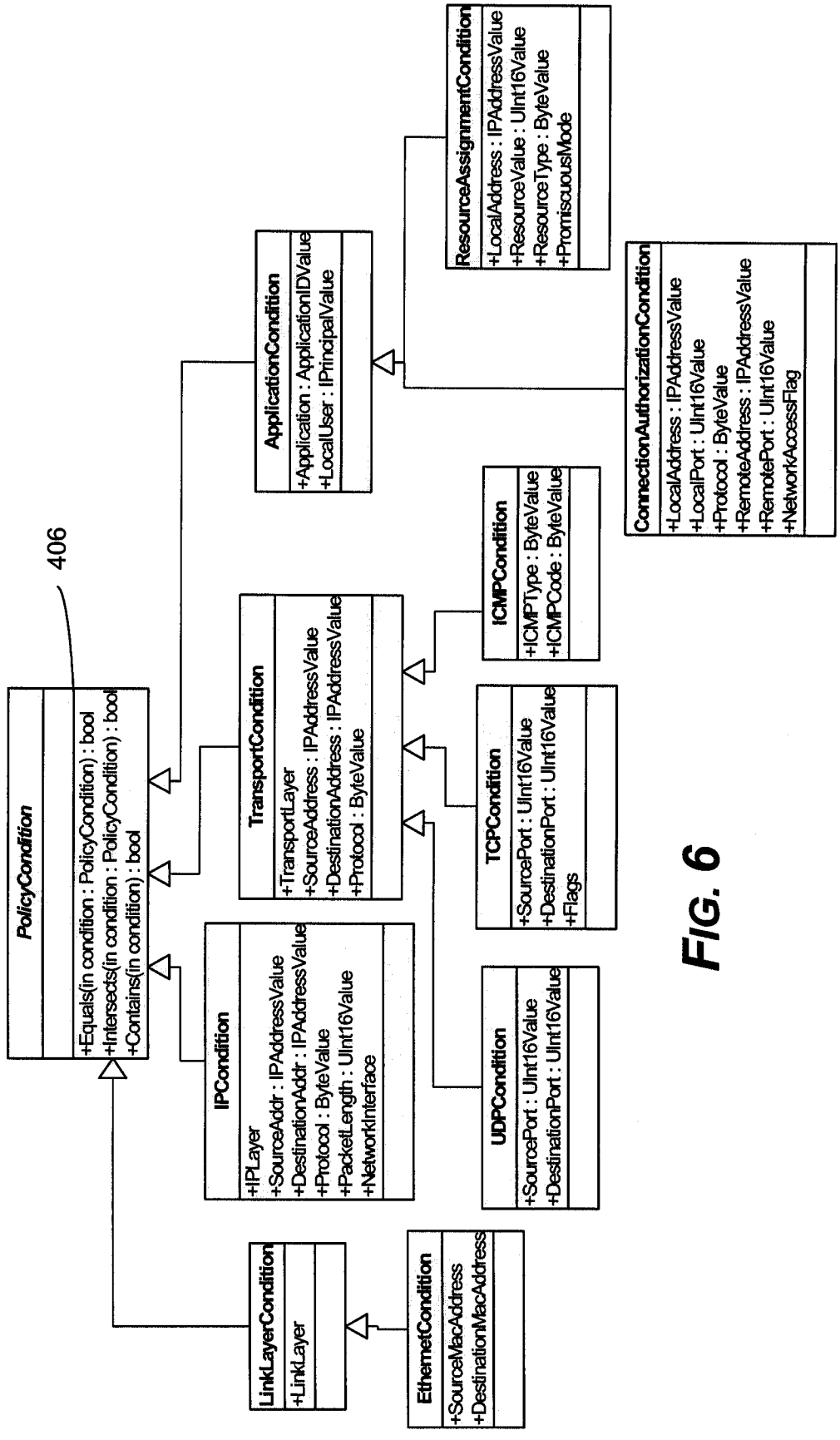

406
PolicyCondition
+Equals(in condition : PolicyCondition) : bool
+Intersects(in condition : PolicyCondition) : bool
+Contains(in condition) : bool
ApplicationCondition
+Application : ApplicationIDValue
+LocalUser : IPrincipalValue
ResourceAssignmentCondition
+LocalAddress : IPAddressValue
+ResourceValue : UInt16Value
+ResourceType : ByteValue
+PromiscuousMode
ConnectionAuthorizationCondition
+LocalAddress : IPAddressValue
+LocalPort : UInt16Value
+Protocol : ByteValue
+RemoteAddress : IPAddressValue
+RemotePort : UInt16Value
+NetworkAccessFlag
TransportCondition
+TransportLayer
+SourceAddress : IPAddressValue
+DestinationAddress : IPAddressValue
+Protocol : ByteValue
ICMPCondition
+ICMPType : ByteValue
+ICMPCode : ByteValue
IPCondition
+IPLayer
+SourceAddr : IPAddressValue
+DestinationAddr : IPAddressValue
+Protocol : ByteValue
+PacketLength : UInt16Value
+NetworkInterface
TCPCondition
+SourcePort : UInt16Value
+DestinationPort : UInt16Value
+Flags
UDPCondition
+SourcePort : UInt16Value
+DestinationPort : UInt16Value
LinkLayerCondition
+LinkLayer
EthernetCondition
+SourceMacAddress
+DestinationMacAddress

FIG. 6

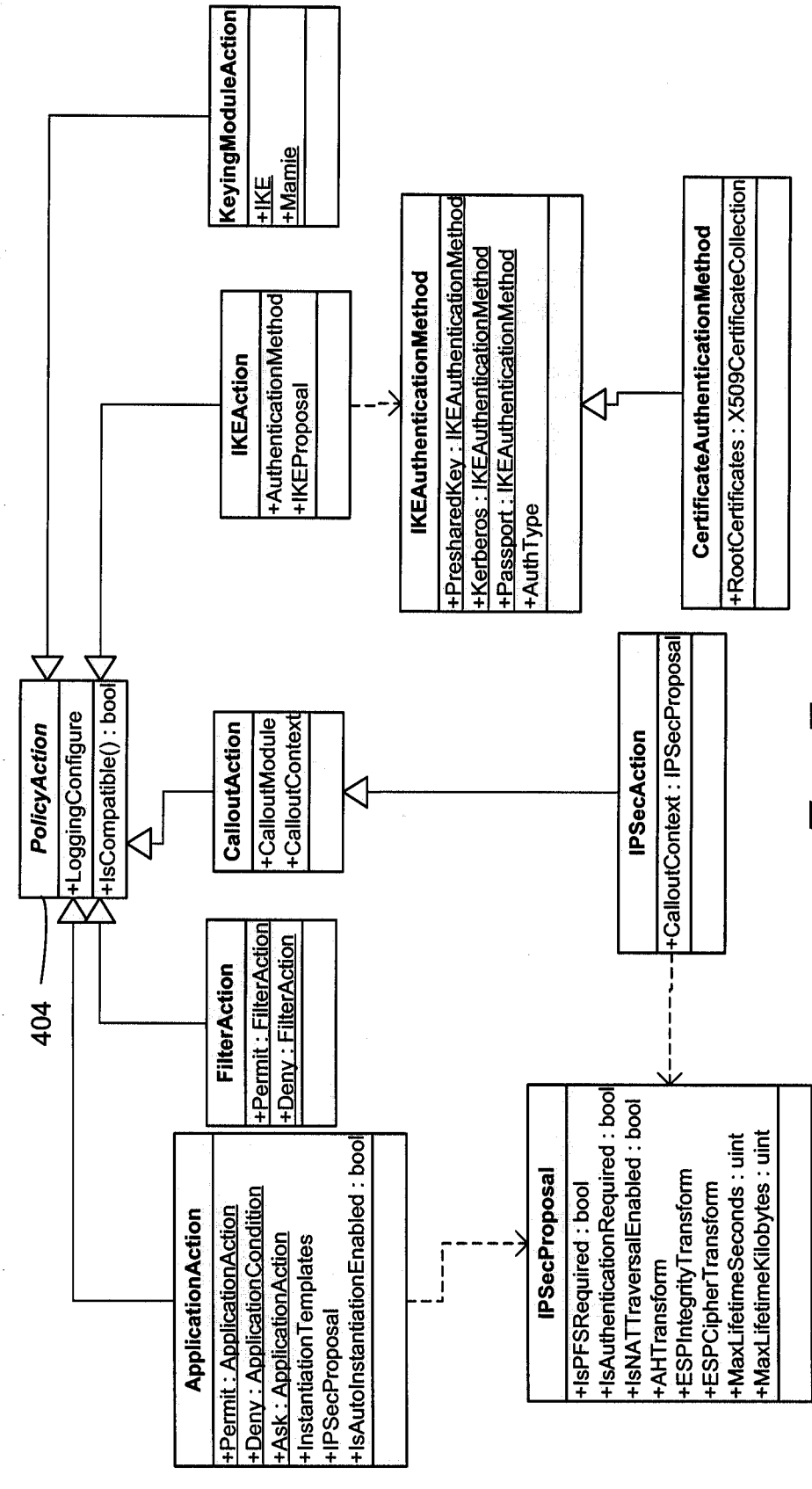

PolicyAction
+LoggingConfigure
+IsCompatible() : bool
404
KeyingModuleAction
+IKE
+Mamie
IKEAction
+AuthenticationMethod
+IKEProposal
IKEAuthenticationMethod
+PresharedKey : IKEAuthenticationMethod
+Kerberos : IKEAuthenticationMethod
+Passport : IKEAuthenticationMethod
+AuthType
CertificateAuthenticationMethod
+RootCertificates : X509CertificateCollection
CalloutAction
+CalloutModule
+CalloutContext
IPSecAction
+CalloutContext : IPSecProposal
FilterAction
+Permit : FilterAction
+Deny : FilterAction
ApplicationAction
+Permit : ApplicationAction
+Deny : ApplicationCondition
+Ask : ApplicationAction
+InstantiationTemplates
+IPSecProposal
+IsAutoInstantiationEnabled : bool
IPSecProposal
+IsPFSRequired : bool
+IsAuthenticationRequired : bool
+IsNATTraversalEnabled : bool
+AHTransform
+ESPIntegrityTransform
+ESPCipherTransform
+MaxLifetimeSeconds : uint
+MaxLifetimeKilobytes : uint

FIG. 7

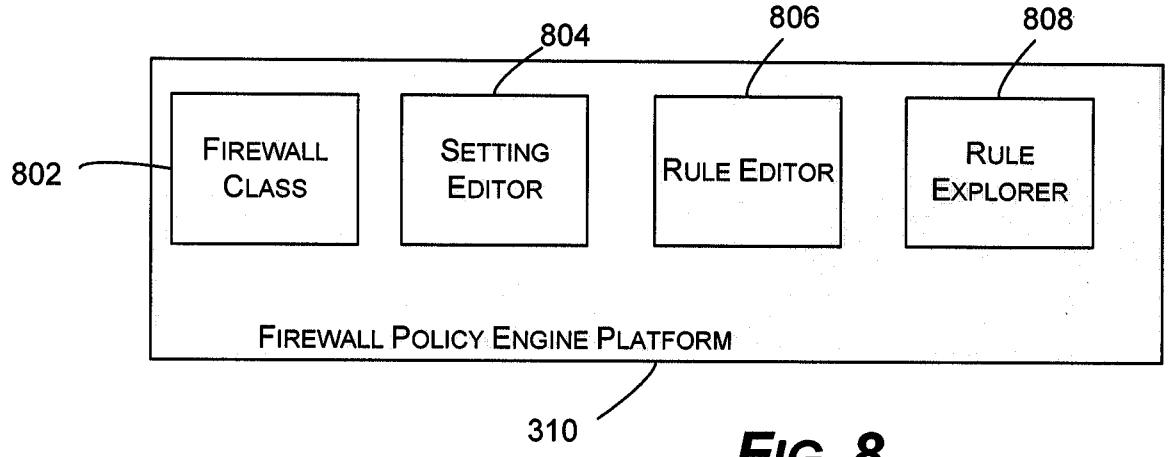

804
806
808
802
FIREWALL CLASS
SETTING EDITOR
RULE EDITOR
RULE EXPLORER
FIREWALL POLICY ENGINE PLATFORM
310

FIG. 8

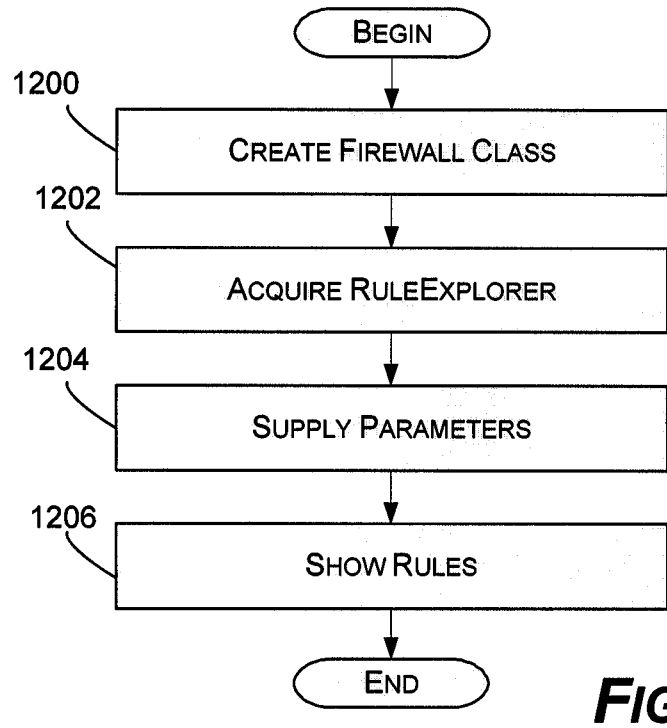

BEGIN
1200
CREATE FIREWALL CLASS
1202
ACQUIRE RULEEXPLORER
1204
SUPPLY PARAMETERS
1206
SHOW RULES
END

FIG. 12

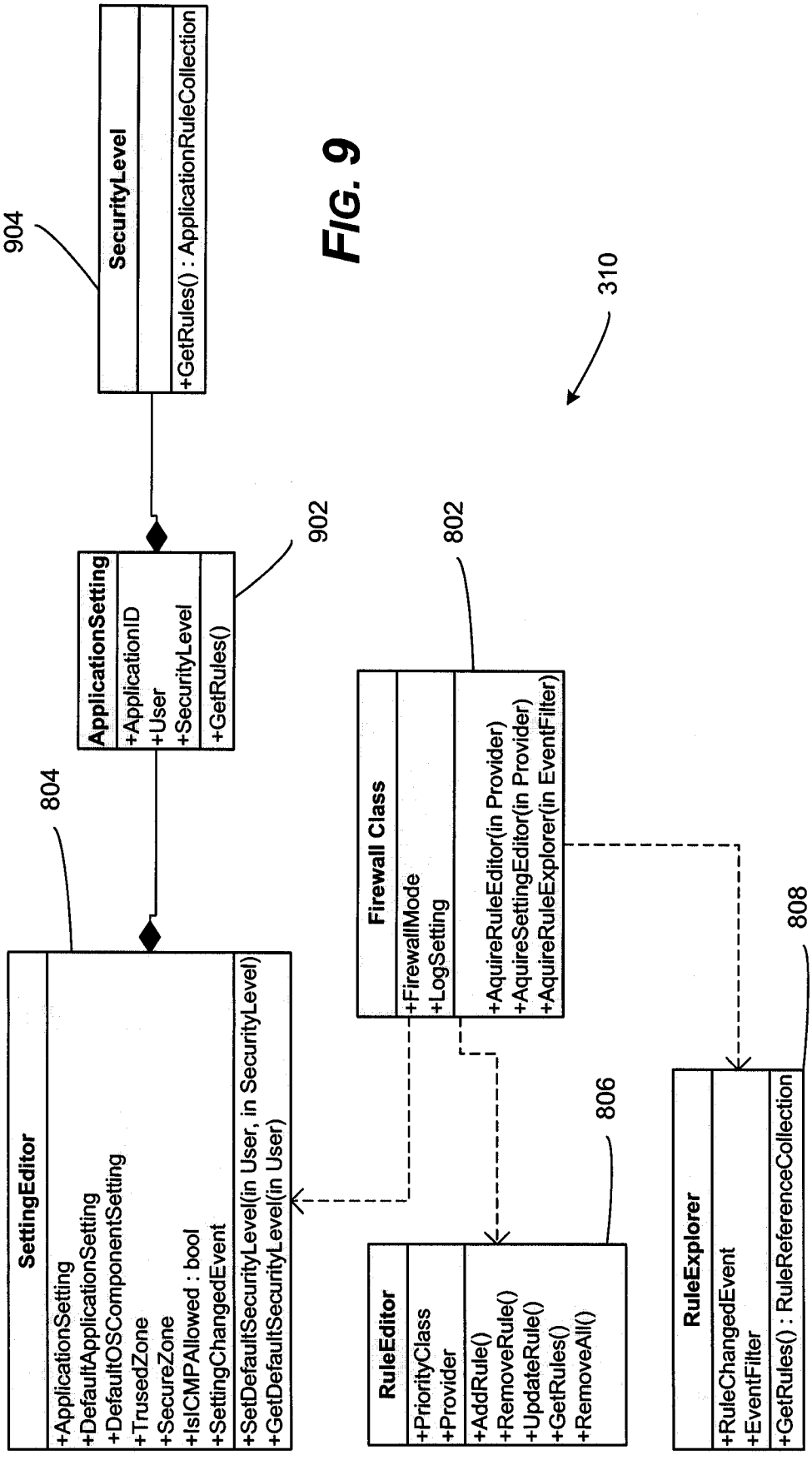

SecurityLevel
+GetRules() : ApplicationRuleCollection
904
ApplicationSetting
+ApplicationID
+User
+SecurityLevel
+GetRules()
902
SettingEditor
+ApplicationSetting
+DefaultApplicationSetting
+DefaultOSComponentSetting
+TrusedZone
+SecureZone
+IsICMPAllowed : bool
+SettingChangedEvent
+SetDefaultSecurityLevel(in User, in SecurityLevel)
+GetDefaultSecurityLevel(in User)
804
Firewall Class
+FirewallMode
+LogSetting
+AquireRuleEditor(in Provider)
+AquireSettingEditor(in Provider)
+AquireRuleExplorer(in EventFilter)
802
310
RuleEditor
+PriorityClass
+Provider
+AddRule()
+RemoveRule()
+UpdateRule()
+GetRules()
+RemoveAll()
806
RuleExplorer
+RuleChangedEvent
+EventFilter
+GetRules() : RuleReferenceCollection
808

FIG. 9

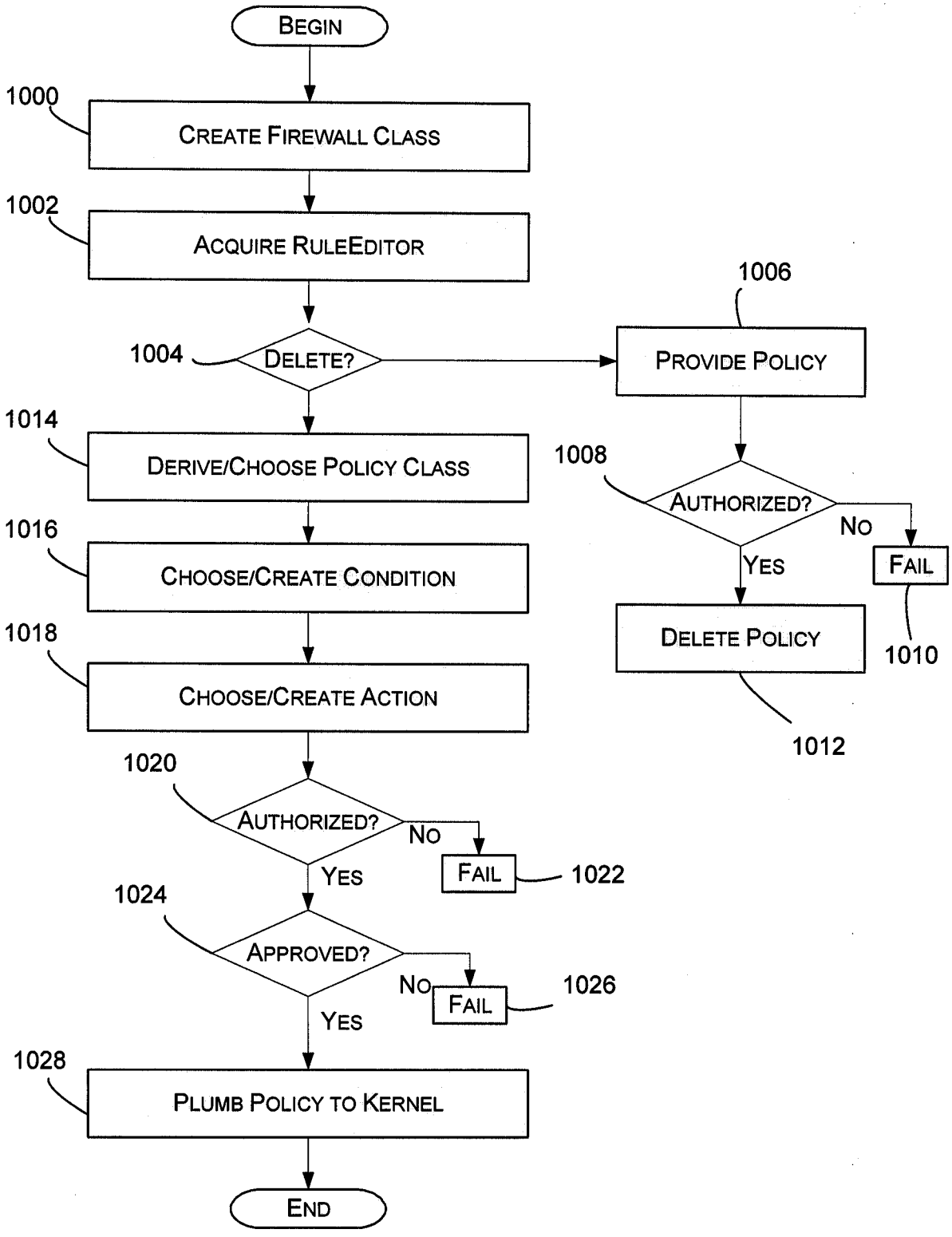

BEGIN
1000
CREATE FIREWALL CLASS
1002
ACQUIRE RULEEDITOR
1004
DELETE?
1006
PROVIDE POLICY
1008
AUTHORIZED?
NO
FAIL
1010
YES
DELETE POLICY
1012
1014
DERIVE/CHOOSE POLICY CLASS
1016
CHOOSE/CREATE CONDITION
1018
CHOOSE/CREATE ACTION
1020
AUTHORIZED?
NO
FAIL
1022
YES
1024
APPROVED?
NO
FAIL
1026
YES
1028
PLUMB POLICY TO KERNEL
END

FIG. 10

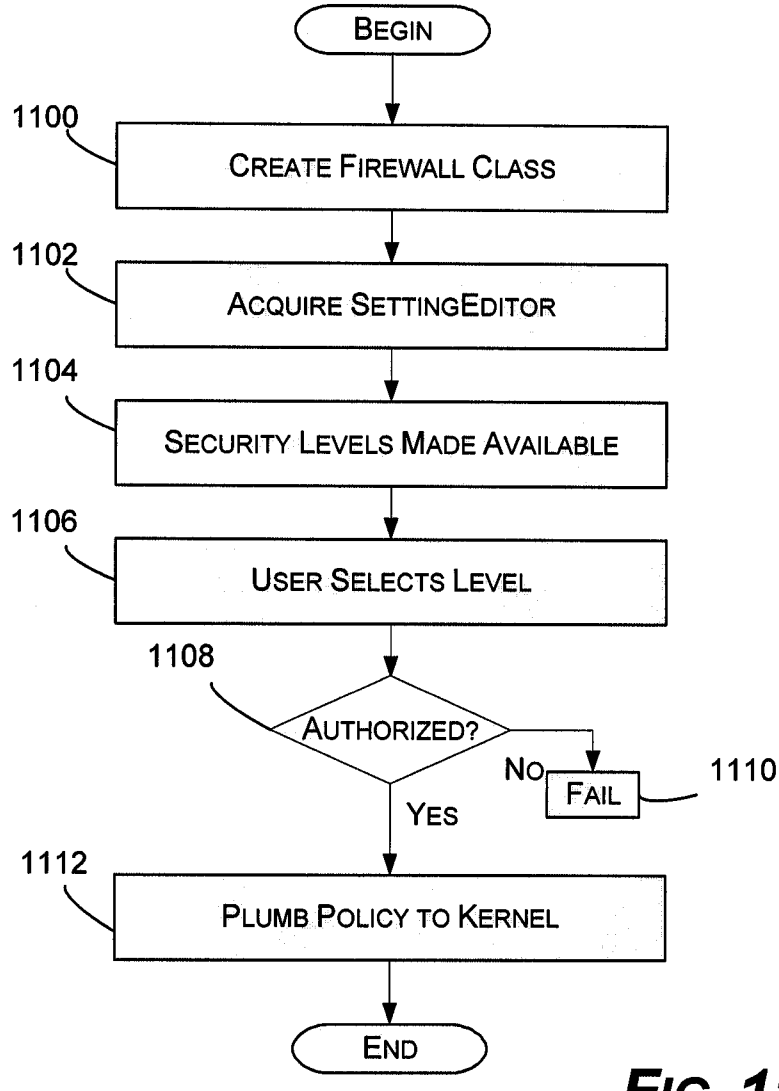

BEGIN
1100
CREATE FIREWALL CLASS
1102
ACQUIRE SETTINGEDITOR
1104
SECURITY LEVELS MADE AVAILABLE
1106
USER SELECTS LEVEL
1108
AUTHORIZED?
NO
FAIL
1110
YES
1112
PLUMB POLICY TO KERNEL
END

FIG. 11