Document Identifier: DSP1048

Date: 2021-02-26

Version: 1.0.0

Network Policy Management Profile

Supersedes: None

Document Class: Normative

Document Status: Published

Document Language: en-US

CONTENTS

Figures

Tables

Foreword

The *Network Policy Management* Profile (DSP1048) was prepared by the Network Services Management Working Group of the DMTF.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability.

Acknowledgments

The DMTF acknowledges the following individuals for their contributions to this document:

Editors:

- Alex Zhdankin – Cisco Systems

Contributors:

- John Crandall – Brocade Communications System
- Dr. Bhumip Khasnabish - ZTE Corporation
- Lawrence Lamers – VMware
- Steve Neely – Cisco Systems
- Shishir Pardikar – Citrix
- John Parchem – DMTF Fellow
- Hemal Shah – Broadcom Corporation
- Alex Zhdankin – Cisco Systems

Introduction

The information in this specification should be sufficient for a provider or consumer of this data to identify unambiguously the classes, properties, methods, and values that shall be instantiated and manipulated to represent and manage Network Services and the associated configuration information. The target audience for this specification is implementers who are writing CIM-based providers or consumers of management interfaces that represent the component described in this document.

Document conventions

Typographical conventions

The following typographical conventions are used in this document:

- Document titles are marked in *italics*.
- ABNF rules are in `monospaced font`.

Network Policy Management Profile

1 Scope

The *Network Policy Management Profile* is a base (abstract) profile that will specify the CIM Schema and use cases associated with the general and common aspects of Network Policy Management. This profile includes a specification of the Network Policy Service, Network Policy, Network Policy Rule and Setting Data, Policy Conditions and Action and describes how the network Policies can be applied to the Managed Elements.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated or versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies. For references without a date or version, the latest published edition of the referenced document (including any corrigenda or DMTF update versions) applies.

DMTF DSP0004, *CIM Infrastructure Specification 2.7*,
http://www.dmtf.org/standards/published_documents/DSP0004_2.7.pdf

DMTF DSP0200, *CIM Operations over HTTP 1.3,*
http://www.dmtf.org/standards/published_documents/DSP0200_1.3.pdf

DMTF DSP0223, *Generic Operations 1.0*,
http://www.dmtf.org/standards/published_documents/DSP0223_1.0.pdf

DMTF DSP1001, *Management Profile Specification Usage Guide 1.0*,
http://www.dmtf.org/standards/published_documents/DSP1001_1.0.pdf

DMTF DSP1033, *Profile Registration Profile 1.0,*
http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf

ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*,
http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype

3 Terms and definitions

In this document, some terms have a specific meaning beyond the normal English meaning. Those terms are defined in this clause.

The terms "shall" ("required"), "shall not", "should" ("recommended"), "should not" ("not recommended"), "may," "need not" ("not required"), "can" and "cannot" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 7. The terms in parenthesis are alternatives for the preceding term, for use in exceptional cases when the preceding term cannot be used for linguistic reasons. Note that ISO/IEC Directives, Part 2, Clause 7 specifies additional alternatives. Occurrences of such additional alternatives shall be interpreted in their normal English meaning.

The terms "clause", "subclause", "paragraph", and "annex" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 6.

The terms "normative" and "informative" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 3. In this document, clauses, subclauses, or annexes labeled "(informative)" do not contain normative content. Notes and examples are always informative elements.

The terms defined in DSP0004, DSP0223, and DSP1001 apply to this document. The following additional terms are used in this document.

3.1
conditional

indicates requirements to be followed strictly to conform to the document when the specified conditions are met

3.2
mandatory

indicates requirements to be followed strictly to conform to the document and from which no deviation is permitted

3.3
optional

indicates a course of action permissible within the limits of the document

3.4
pending configuration

indicates the configuration that will be applied to an IP network connection the next time the IP network connection accepts a configuration

3.5
referencing profile

indicates a profile that owns the definition of this class and can include a reference to this profile in its "Referenced Profiles" table

3.6
unspecified

indicates that this profile does not define any constraints for the referenced CIM element or operation

4 Symbols and abbreviated terms

The abbreviations defined in DSP0004, DSP0223, and DSP1001 apply to this document. The following additional abbreviations are used in this document.

4.1
IP

Internet Protocol

4.2
VLAN

Virtual Local Area Network

5 Synopsis

Profile name: Network Policy Management

Version: 1.0.0

Organization: DMTF

CIM Schema version: 2.43

Central class: CIM_NetworkPolicyService

Scoping class: CIM_System

The *Network Policy Management Profile* is a base profile that specifies the CIM Schema and use cases associated with the general and common aspects of Network Policy Management. The Network Policy Management Profile is an adaptation of the CIM Policy Management Profile.

Table 1 identifies profiles on which this profile has a dependency.

Table 1 – Referenced profiles

Profile Name	Organization	Version	Requirement	Description
Profile Registration	DMTF	1.0	Mandatory	None
Network Management Profile	DMTF	1.0	Optional	None
Policy Profile	DMTF	1.0	Mandatory	None

6 Description

The *Network Policy Management Profile* includes base specification of the Network Policy Management Service, Network Policy, Network Policy Rule and Setting Data, and Policy Conditions and Action. This standard describes how a Network Policy is applied to the Managed Elements and contains three possible extensions representing QoS, Firewall, and Load Balancer policies. Other types of policies, for example Access Control List (ACL) or routing policies, may be represented in a similar manner.

6.1 Class diagram

Figure 1 represents the class schema for the *Network Policy Management Profile*. For simplicity, the CIM_ prefix has been removed from the names of the classes.

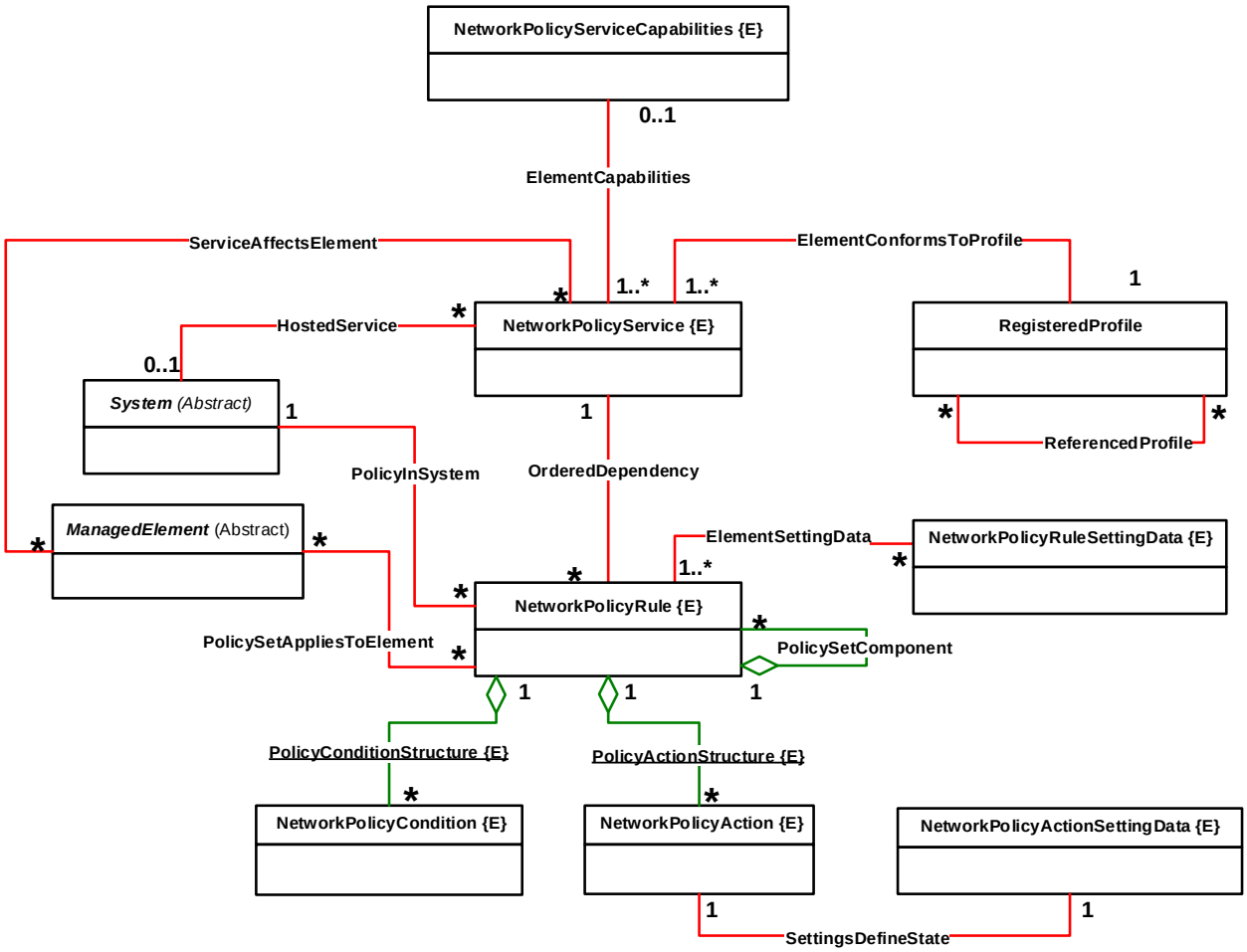


Figure 1 – Network Policy Management Profile: Class diagram

Network Policy model is an extension of the existing CIM Policy model, where the CIM_NetworkPolicyRule extends the CIM_PolicyRule class, and CIM_NetworkPolicyCondition and CIM_NetworkPolicyAction extend CIM_Policy. CIM_NetworkPolicyService extends the CIM_Service class and provides policy management capabilities.

The Network Policy Service is hosted on a System (for example an instance of the Computer System representing a network appliance, device or a network management system/controller) and serves as a management gateway through which the instances of CIM_NetworkPolicyRule are created, configured, and applied to the instances of CIM_ManagedElement subclasses, for example, CIM_Network, CIM_ProtocolEndpoint, subclasses of CIM_Service (e.g., for configuration of the routing policies), etc.

The CIM_NetworkPolicyRule may be subclassed to represent different types of network policies, for example CIM_QoSPolicyRule or CIM_LoadBalancingPolicyRule.

There is a set of Network Policy Conditions that can be associated with the particular Network Policy Rule. These conditions determine when the particular policy will be invoked. The conditions can be evaluated in the specified order (see the definition of the CIM_PolicyConditionStructure association for

how the condition evaluation order is specified). The set of the CIM_NetworkPolicyAction instances associated with the Network Policy via the CIM_PolicyActionStructure determines the actions that will be executed once the policy is triggered.

The Network Policy Rule and Network Policy Action are configured via the instances of CIM_NetworkPolicyRuleSettingData and CIM_NetworkPolicyActionSettingData classes or subclasses thereof.

The CIM_NetworkPolicyRuleSettingData may be subclassed to represent the settings of the policies extending Network Policy Management Profile, for example CIM_QoSRuleSettingData or CIM_LoadBalancingRuleSettingData.

The CIM_NetworkPolicyActionSettingData may be subclassed to represent the settings of the policies extending Network Policy Management Profile, for example CIM_LoadBalancingActionSettingData.

The CIM_NetworkPolicyServiceCapabilities class describes the capabilities offered by the Network Policy Management Service. The CIM_RegisteredProfile provides the information about the Policy Management Profile registration.

7 Implementation

This clause details the requirements related to the arrangement of instances and properties of instances for implementations of this profile.

7.1 Representing the policy management capabilities

7.1.1 CIM_NetworkPolicyService

The instance of the CIM_NetworkPolicyService class serves as a management endpoint through which the instances of CIM_NetworkPolicyRule shall be created, configured, and applied to the managed elements. Zero or more instances of CIM_NetworkPolicyService shall be instantiated.

The instances of the CIM_NetworkPolicyService shall be associated with the instance of the scoping CIM_System through an instance of CIM_HostedService association.

7.1.2 CIM_NetworkPolicyServiceCapabilities

The CIM_NetworkPolicyServiceCapabilities class represents the capabilities offered by the CIM_NetworkPolicyService. There shall be at most one instance of the CIM_NetworkPolicyServiceCapabilities class associated with at least one or more instances of CIM_NetworkPolicyService.

7.2 Representing the Network Policy

7.2.1 CIM_NetworkPolicyRule

The CIM_NetworkPolicyRule class extends the CIM_PolicyRule and represents the Network Policy that is instantiated, configured, and applied to the various managed elements. The CIM_NetworkPolicyRule instance shall be associated with the scoping CIM_System through an instance of CIM_PolicyInSystem association. The instance of the CIM_NetworkPolicyRule shall be associated with one instance of the scoping CIM_System.

A CIM_NetworkPolicyRule instance that is applied to an instance of CIM_ManagedElement shall be associated with the CIM_ManagedElement instance through an instance of CIM_PolicySetAppliesToElement association.

7.2.2 CIM_NetworkPolicyCondition

The CIM_NetworkPolicyCondition extends the CIM_Policy class and specifies a particular condition, which causes the associated network policy to be triggered once met. Each CIM_NetworkPolicyCondition instance shall be associated with one instance of the CIM_NetworkPolicyRule through the instance of CIM_PolicyConditionStructure association.

7.2.3 CIM_NetworkPolicyAction

The CIM_NetworkPolicyAction class extends the CIM_Policy class and determines an action taken once the policy is triggered. Each CIM_NetworkPolicyAction instance shall be associated with one instance of the CIM_NetworkPolicyRule through the CIM_PolicyActionStructure association instance.

7.3 Network Policy configuration

7.3.1 CIM_NetworkPolicyRuleSettingData

The CIM_NetworkPolicyRuleSettingData class extends the CIM_SettingData class and specifies the setting data for the network policy.

An instance of the CIM_NetworkPolicyRuleSettingData shall be associated to the instance of CIM_NetworkPolicyRule through an instance of CIM_ElementSettingsData association.

7.3.1.1 CIM_QoSPolicyRuleSettingData

The CIM_QoSPolicyRuleSettingData class extends the CIM_NetworkPolicyRuleSettingData class and specifies the setting data for the QoS network policy.

7.3.1.2 CIM_FirewallRuleSettingData

The CIM_FirewallRuleSettingData class extends the CIM_NetworkPolicyRuleSettingData class and specifies the setting data for the QoS network policy.

7.3.1.3 CIM_LoadBalancingRuleSettingData

The CIM_LoadBalancingRuleSettingData class extends the CIM_NetworkPolicyRuleSettingData class and specifies the setting data for the load balancing network policy.

7.3.2 CIM_NetworkPolicyActionSettingData

CIM_NetworkPolicyActionSettingData class extends the CIM_NetworkPolicySettingData and specifies the setting data for the Network Policy Action.

An instance of the CIM_NetworkPolicyActionSettingData shall be associated to the instance of CIM_NetworkPolicyAction through an instance of CIM_SettingsDefineState association.

7.3.2.1 CIM_LoadBalancingActionSettingData

CIM_LoadBalancingActionSettingData class extends the CIM_NetworkPolicyActionSettingData and specifies the setting data for the load balancing network policy action.

8 Methods

This clause details the requirements for supporting intrinsic operations and extrinsic methods for the CIM elements defined by this profile.

8.1 Extrinsic methods

If synchronous execution of a method succeeds, the implementation shall set a return value of 0 (Completed with No Error).

If synchronous execution of a method fails, the implementation shall set a return value of 2 (Failed) or a more specific return code as specified with the respective method.

If a method is executed as an asynchronous task, the implementation shall perform all of the following actions:

- Create a Job object according to DSP1103 Job Control Profile.
- Set a return value of 4096 (Job Started).

8.1.1 Job parameter

The implementation shall set the value of the Job parameter as a result of an asynchronous execution of a method of the CIM_NetworkPolicyService as follows:

- If the method execution is performed synchronously, the implementation shall set the value to NULL.
- If the method execution is performed asynchronously, the implementation shall set the value to refer to the instance of the CIM_ConcreteJob class that represents the asynchronous task.

8.1.2 CIM_NetworkPolicyService.CreatePolicyRule()

The implementation of the CreatePolicyRules( ) method is required; the provisions in this subclause apply in addition to behavior applicable to all extrinsic methods as specified in **Error! Reference source not found.**.

This method creates instances of CIM_NetworkPolicyRule class, CIM_NetworkPolicyCondition, CIM_NetworkPolicyAction, CIM_NetworkPolicyRuleSettingData, and CIM_NetworkPolicyActionSettingData classes and all mandatory associations between these instances as described in clause 7.

Profile implementation should make sure that the types of the policy actions, network policy rule setting data, and network policy action setting data match to represent a configuration of the particular policy type, for example load balancing or firewall policy.

Input: NetworkPolicyAction[], ActionsOrder[] (uint16) (optional), NetworkPolicyCondition[], ConditionGroupNumber[] (uint16), NetworkPolicyRuleSettingData[], NetworkPolicyActionSettingData[], SequenceNumber, NetworkPolicyRule, REF ParentNetworkPolicyRule (optional), REF ManagedElement[] (optional)

Output: REF to NetworkPolicyRule

8.1.3 CIM_NetworkPolicyService.DeletePolicyRules( )

The implementation of the DeletePolicyRules( ) method is required; the provisions in this subclause apply in addition to behavior applicable to all extrinsic methods as specified in 8.1.

This method removes all associated instances of CIM_NetworkPolicyAction, CIM_NetworkPolicyCondition, CIM_NetworkPolicyRuleSettingData, and CIM_NetworkPolicyActionSettingData that are only associated with the rule specified in this method input parameter.

The requested CIM_NetworkPolicyRule instances shall be associated with this network policy service in order for them to be removed

Input: REF NetworkPolicyRule[]

8.1.4 CIM_NetworkPolicyService.ApplyPolicyRule( ) (optional)

The implementation of the ApplyPolicyRules( ) method is optional; the provisions in this subclause apply in addition to behavior applicable to all extrinsic methods as specified in 8.1.

Applies the Network Policy Rule to the specified instances of the CIM_ManagedElement. This method creates the instances of the CIM_PolicySetAppliesToElement association between the specified instance of the CIM_NetworkPolicyRule and the instances of CIM_ManagedElement subclasses, which references are supplied.

Input: REF NetworkPolicyRule, REF ManagedElement[]

8.1.5 CIM_NetworkPolicyService.ReleasePolicyRule( ) (optional)

The implementation of the ReleasePolicyRules( ) method is optional; the provisions in this subclause apply in addition to behavior applicable to all extrinsic methods as specified in 8.1.

Removes the Network Policy Rule from the ManagedElement instances it was applied before. This method deletes the instances of the CIM_PolicySetAppliesToElement association between the specified instance of the CIM_NetworkPolicyRule and the instances of CIM_ManagedElement subclasses, which references are supplied.

Input: REF NetworkPolicyRule, REF ManagedElement[]

8.2 Profile conventions for operations

For each profile class (including associations), the implementation requirements for operations, including those in the following default list, are specified in class-specific subclauses of this clause.

The default list of operations is as follows:

- GetInstance
- EnumerateInstances
- EnumerateInstanceNames
- Associators
- AssociatorNames
- References
- ReferenceNames

8.3 CIM_NetworkPolicyService

All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

8.4 CIM_NetworkPolicyServiceCapabilities

All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

8.5 CIM_NetworkPolicyRule

All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

8.6 CIM_NetworkPolicyCondition

386 All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

387 8.7 CIM_NetworkPolicyAction

388 All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

389 8.8 CIM_NetworkPolicyRuleSettinigData

390 All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

391 8.9 CIM_NetworkPolicyActionSettingData

392 All operations in the default list in 8.1 shall be implemented as defined in DSP0200.

9 Use cases

This clause contains object diagrams and use cases for the *Network Policy Management Profile*.

9.1 Profile registration

The object diagram in Figure 2 shows one possible method for advertising profile conformance.

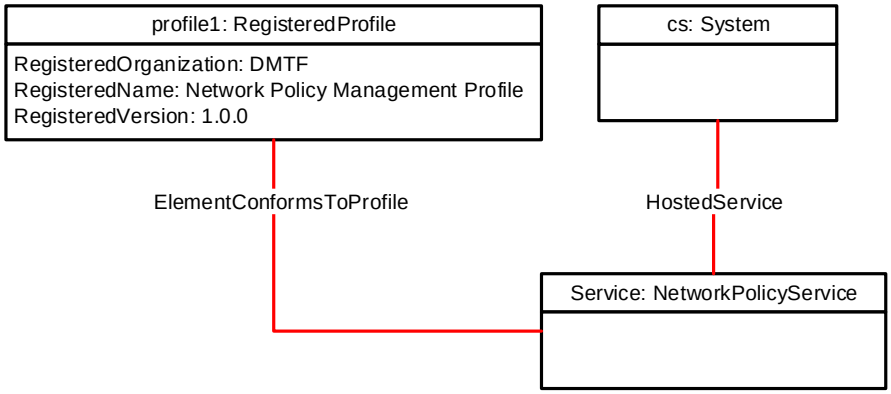


Figure 2 – Registered profile

9.2 Profile extension and usage examples

9.2.1 Extending and using the Network Policy Management Profile

The *Network Policy Management Profile* is a base profile that specifies the CIM Schema and use cases associated with the general and common aspects of Network Policy Management. This profile is intended to be extended to represent various kinds of network policies, such as Load Balancing, Firewall, QoS, Routing, etc.

The extension is generally performed by subclassing CIM_NetworkPolicyRuleSettingData to represent the settings specific to the particular type of Network Policy, for example Load Balancer by introducing CIM_LoadBalancingRuleSettingData and by subclassing CIM_NetworkPolicyActionSettingData if the particular type of actions require specific configuration parameters, for example by introducing CIM_LoadBalancingActionSettingData to specify the action settings for the load balancing actions.

The class diagram on Figure 3 represents the Policy Rule and Action extensions for the Load Balancer, Firewall, and QoS specific Network Policies.

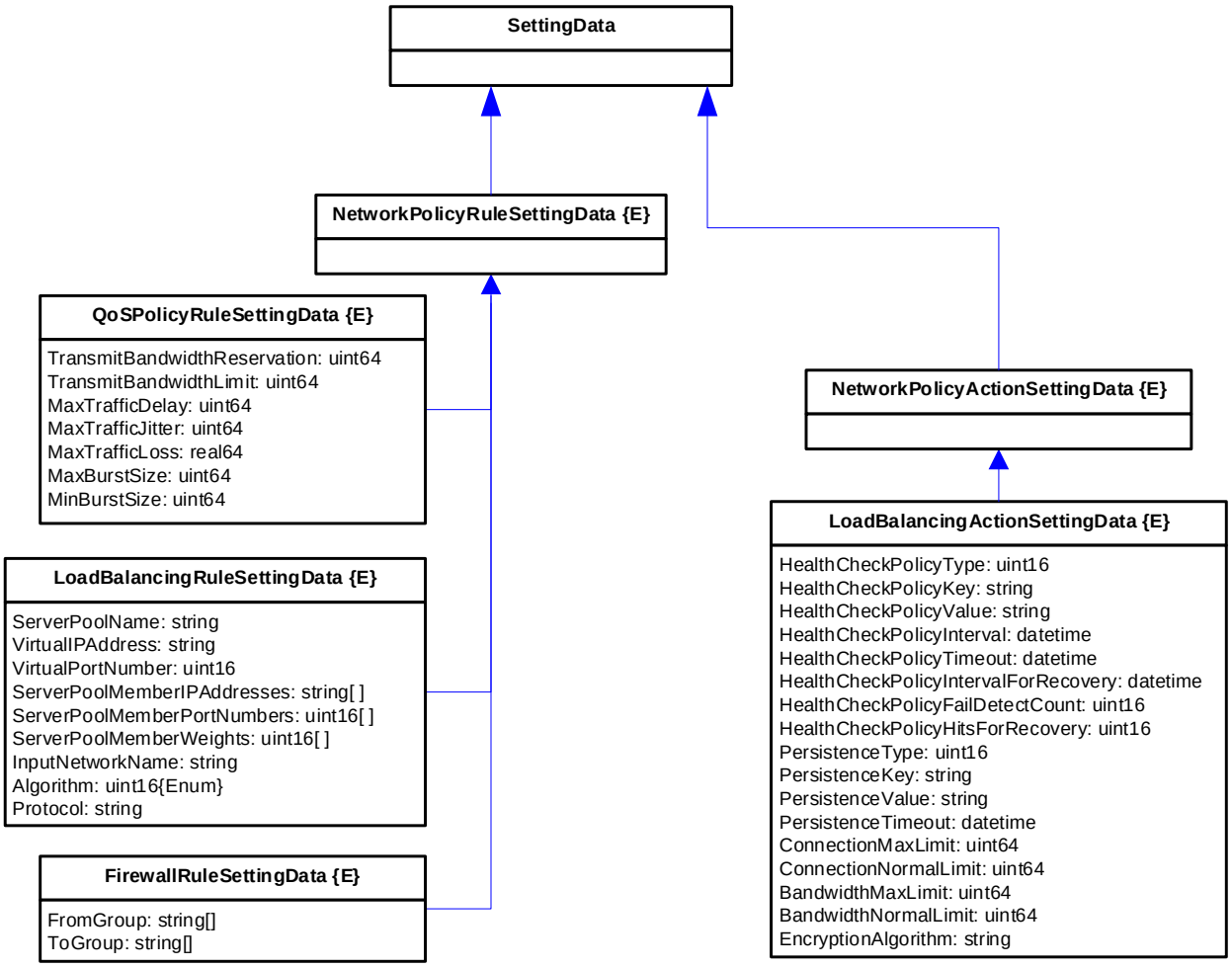
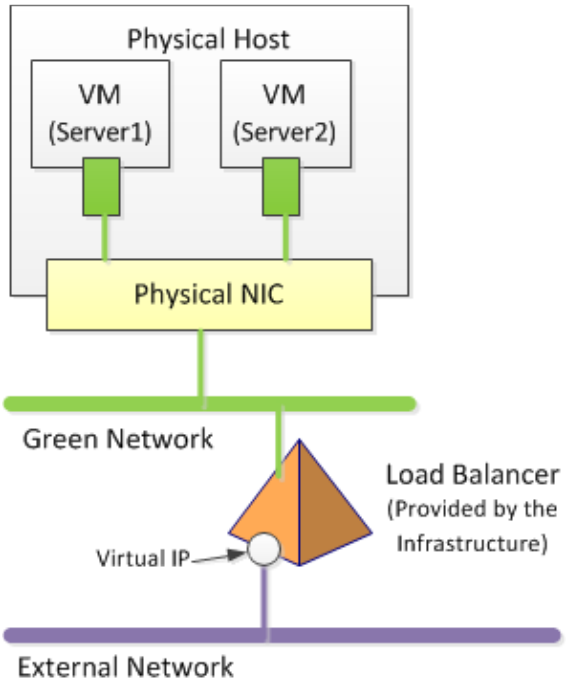


Figure 3 – Network Management Policy extensions

9.2.2 Load Balancer configuration

Figure 4 illustrates one of the possible load balancing scenarios. In this case the Load Balancer needs to redirect the IP traffic, coming from the external network to one of the Virtual Machines (VM), hosted by the same Physical Host. The VMs are connected to the internal network and their IP addresses can be resolved via NAT.

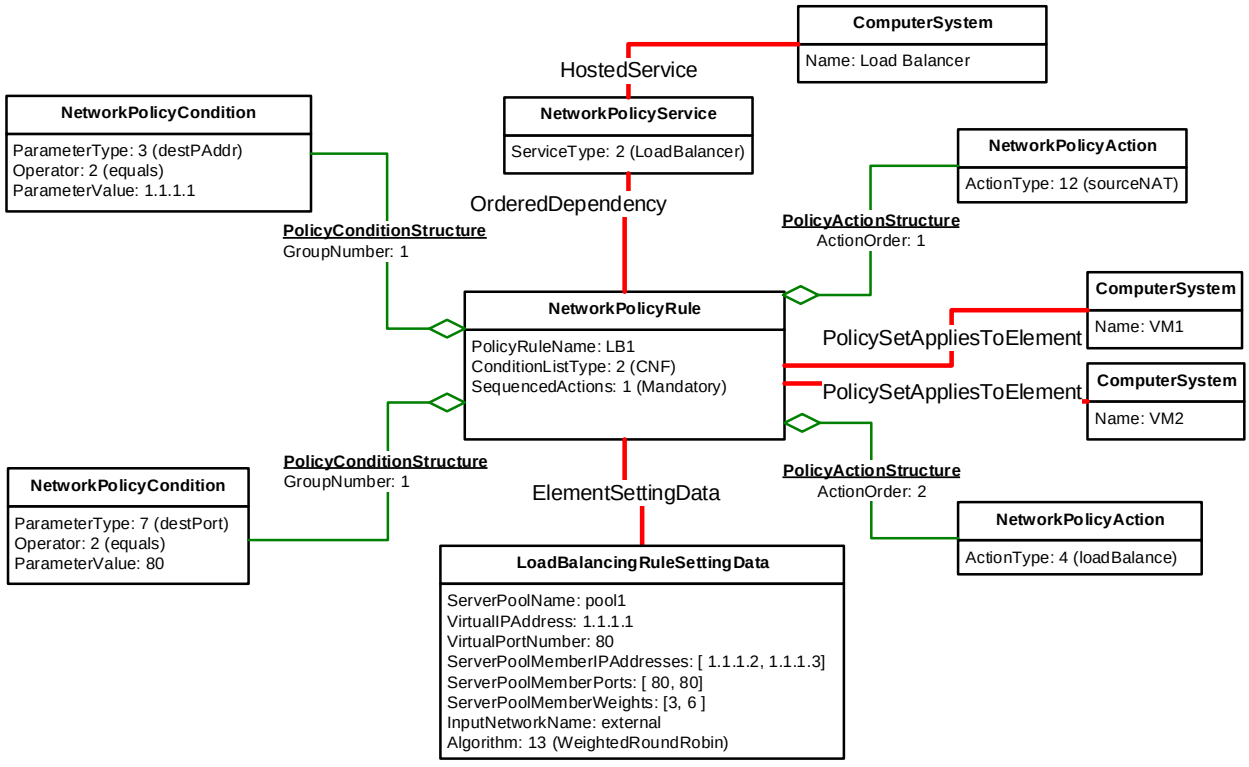
The IP traffic that needs to be load balanced is coming to port 80 and the load balancing needs to be performed using Round Robin algorithm, where each VM can be assigned its own weight. In this example VM1 has been assigned weight equal to 6 and VM2 has been assigned weight equal to 3.



Parameter	Configuration Value
Algorithm	RoundRobin
Virtual Port	80
VM1 Destination Port	80
VM2 Destination Port	80
VM1 weight	6
VM2 weight	3
NetworkPolicyActions	Source NAT
	Load balance

422

423 **Figure 4 – Example load balancing scenario**



424

425 **Figure 5 – Example load balancing configuration using Network Policy**

426 Figure 5 shows how such load balancing configuration can be modeled using Network Policy model. As
427 per Network Policy model extension principles described earlier in clause 9.2.1, we are creating instances

of CIM_LoadBalancingRuleSettingData classes to capture the specific configuration parameters of the load balancer, such as VM weights, load balancing algorithm, and VM destination ports.

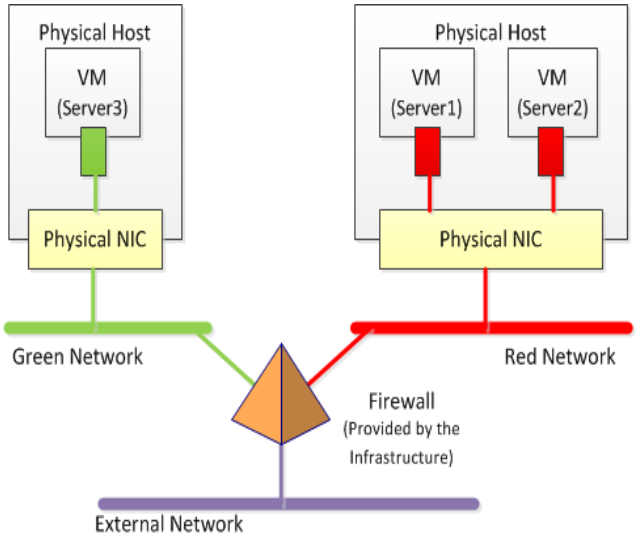
In the case of the Round Robin load balancing algorithm, there is no need to create the additional instances of the CIM_LoadBalancingActionSettingData class.

The instances of CIM_NetworkPolicyCondition classes capture some of the configuration parameters, notably the destination ports for incoming IP traffic.

9.2.3 Firewall configuration

Another example of extending and using the Network Policy Management profile is configuration of firewalls. Consider the example firewall configuration scenario outlined on the Figure 6. Here we are configuring four network groups with the different rules permitting or denying traffic flow between them and the external network.

Each group can contain individual or several networks (e.g., Red Network or Green Network) or can be a collection of virtual machines or servers in the particular network (e.g., Server 1 in Red Network).



Group Name	Description
Group1	Red Network
Group2	Green Network
Group3	Server1 in red Network
Group4	External Network

Firewall Rules		
From	To	Description
Group2	Group1	Allow HTTP
Group4	Group1	Allow SSH from a concrete IP
Group1	Group2	Allow HTTP
Group2	Group3	Allow HTTPS

Figure 6 – Example firewall configuration scenario

The Firewall Rules table in Figure 6 describes the traffic flow rules between various groups used in this example.

Figure 7 illustrates how the firewall rules described earlier can be modeled using Network Policy model.

In this case we are using instances of CIM_FirewallRuleSettingData to specify some of the firewall configuration data, such as the names of the Groups for which the particular policy instance is configured.

The instances of CIM_NetworkPolicyCondition class specify the traffic characteristics (e.g., source IP address and port number) that are used to trigger the particular policy (represented as an instance of CIM_NetworkPolicyRule), which controls the traffic flow in the system.

The only type of action used by this model is the Permit action (represented via the instance of CIM_NetworkPolicyAction class with the actionType property set to ‘permit’), which indicates that the particular policy permits the flow of traffic between the groups once the matching conditions trigger the execution of the particular policy instance.

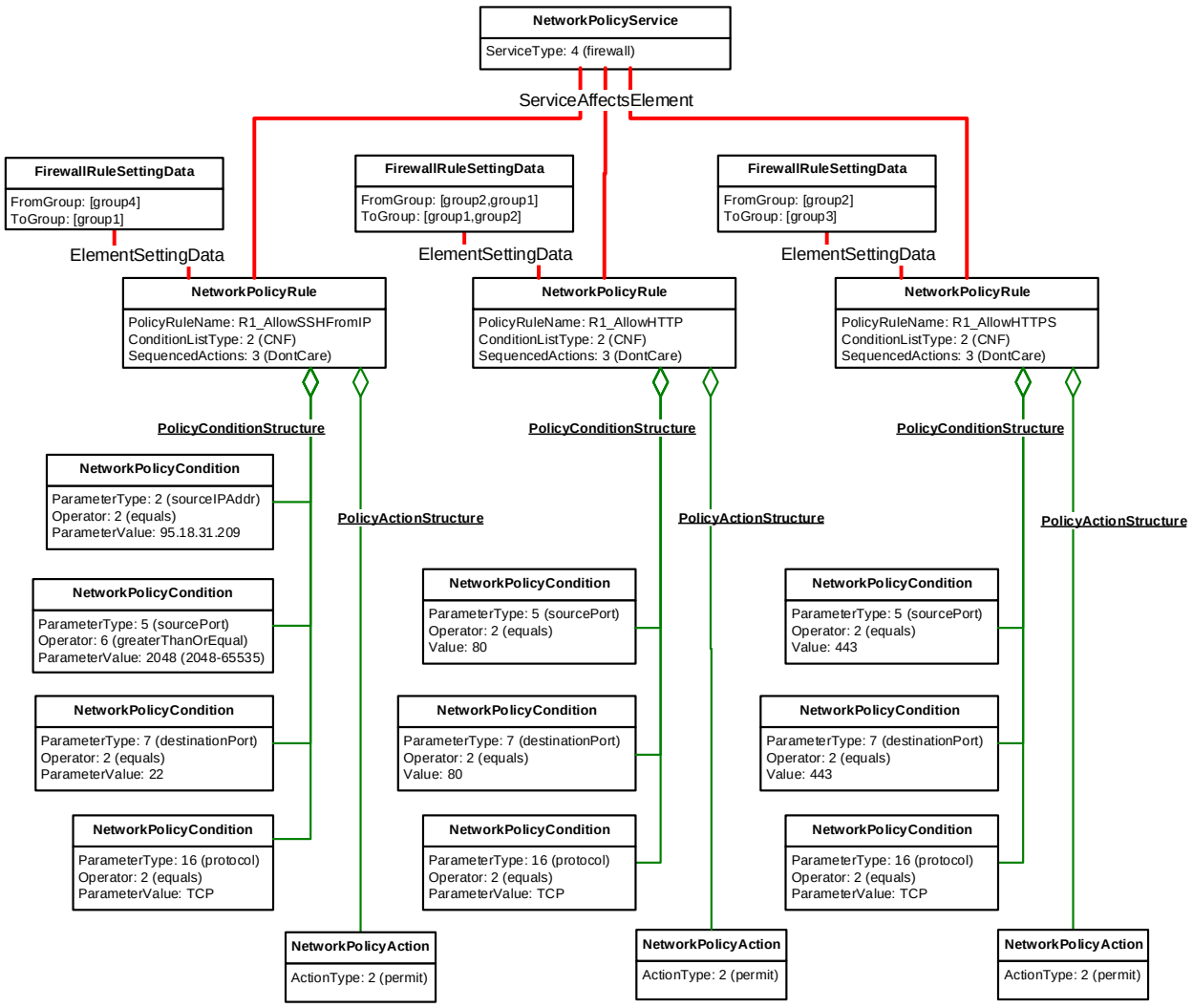


Figure 7 – Example firewall configuration scenario using Network Policy

9.2.4 QoS Service configuration

Figure 8 shows the example Quality of Service (QoS) configurations. Here we have three classes of service – Gold, Bronze, and Silver, each with different traffic characteristics, such as maximum allowed bandwidth, maximum delay, jitter, and others.

These QoS characteristics can be applied to the traffic, generated by the particular applications, for example between SIP clients and server, MySQL applications deployed in Tomcat, etc.

The purpose of the QoS policies is to control the use of the network resources according to selected class of service.

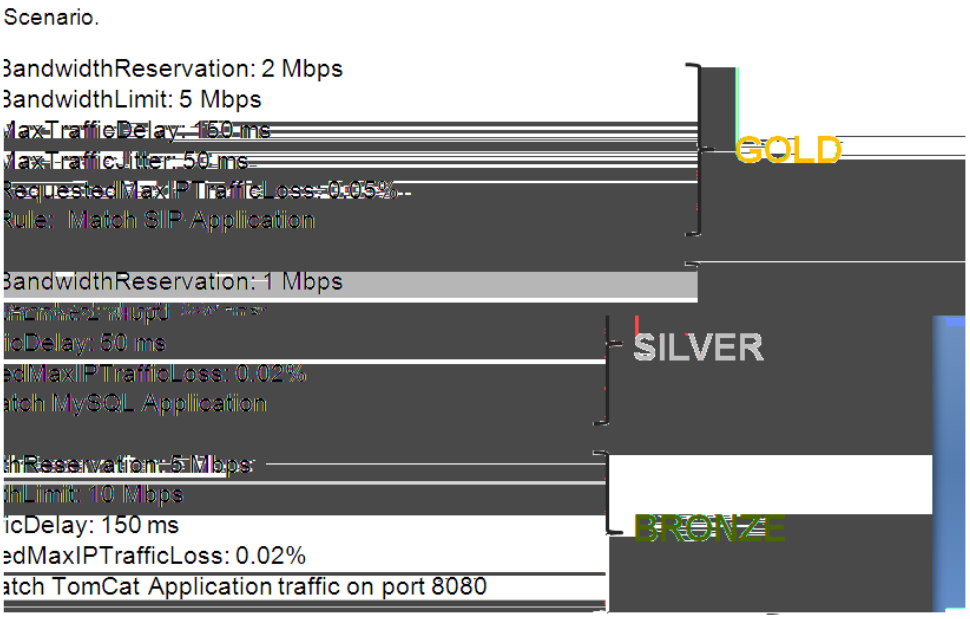


Figure 8 – Example QoS Service configuration

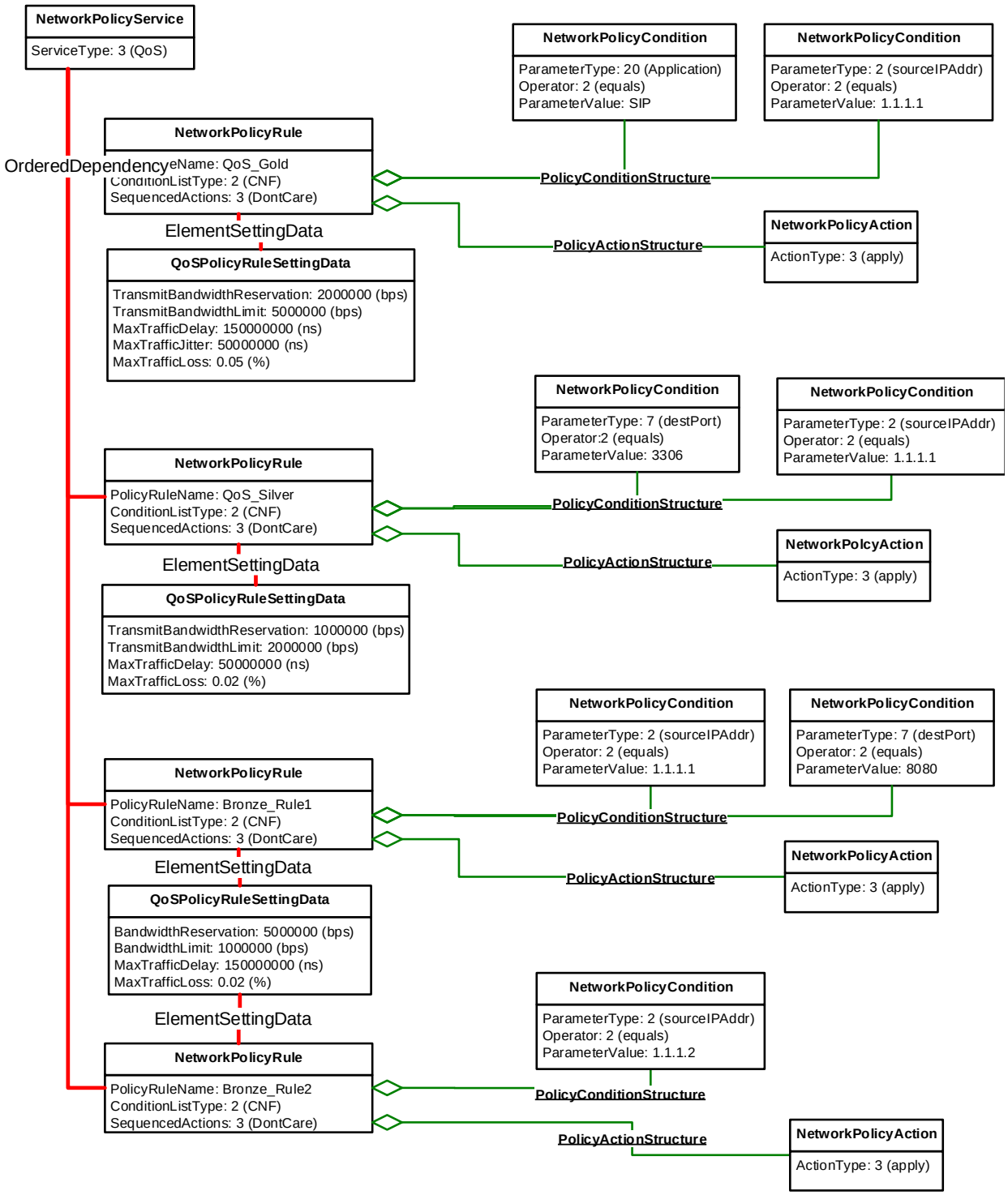


Figure 9 - Example QoS Service configuration

Figure 9 illustrates how various QoS policies can be configured using Network Policy Management Profile.

10 CIM Elements

Table 2 shows the instances of CIM Elements for this profile. Instances of the CIM Elements shall be implemented as described in Table 2. Clauses 7 (“Implementation”) and 8 (“Methods”) may impose additional requirements on these elements.

Table 2 – CIM Elements: Network Policy Management Profile

Element Name	Requirement	Description
Classes		
CIM_NetworkPolicyService	Required	See clauses 7.1.1
CIM_NetworkPolicyRule	Optional	See clauses 7.2.1
CIM_NetworkPolicyCondition	Optional	See clauses 7.2.2
CIM_NetworkPolicyAction	Optional	See clauses 7.2.3
CIM_NetworkPolicyRuleSettingData	Optional	See clauses 7.3.1
CIM_NetworkPolicyActionSettingData	Optional	See clauses 7.3.2
CIM_NetworkPolicyServiceCapabilities	Optional	See clauses 7.1.2
Association and endpoints		
Indications		
None defined in this profile		

ANNEX A
(informative)

Change log

Version	Date	Description
1.0.0	2021-02-26	