Network Working Group
Request for Comments: 3304
Category: Informational

R. P. Swale
BTexact Technologies
P. A. Mart
Marconi Communications
P. Sijben
Lucent Technologies
S. Brim
M. Shore
Cisco Systems

August 2002

Middlebox Communications (midcom) Protocol Requirements

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document specifies the requirements that the Middlebox Communication (midcom) protocol must satisfy in order to meet the needs of applications wishing to influence the middlebox function. These requirements were developed with a specific focus on network address translation and firewall middleboxes.

1. Introduction

This document is one of two developed by the Middlebox Communication (midcom) working group to address the requirements and framework for a protocol between middleboxes and "midcom agents." This document presents midcom requirements; [MCFW] presents the context and framework. [MCFW] also presents terminology and definitions and should be read in tandem with this one.

These requirements were developed by examining the midcom framework and extracting requirements, both explicit and implicit, that appeared there.

2. Requirements

Each requirement is presented as a statement, followed by brief explanatory material as appropriate. Terminology is defined in [MCFW]. There may be overlap between requirements.

2.1. Protocol machinery

2.1.1.

The Midcom protocol must enable a Midcom agent requiring the services of a middlebox to establish an authorized association between itself and the middlebox.

This states that the protocol must allow the middlebox to identify an agent requesting services and make a determination as to whether or not the agent will be permitted to do so.

2.1.2.

The Midcom protocol must allow a Midcom agent to communicate with more than one middlebox simultaneously.

In any but the most simple network, an agent is likely to want to influence the behavior of more than one middlebox. The protocol design must not preclude the ability to do this.

2.1.3.

The Midcom protocol must allow a middlebox to communicate with more than one Midcom agent simultaneously.

There may be multiple instances of a single application or multiple applications desiring service from a single middlebox, and different agents may represent them. The protocol design must not preclude the ability to do so.

2.1.4.

Where a multiplicity of Midcom Agents are interacting with a given middlebox, the Midcom protocol must provide mechanisms ensuring that the overall behavior is deterministic.

This states that the protocol must include mechanisms for avoiding race conditions or other situations in which the requests of one agent may influence the results of the requests of other agents in an unpredictable manner.

2.1.5.

The Midcom protocol must enable the middlebox and any associated Midcom agents to establish a known and stable state. This must include the case of power failure, or other failure, where the protocol must ensure that any resources used by a failed element can be released.

This states that the protocol must provide clear identification for requests and results and that protocol operations must be atomic with respect to the midcom protocol.

2.1.6.

The middlebox must be able to report its status to a Midcom agent with which it is associated.

2.1.7.

The protocol must support unsolicited messages from middlebox to agent, for reporting conditions detected asynchronously at the middlebox.

It may be the case that exceptional conditions or other events at the middlebox (resource shortages, intrusion mitigation) will cause the middlebox to close pinholes or release resources without consulting the associated Midcom agent. In that event, the protocol must allow the middlebox to notify the agent.

2.1.8.

The Midcom protocol must provide for the mutual authentication of Midcom agent and middlebox to one another.

In addition for the more obvious need for the Midcom agent to authenticate itself to the middlebox, there are some attacks against the protocol which can be mitigated by having the middlebox authenticate to the agent. See [MCFW].

2.1.9.

The Midcom protocol must allow either the Midcom agent or the middlebox to terminate the Midcom session between a Midcom Agent and a middlebox. This allows either entity to close the session for maintenance, security, or other reasons.

2.1.10.

A Midcom agent must be able to determine whether or not a request was successful.

This states that a middlebox must return a success or failure indication to a request made by an agent.

2.1.11.

The Midcom protocol must contain version interworking capabilities to enable subsequent extensions to support different types of middlebox and future requirements of applications not considered at this stage.

We assume that there will be later revisions of this protocol. The initial version will focus on communication with firewalls and NATs, and it is possible that the protocol will need to be modified, as support for other middlebox types is added. These version interworking capabilities may include (but are not limited to) a protocol version number.

2.1.12.

It must be possible to deterministically predict the behavior of the middlebox in the presence of overlapping rules.

The protocol must preclude nondeterministic behavior in the case of overlapping rulesets, e.g. by ensuring that some known precedence is imposed.

2.2. Midcom Protocol Semantics

2.2.1.

The syntax and semantics of the Midcom protocol must be extensible to allow the requirements of future applications to be adopted.

This is related to, but different from, the requirement for versioning support. As support for additional middlebox types is added there may be a need to add new message types.

2.2.2.

The Midcom protocol must support the ability of an agent to install a ruleset that governs multiple types of middlebox actions (e.g. firewall and NAT).

This states that a the protocol must support rules and actions for a variety of types of middleboxes. A Midcom agent ought to be able to have a single Midcom session with a middlebox and use the Midcom interface on the middlebox to interface with different middlebox functions on the same middlebox interface.

2.2.3.

The protocol must support the concept of a ruleset group comprising a multiple of individual rulesets to be treated as an aggregate.

Applications using more than one data stream may find it more convenient and more efficient to be able to use single messages to tear down, extend, and manipulate all middlebox rulesets being used by one instance of the application.

2.2.4.

The protocol must allow the midcom agent to extend the lifetime of an existing ruleset that otherwise would be deleted by the middlebox.

2.2.5.

If a peer does not understand an option, it must be clear whether the action required is to proceed without the unknown attribute being taken into account or the request is to be rejected. Where attributes may be ignored if not understood, a means may be provided to inform the client about what has been ignored.

This states that failure modes must be robust, providing sufficient information for the agent or middlebox, to be able to accommodate the failure or to retry with a new option that is more likely to succeed.

2.2.6.

To enable management systems to interact with the Midcom environment, the protocol must include failure reasons that allow the Midcom Agent behavior to be modified as a result of the information contained in the reason. Failure reasons need to be chosen such that they do not make an attack on security easier.

2.2.7.

The Midcom protocol must not preclude multiple authorized agents from working on the same ruleset.

2.2.8.

The Midcom protocol must be able to carry filtering rules, including but not limited to the 5-tuple, from the midcom agent to the middlebox.

By "5-tuple", we refer to the standard <source address, source port, destination address, destination port, transport protocol> tuple. Other filtering elements may be carried, as well.

2.2.9.

When the middlebox performs a port mapping function, the protocol should allow the Midcom agent to request that the external port number have the same oddity as the internal port.

This requirement is to support RTP and RTCP [RFC1889] "oddity" requirements.

2.2.10.

When the middlebox performs a port mapping function, the protocol should allow the Midcom agent to request that a consecutive range of external port numbers be mapped to consecutive internal ports. This requirement is to support RTP and RTCP "sequence" requirements.

2.2.11.

It should be possible to define rulesets that contain a more specific filter spec than an overlapping ruleset. This should allow agents to request actions for the subset that contradict those of the overlapping set.

This should allow a Midcom agent to request to a Midcom server controlling a firewall function that a subset of the traffic that would be allowed by the overlapping ruleset be specifically disallowed.

2.3. General Security Requirements

2.3.1.

The Midcom protocol must provide for message authentication, confidentiality, and integrity.

2.3.2.

The Midcom protocol must allow for optional confidentiality protection of control messages. If provided, the mechanism should allow a choice in the algorithm to be used.

2.3.3.

The Midcom protocol must operate across un-trusted domains, between the Midcom agent and middlebox in a secure fashion.

2.3.4.

The Midcom protocol must define mechanisms to mitigate replay attacks on the control messages.

3. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use other technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

4. Security Considerations

The security requirements for a midcom protocol are discussed in section 2.3.

5. Normative References

[MCFW] Srisuresh, S., Kuthan, J., Rosenberg, J., Molitor, A. and A. Rayhan, "Middlebox communication architecture and framework", RFC 3303, Date.*

[RFC1889] Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January 1996.

6. Informative References

[RFC2026] Bradner, S. "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026. October 1996.

Authors' Addresses

Richard Swale
BTexact Technologies
Callisto House
Adastral Park
Ipswich United Kingdom
EMail: richard.swale@bt.com

Paul Sijben
Lucent Technologies EMEA BV
Huizen
Netherlands
EMail: paul.sijben@picopoint.com

Philip Mart
Marconi Communications Ltd.
Edge Lane
Liverpool
United Kingdom
EMail: philip.mart@marconi.com

Scott Brim
Cisco Systems
146 Honness Lane
Ithaca, NY 14850
EMail: sbrim@cisco.com

Melinda Shore
Cisco Systems
809 Hayts Road
Ithaca, NY 14850
EMail: mshore@cisco.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.