MidCom BoF
Internet Draft

Document: draft-tiphon-foglamps-01.txt

P.A. Mart
Marconi
Communications
P. Sijben
Lucent Technologies
R.P. Swale
BTexaCT
November 2000

Firewall Control Requirements

Status of this Memo

1. Abstract

This draft describes a set of requirements for a protocol between application level entities, acting as proxies, and packet processing and filtering devices that implement policies determined by the application. The packet filters apply header translation and police flow rates. These requirements are considered initially in the context of IP telephony but may be extended further.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

3. Introduction

The requirements in this memo arise from work in the ETSI TIPHON project. The requirements were generated in a context that allows the use of SIP, H.323 or other Multi-Media session control environments and are not intended to reflect the specific requirements of any system.

A more detailed set of background information for these requirements can be found in the document "Compilation of TIPHON contributions on the firewall problem"[3].

The problem to be solved by the protocol is the need to able to pass packets from one IP based network under the same administration (an Autonomous System, AS) to another, while imposing packet based flow control, as required by a session-based application (like IP telephony). It seems reasonable to assume that these Autonomous Systems protect their internal policies using firewalls.

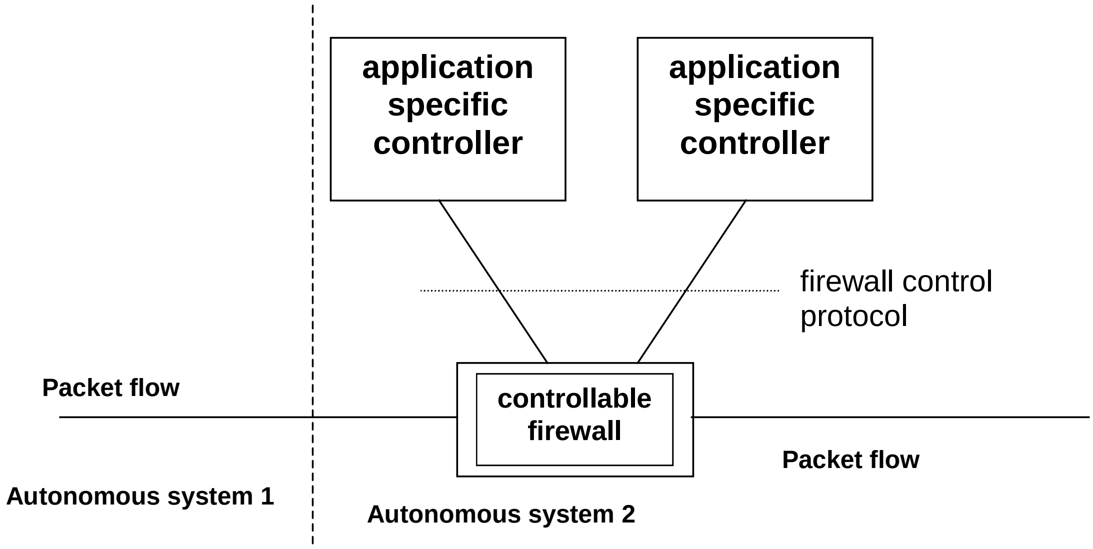
The application uses a session control protocol to communicate among its entities. This protocol is not terminated on the firewall device itself.

Each application needing packets to traverse between autonomous systems and hence the firewall should be able to request that flows be allowed or disallowed independently of other applications.

There is an underlying assumption that the firewalls may offer Network Address Translation and/or Port Address Translation for media flows.

4. Architecture

The architecture assumed for the rest of this paper is given below:



5. Requirements to be placed on the Firewall

Multiple Services

Multiple services need to be supported e.g. VoIP, FoIP, MMoIP.

This requirement extends to services which control flows and are not yet designed. This requirement is intended to provide a general-purpose mechanism for Applications to use in traversing NAT like devices.

QoS considerations

The firewall may provide QoS transport facilities for the packet flows. For example setting of DS-bytes, MPLS mappings or RSVP reservations.

QoS of Flows

On receipt of a request to allow a flow with a particular flow specification the firewall shall indicate whether or not available resources allow the flow to be carried.

QoS Flow Enforcement

Where the firewall has indicated that available resources allow a flow to be carried the firewall will enforce the flow specification contained in the original request.

QoS Flow Exceptions

The action to be taken when the flow specification is breached shall be determined on a flow by flow basis. The behaviour shall be a default set unless the firewall controller specifies a particular behaviour. The default behaviour is not to permit a flow of packets.

QoS Flow Measurements

It shall be possible to report the observed behaviour of a nominated flow.

Address Translation capabilities

The Address Translation behaviour intended is that IP addresses within the associated packet flows are not altered unless they appear in the packet header information.

Flow Topology

A particular flow may pass through one, two or more firewall devices connected in series. Address Translation is possible at any or all of the firewall devices. The firewall control devices may be different, but need not be different, for each firewall.

Allow Multiple Controllers

The firewall shall support multiple controllers. Each controller may be acting on behalf of one or more applications and no relationship between controllers may be assumed by the firewall.

Application Signalling

The firewall shall support the forwarding of signalling received to one, or more, appropriate destination address/port combinations to the appropriate controllers, e.g. a session control entity.

Packet denial

Other than the communication of control information between the controlled firewall device and the firewall controller, no packets will be allowed to flow across the firewall without prior instructions from the controller. i.e. the default will be "no packets allowed".

6. Requirements to be placed on the Firewall Controller

No assumption of Stand-alone implementation

The firewall controller shall be capable of implementation on the same platform as other functional entities e.g. a SIP proxy or H.323.Gatekeeper.

Physical separation from Firewall

The firewall controller and the firewall may be some distance apart or may be co-located.

Proxy capability

The firewall controller may act on behalf of other parties i.e. behave as a proxy device.

Protocol performance

The protocol must support time-constrained operation. This may include, amongst other things, the use of short messages and minimal messages per operation.

The protocol must not assume 0 (zero) delay in communication paths.

The protocol must be able to be used over low speed links.

7. Requirements to be placed on the Firewall Control Protocol

Unsolicited messages

The protocol needs to support unsolicited messages, for event reporting and alarms.

Normal Operations

An operation is needed to permit a flow, with a given flow specification and address translation, across the firewall. It shall be possible to indicate whether packets should be carried or discarded when a given flow specification is exceeded.

An operation is needed to stop a flow across the firewall.

An operation is needed to modify the address translation of an existing permitted flow.

8. Security Considerations

Security issues are covered in the following requirements:

Authentication

Peers using this protocol must be authenticated in order for message exchange to proceed.

Automatic discovery mechanisms shall not be permitted other than between mutually authenticated peers. This in order to prevent hacking into the firewall by impersonating a controller.

Encryption

The protocol must allow for strong encryption to be used to protect the privacy on requests and responses.

The protocol must allow for strong encryption to be used to protect the trustworthiness of the requests and responses. This in order to prevent hacking into the firewall by intercepting communication.

9. Example scenario

Figure 1 shows an example scenario showing two enterprise domains and a core domain. Each domain has its own network policies enforced by firewalls.

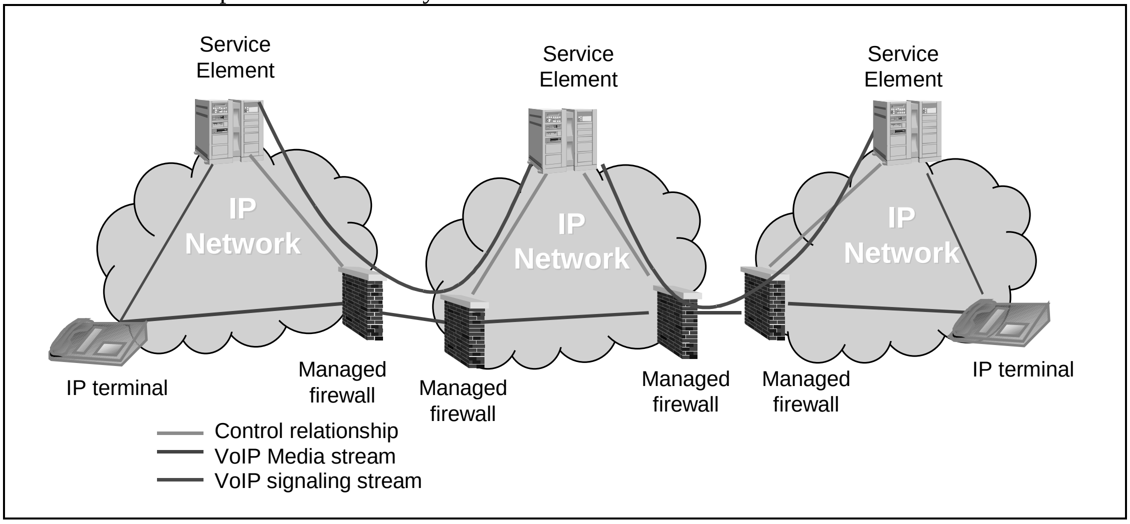


Figure 1. Example scenario

A user wishing to make a call from an IP terminal in the left-hand domain has its IP terminal contact its service element (Gatekeeper, SoftSwitch, SIP-proxy) and set up a call to the other user. The Service Element can be expected to have a signaling channel to the Service Element on the core network. When the call request arrives at the Service Element in the core network it can be relayed to the service element in the right-hand network. The service elements can inspect the parameters of the media streams that the terminals are trying to set up and hence can open the appropriate holes in the firewalls.

Information flows

TIPHON DTS02009 [4] describes flows across the reference points. We believe that the flows TIPHON defines at reference point I3 provide adequate implementation of the requirements. The primitives involved are shown below:

Primitive	Parameter	Status
I3.ICFrequest	TransportFlowID	Mandatory
	Rate descriptor	Optional
	Transport QoS parameters	Optional
	Transport addresses	Mandatory
	Packet transport protocol	Optional
	QoS mechanism	Optional

I3.ICFconfirm	TransportFlowID Rate descriptor Transport QoS parameters Transport addresses Packet transport protocol QoS mechanism	Mandatory Optional Optional Mandatory Optional Optional
I3.ICFreject	TransportFlowID Error reason Rate descriptor Transport QoS parameters Transport addresses Packet transport protocol QoS mechanism	Mandatory Mandatory Optional Optional Optional Optional Optional

Where the parameters contain the following information:

- **TransportFlowID**: Identifier of the flow
- **Rate descriptor:** describes de data rate of the flow (bandwidth and maximum packet size)
- **Transport QoS parameters:** desired QoS behavior of the flow through the firewall contains maximum delay, packet loss, and jitter.
- **Transport addresses**: address pairs of the incoming flow (address&port) and a list of addresses for the outgoing flows (the list allows optional multicasting of the flows)
- **Packet transport protocol**: TCP/UDP/SCTP/…..
- **QoS mechanism:** Describes the QoS mechanism on the outgoing flow none/ RSVP/ DiffServ/ MPLS/… plus mechanism specific parameters.
- **Error reason**: indicates why the request was rejected. E.g. *no more resources, illegal addresses, absurd QoS requirements.*

Example Flow

The flows that are of relevance are shown in Figure 2.

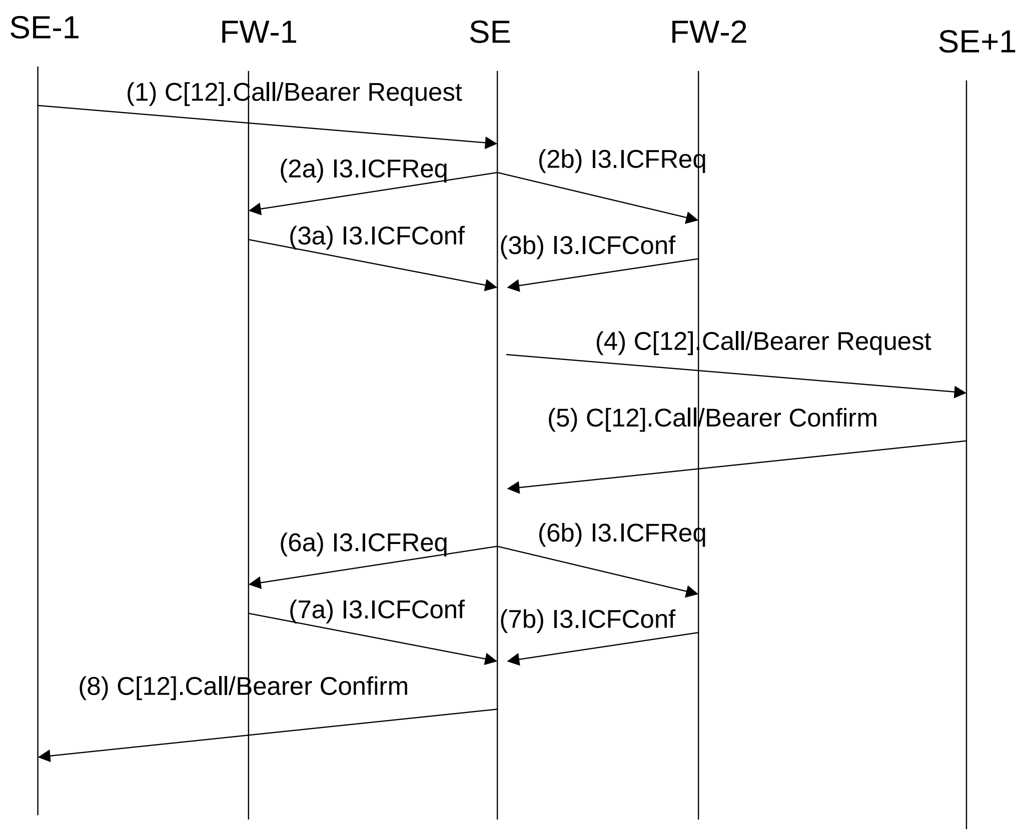


Figure 2. Information flows of relevance

(1) A Call and Bearer request (possibly implemented as a H.323 Setup with FastStart or SIP INVITE with SDP token) is sent to the Service Element.
(2) The firewalls are instructed to open the hole for the incoming media stream.
(3) The firewalls acknowledge this.
(4) The Service Element sends a Call and Bearer request to the next Service element.
(5) The next Service element acknowledges this providing its own media parameters again using H.248 or SDP tokens.
(6) The firewalls are instructed to open the hole for the other media path.
(7) The firewalls acknowledge this.
(8) The next Service element acknowledges to SE-1 relaying the H.248 or SDP tokens.

The interested reader is referred to DTS02009 for the details of these information flows.

Support for private address ranges

The generic flow described above can easily be refined to support private address ranges. The Service Elements can change the media (address) parameters while they are passing them on and modify the addresses and other parameters as appropriate.

Support for private address ranges requires the firewalls to be able to communicate with the service elements the address translation that is to be performed on a stream. The refinement necessary to the flows across reference point I3 as shown in Figure 2 is the possibility for either the SE to set the address mapping on the request or the firewall to provide the address to be mapped to in the confirm.

Conclusion

The flows as described in TIPHON DTS02009 seem to address the problem of Firewall control and are therefore proposed as the flows to further describe the firewall control problem. Extensions to private address ranges is considered to be a simple refinement. QoS support, encryption etc. are not addressed in this document and left for further study.

References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
[3] ETSI TIPHON meeting 18, Ottawa, May 22-26, Temporary Document 18TD028r1. R. Swale, BT. See www.etsi.org/tiphon for open access to documents.
[4] ETSI TIPHON DTS 2009 Baseline architecture for Release 3. See www.etsi.org/tiphon for open access to documents.

Author’s Addresses

Philip Mart Marconi Communications Ltd. Edge Lane Liverpool United Kingdom Email: philip.mart@marconi.com	Paul Sijben Lucent Technologies EMEA BV Huizen Netherlands Email: sijben@lucent.com	Richard Swale BT Adastral Park Ipswich United Kingdom mail: richard.swale@bt.com