Network Working Group
Request for Comments: 2356
Category: Informational

G. Montenegro
V. Gupta
Sun Microsystems, Inc.

June 1998

Sun's SKIP Firewall Traversal for Mobile IP

Status of This Memo

Copyright Notice

Abstract

The Mobile IP specification establishes the mechanisms that enable a mobile host to maintain and use the same IP address as it changes its point of attachment to the network. Mobility implies higher security risks than static operation, because the traffic may at times take unforeseen network paths with unknown or unpredictable security characteristics. The Mobile IP specification makes no provisions for securing data traffic. The mechanisms described in this document allow a mobile node out on a public sector of the internet to negotiate access past a SKIP firewall, and construct a secure channel into its home network.

In addition to securing traffic, our mechanisms allow a mobile node to roam into regions that (1) impose ingress filtering, and (2) use a different address space.

Table of Contents

1. Introduction

This document specifies what support is required at the firewall, the Mobile IP [1] home agent and the Mobile IP mobile node to enable the latter to access a private network from the Internet. For example, a company employee could attach his/her laptop to some Internet access point by:

a) Dialing into a PPP/SLIP account on an Internet service provider's network.

b) Connecting into a 10Base-T or similar LAN network available at, for example, an IETF terminal room, a local university, or another company's premises.

Notice that in these examples, the mobile node's relevant interface (PPP or 10Base-T) is configured with an IP address different from that which it uses "normally" (i.e. at the office). Furthermore, the IP address used is not necessarily a fixed assignment. It may be assigned temporarily and dynamically at the beginning of the session (e.g. by IPCP in the PPP case, or DHCP in the 10Base-T case).

The following discussion assumes a network configuration consisting of a private network separated by a firewall from the general Internet or public network. The systems involved are:

Private Network

A protected network separated from the Internet by hosts enforcing access restrictions (firewalls). A private network may use a private address space, and its addresses may not even be routable by the general internet.

Public Network

The Internet at large. Hosts are able to communicate with each other throughout the public network without firewall-imposed restrictions.

Mobile Node (MN)

Its permanent address falls within the range of the private network. The user removes the system from its home network, and connects it to the Internet at another point. The mechanisms outlined in this discussion render this mobility transparent: the mobile node continues accessing its home network and its resources exactly as if it were still within it. Notice that when the mobile node leaves its home network, it may migrate both within and outside of the private network's boundaries. As defined by Mobile IP [1], a mobile node uses a care-of address while roaming.

Home Agent (HA) for the mobile node

Serves as a location registry and router as described in the Mobile IP IETF draft.

Foreign Agent (FA)

Serves as a registration relayer and care of address for the mobile node as described in the Mobile IP IETF draft.

Correspondent Node (CH)

A system that is exchanging data packets with the mobile node.

Firewall (FW)

The system (or collection of systems) that enforces access control between the private network and the general Internet. It may do so by a combination of functions such as application gatewaying, packet filtering and cryptographic techniques.

The mechanisms described in this document allow a mobile node out on a public sector of the network to negotiate access past a SKIP firewall, and construct a secure channel into its home network. This enables it to communicate with correspondent nodes that belong to the private network, and, if bi-directional tunnels are used, with external hosts that are reachable when the mobile node is at home. The mobile node enjoys the same level of connectivity and privacy as it does when it is in its home network.

This document does not address the scenario in which the mobile node attempts to access its private network, while within another private network.

Sections 2 and 3 provide an overview of the environment being considered and the restrictions it imposes. Section 4 examines firewall technologies. Section 5 discusses the best mode of operation of the participating entities from the point of view of Mobile IP. Section 6 discusses possible configuration for the secure channel. Finally, packet formats are the topic of sections 7 and 8.

2. Mobility without a Firewall

Suppose the mobile node is roaming throughout the general Internet, but its home network is not protected by a firewall. This is typically found in academic environment as opposed to corporate networks.

This works as prescribed by Mobile IP [1]. The only proviso is that the mobile node would most probably operate with a co-located address instead of using a separate foreign agent's care-of address. This is because, at least in the near term, it is far more likely to be able to secure a temporary care-of-address than it is to find a foreign agent already deployed at the site you are visiting. For example:

- Internet Service Provider: pre-assigns customers IP addresses, or assigns them out dynamically via PPP's address negotiation.

- An IETF terminal room may pre-assign addresses for your use or offer DHCP services.

- Other locations probably would offer DHCP services.

3. Restrictions imposed by a Firewall

The firewall imposes restrictions on packets entering or leaving the private network. Packets are not allowed through unless they conform to a filtering specification, or unless there is a negotiation involving some sort of authentication.

Another restriction is imposed by the separation between private addresses and general Internet addresses. Strictly speaking, this is not imposed by a firewall, but by the characteristics of the private network. For example, if a packet destined to an internal address originates in the general Internet, it will probably not be delivered. It is not that the firewall drops it. Rather, the Internet's routing fabric is unable to process it. This elicits an ICMP host unreachable packet sent back to the originating node.

Because of this, the firewall MUST be explicitly targeted as the destination node by outside packets seeking to enter the private network. The routing fabric in the general Internet will only see the public address of the firewall and route accordingly. Once the packet arrives at the firewall, the real packet destined to a private address is recovered.

4. Two Firewall Options: Application relay and IP Security

Before delving into any details, lets examine two technologies which may provide firewall support for mobile nodes:

- application relaying or proxying, or
- IP Security.

To understand the implications, let's examine two specific schemes to accomplish the above: SOCKS version 5 and SKIP.

4.1 SOCKS version 5 [4]

There is an effort within the authenticated firewall traversal WG (aft) of the IETF to provide a common interface for application relays.

The solution being proposed is a revised specification of the SOCKS protocol. Version 5 has been extended to include UDP services as well. The SOCKS solution requires that the mobile node -- or another node on its behalf -- establish a TCP session to exchange UDP traffic with the FW. It also has to use the SOCKS library to encapsulate the traffic meant for the FW. The steps required by a SOCKS solution are:

- TCP connection established to port 1080 (1.5 round trips)
- version identifier/method selection negotiation (1 round trip)
    - method-dependent negotiation. For example, the Username/Password Authentication [5] requires 1 round trip:

1. client sends a Username/Password request
2. FW (server) responds

The GSS-API negotiation requires at least 3 round trips:

1. client context establishment (at least 1 round trip)
2. client initial token/server reply (1 round trip)
3. message protection subnegotiation (at least 1 round trip)

- (finally) SOCKS request/reply (1 round trip)

This is a minimum of 4 (6 with GSS-API) round-trips before the client is able to pass data through the FW using the following header:

RSV	FRAG	ATYP	DST.ADDR	DST.PORT	DATA
2	1	1	Variable	2	Variable

Bear in mind that the above must be done each time the mobile registers a new care-of address. In addition to this inefficiency, this scheme requires that we use UDP to encapsulate IP datagrams. There is at least one commercial network that does this, but it is not the best solution.

Furthermore, SOCKS defines how to establish authenticated connections, but currently it does not provide a clear solution to the problem of encrypting the traffic.

This header contains the relay information needed by all parties involved to reach those not directly reachable.

4.2 SKIP [3]

Alternatively, traffic from the mobile node to the firewall could be encrypted and authenticated using a session-less IP security mechanism like SKIP. This obviates the need to set up a session just to exchange UDP traffic with the firewall.

A solution based on SKIP is very attractive in this scenario, as no round trip times are incurred before the mobile node and the firewall achieve mutual trust: the firewall can start relaying packets for the mobile node as soon as it receives the first one. This, of course, implies that SKIP is being used with AH [7] so that authentication information is contained in each packet. Encryption by using ESP [6] is also assumed in this scenario, since the Internet at large is considered a hostile environment. An ESP transform that provides

both authentication and encryption could be used, in which case the AH header need not be included.

The firewall and the mobile node may be previously configured with each other's authenticated Diffie-Hellman public components (also known as public values). Alternatively, they could exchange them in real-time using any of the mechanisms defined by the SKIP protocol (on-line certificate directory service or certificate discovery protocol). Home agents and the firewall also MUST have, be able to exchange or obtain each other's public components.

There are other proposals besides SKIP to achieve IP layer security. However, they are session-oriented key management solutions, and typically imply negotiations spanning several round-trip times before cryptographically secure communications are possible. In this respect they raise similar concerns to those outlined previously in the discussion on SOCKS-based solutions. Others have arrived at similar conclusions regarding the importance of session-less key management for Mobile IP applications [8].

Another advantage of SKIP is its support for nomadic applications. Typically, two hosts communicating via a secure IP layer channel use the IP source and destination addresses on incoming packets to arrive at the appropriate security association. The SKIP header can easily supersede this default mechanism by including the key ID the recipient must use to obtain the right certificate.

The key id is specified by two fields in the SKIP header:

1) a name space identifier (NSID) to indicate which of the possible name spaces is being used, and,

2) a master key identifier (MKID) that uniquely indicates (within the given name space) an id to use in fetching the proper certificate.

As an example, by setting NSID to 1 and MKID to its home address, a mobile node tells a receiver "ignore the IP source and use my home address instead to look up my public component". Similarly, setting NSID to 8 enables using Unsigned Diffie-Hellman (UDH) certificates.

In this case, the MKID is set to the MD5 hash of the DH public component [10].

In addition to the NSID/MKID feature, Mobile IP is best supported by an appropriate policy at the SKIP firewall in the form of a "nomadic" access control list entry. This is an entry which is filtered by key ID, instead of by IP source address, as is the usual case. It

translates to "allow access from any IP source address for a given NSID/MKID combination". Furthermore, incoming packets MUST have an AH header, so that after properly authenticating them, the firewall establishes a "current address" or "dynamic binding" for the nomadic host. The NSID/MKID combination determines which key should be used with the nomadic host [9].

Notice that this supports Mobile IP, because the mobile node always initiates contact. Hence, the SKIP firewall has a chance to learn the mobile node's "current address" from an incoming packet before it attempts to encrypt an outgoing packet.

However, this precludes the use of simultaneous bindings by a mobile node. At the firewall, the last Registration Request sent by the mobile node replaces the association between its permanent address and any prior care-of address. In order to support simultaneous bindings the firewall must be able to interpret Mobile IP registration messages.

Section 7.2.2 discusses another advantage of making the firewall understand Mobile IP packet formats.

In what follows we assume a SKIP-based solution.

5. Agents and Mobile Node Configurations

Depending on which address it uses as its tunnel endpoint, the Mobile IP protocol specifies two ways in which a mobile node can register a mobility binding with its home agent.

a) an address advertised for that purpose by the foreign agent

b) an address belonging to one of the mobile node's interfaces (i.e. operation with a co-located address).

From the firewall's point of view, the main difference between these two cases hinges on which node prepares the outermost encrypting encapsulation. The firewall MUST be able to obtain the Diffie-Hellman public component of the node that creates the outermost SKIP header in an incoming packet. This is only possible to guarantee in case "b", because the mobile node and the firewall both belong to the same administrative domain. The problem is even more apparent when the mobile node attempts a Registration Request. Here, the foreign agent is not just a relayer, it actually examines the packet sent by the mobile node, and modifies its agent services accordingly. In short, assuming the current specification of Mobile IP and the current lack of trust in the internet at large, only case "b" is possible. Case "a" would require an extension (e.g. a "relay"

Registration Request), and modifying code at the home agent, the firewall and the foreign agent.

Assuming that the firewall offers a secure relay service (i.e. decapsulation and forwarding of packets), the mobile node can reach addresses internal to the private network by encapsulating the packets in a SKIP header and directing them to the firewall.

Therefore, It is simplest to assume that the mobile node operates with a co-located address.

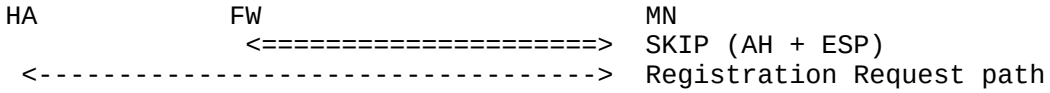
6. Supporting Mobile IP: Secure Channel Configurations

The mobile node participates in two different types of traffic: Mobile IP registration protocol and data. For the sake of simplicity, the following discussion evaluates different secure channel configurations by examining the initial Registration Request sent by the mobile node to its home agent.

Assuming the mobile node operates with a co-located address, it can communicate directly with the firewall. The latter is able to reach the home agent in the private network. Also, the firewall MUST be able to authenticate the mobile node.

The following channel configurations assume the mobile node operates with a co-located address. The region between the HA (home agent) and the FW (firewall) is a private network. The region between the FW and the MN (mobile node) is the outside or public network.

6.1 I: Encryption only Outside of Private Network



The traffic is only encrypted between the mobile node out on the general Internet, and the firewall's external interface. This is minimum required. It is the most desirable configuration as the more expensive encrypted channel is only used where it is necessary: on the public network.

6.2 II: End-to-End Encryption

Another possible configuration extends the encrypted tunnel through the firewall:

```
HA            FW                            MN
 <==================================>  SKIP (AH + ESP)
 <----------------------------------->  Registration Request path
```

This limits the firewall to perform a simple packet relay or gatewaying function. Even though this could be accomplished by using the proper destination NSID in the packet, in practice it is probably unrealizable. The reason is that this alternative is probably not very popular with computer security personnel, because authentication is not carried out by the firewall but by the home agent, and the latter's security is potentially much weaker than the former's.

6.3 III: End-to-End Encryption, Intermediate Authentication

A third alternative is to allow the firewall to be party to the security association between the home agent and the mobile node. After verifying authentication (AH header), the firewall forwards the encrypted packet (ESP hdr) to the home agent.

```
HA            FW                            MN
               <++++++++++++++++++++>  SKIP authentication
 <==================================>  SKIP encryption
 <----------------------------------->  Registration Request path
```

Here, SKIP is used to provide intermediate authentication with end-to-end security. Although possible, this option implies that the participating entities disclose their pairwise long-term Diffie-Hellman shared secret to the intermediate node.

Whereas Option 2 above is probably not agreeable to security and system administration personnel, option 3 is unsavory to the end user.

6.4 IV: Encryption Inside and Outside

```
HA            FW                            MN
 <============><====================>  SKIP (AH + ESP)
 <----------------------------------->  Registration Request path
```

Traffic is encrypted on the public as well as on the private network. On the public network, encryption is dictated by a security association between the mobile node and the firewall. On the private network, it is dictated by a security association between the home

agent and the firewall.

6.5 Choosing a Secure Channel Configuration

A potential problem in both options 2 and 3 is that their end-to-end channel components assume that the mobile node and the home agent can exchange IP traffic directly with each other. This is generally not the case, as the Internet routing fabric may not have routes to addresses that belong to private networks, and the private routing fabric may ignore how to route to public addresses -- or doing so may be administratively restricted. Therefore, it is necessary for packets to be addressed directly to the firewall, and indirectly -- via some tunneling or relaying capability -- to the real destination on the other side of the firewall.

Options 1 and 4 are essentially equivalent. The latter may be considered overkill, because it uses encryption even within the private network, and this is generally not necessary. What is necessary even within the private network is for the home agent to add an encapsulation (not necessarily encrypted) so as to direct datagrams to the mobile node via the firewall. The type of encapsulation used determines the difference between options 1 and 4. Whereas option 4 uses SKIP, option 1 uses a cleartext encapsulation mechanism. This is obtainable by, for example, using IP in IP encapsulation [2].

Options 1 and 4 are mostly interchangeable. The difference is, of course, that the former does not protect the data from eavesdroppers within the private network itself. This may be unacceptable in certain cases. Traffic from some departments in a company (for example payroll or legal) may need to be encrypted as it traverses other sections of the company.

In the interest of being conservative, in what follows we assume option 4 (i.e. traffic is encrypted on the general Internet, as well as within the private network.

Since the firewall is party to the security associations governing encryption on both the public and private networks, it is always able to inspect the traffic being exchanged by the home agent and the mobile node. If this is of any concern, the home agent and mobile node could set up a bi-directional tunnel and encrypt it.

7. Mobile IP Registration Procedure with a SKIP Firewall

When roaming within a private network, a mobile node sends Registration Requests directly to its home agent. On the public Internet, it MUST encapsulate the original Registration Request in a

SKIP packet destined to the firewall. The mobile node MUST distinguish between "inside" and "outside" addresses. This could be accomplished by a set of rules defining the address ranges. Nevertheless, actual installations may present serious difficulties in defining exactly what is a private address and what is not.

Direct human input is a very effective method: it may be obvious to the user that the current point of attachment is outside its private network, and it should be possible to communicate this knowledge to the mobile node software.

The home agent must also distinguish between "inside" and "outside" addresses, but lacks the potential benefit of direct user input. Accordingly, it should be possible for the mobile node to communicate that knowledge to the home agent. To accomplish this we define a Traversal Extension to the Registration Requests and Replies. This extension is also useful when traversing multiple firewalls.

In spite of the above mechanisms, errors in judgement are to be expected. Accordingly, the firewall SHOULD be configured such that it will still perform its relaying duties even if they are unnecessarily required by a mobile node with an inside care-of address.

Upon arriving at a foreign net and acquiring a care-of address, the mobile node must first -- before any data transfer is possible -- initiate a registration procedure. This consists of an authenticated exchange by which the mobile node informs its home agent of its current whereabouts (i.e. its current care-of address), and receives an acknowledgement. This first step of the protocol is very convenient, because the SKIP firewall can use it to dynamically configure its packet filter.

The remainder of this section shows the packet formats used. Section 7.1 discusses how a mobile node sends a Registration Request to its home agent via the SKIP firewall. Section 7.2 discusses how the home agent send the corresponding Registration Reply to the mobile node. Section 7.3 defines the Traversal Extension for use with Registration Requests and Replies.

7.1. Registration Request through the Firewall

The mobile node arrives at a foreign net, and using mechanisms defined by Mobile IP, discovers it has moved away from home. It acquires a local address at the foreign site, and composes a Registration Request meant for its home agent. The mobile node must decide whether this packet needs to be processed by SKIP or not.

This is not a simple rule triggered by a given destination address. It must be applied whenever the following conditions are met:

a) the mobile node is using a care-of address that does not belong to the private network (i.e. the mobile node is currently "outside" its private network), and

b) either of:

b1) the source address of the packet is the mobile node's home address (e.g. this packet's endpoints are dictated by a connection initiated while at home), or

b2) the source address of the packet is the care-of address and the destination address belongs to the private network

Since the above conditions are mobility related, it is best for the Mobile IP function in the node to evaluate them, and then request the appropriate security services from SKIP.

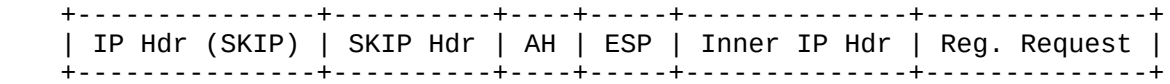
7.1.1. On the Outside (Public) Network

The SKIP module must use the firewall destination address and the firewall's certificate in order to address and encrypt the packet. It encrypts it using SKIP combined with the ESP [6] protocol and possibly the AH [7] protocol.

The SKIP header's source NSID equals 1, indicating that the Master Key-ID is the mobile node's home address. Notice that the IP packet's source address corresponds to the care-of address -- an address whose corresponding public component is unknown to the firewall.

It is also possible to use Unsigned Diffie-Hellman public components [10]. Doing so greatly reduces SKIP's infrastructure requirements, because there is no need for a Certificate Authority. Of course, for this to be possible the principals' names MUST be securely communicated.

REGISTRATION REQUEST: BETWEEN THE MOBILE NODE AND THE FIREWALL



IP Hdr (SKIP):
Source mobile node's care-of address
Destination firewall's public (outside) address

```
SKIP Hdr:
   Source          NSID = 1
                   Master Key-ID = IPv4 address of the mobile node
   Destination     NSID = 0
                   Master Key-ID = none
Inner IP Hdr:
   Source          mobile node's care-of address
   Destination     home agent's address
```

7.1.2. On the Inside (Private) Network

The SKIP Firewall's dynamic packet filtering uses this information to establish a dynamic binding between the care-of address and the mobile node's permanent home address.

The destination NSID field in the above packet is zero, prompting the firewall to process the SKIP header and recover the internal packet. It then delivers the original packet to another outbound interface, because it is addressed to the home agent (an address within the private network). Assuming secure channel configuration number 4, the firewall encrypts the packet using SKIP before forwarding to the home agent.

REGISTRATION REQUEST: BETWEEN THE FIREWALL AND THE HOME AGENT

IP Hdr (SKIP)	SKIP Hdr	AH	ESP	Inner IP Hdr	Reg. Request

```
IP Hdr (SKIP):
   Source          firewall's private (inside) address
   Destination     home agent's address

SKIP Hdr:
   Source          NSID = 0
                   Master Key-ID = none
   Destination     NSID = 0
                   Master Key-ID = none
Inner IP Hdr:
   Source          mobile node's care-of address
   Destination     home agent's address
```

7.2. Registration Reply through the Firewall

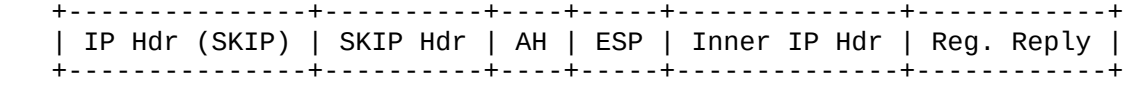
The home agent processes the Registration Request, and composes a Registration Reply. Before responding, it examines the care-of address reported by the mobile node, and determines whether or not it corresponds to an outside address. If so, the home agent needs to send all traffic back through the firewall. The home agent can

accomplish this by encapsulating the original Registration Reply in a SKIP packet destined to the firewall (i.e. we assume secure channel configuration number 4).

7.2.1. On the Inside (Private) Network

The packet from the home agent to the mobile node via the SKIP Firewall has the same format as shown above. The relevant fields are:

REGISTRATION REPLY: BETWEEN THE HOME AGENT AND THE FIREWALL



IP Hdr (SKIP):
- Source: home agent's address
- Destination: firewall's private (inside) address

SKIP Hdr:
- Source: NSID = 0, Master Key-ID = none
- Destination: NSID = 0, Master Key-ID = none

Inner IP Hdr:
- Source: home agent's address
- Destination: mobile node's care-of address

7.2.2. On the Outside (Public) Network

The SKIP Firewall recovers the original Registration Reply packet and looks at the destination address: the mobile node's care-of address.

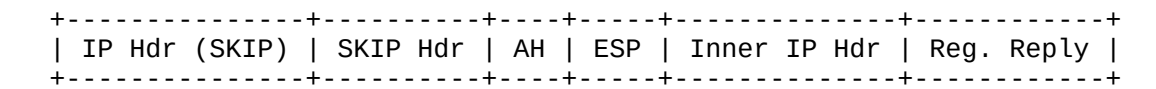
The SKIP Firewall's dynamic packet filtering used the initial Registration Request (Secton 7.1) to establish a dynamic mapping between the care-of address and the mobile node's Master Key-ID. Hence, before forwarding the Registration Reply, it encrypts it using the mobile node's public component.

This dynamic binding capability and the use of tunneling mode ESP obviate the need to extend the Mobile IP protocol with a "relay Registration Request". However, it requires that the Registration Reply exit the private network through the same firewall that forwarded the corresponding Registration Request.

Instead of obtaining the mobile node's permanent address from the dynamic binding, a Mobile IP aware firewall could also obtain it from the Registration Reply itself. This renders the firewall stateless, and lets Registration Requests and Replies traverse the periphery of

the private network through different firewalls.

REGISTRATION REPLY: BETWEEN THE FIREWALL AND THE MOBILE NODE



IP Hdr (SKIP):

Source	firewall's public (outside) address
Destination	mobile node's care-of address

SKIP Hdr:

Source	NSID = 0 Master Key-ID = none
Destination	NSID = 1 Master Key-ID = IPv4 addr of the mobile node

Inner IP Hdr:

Source	home agent's address
Destination	mobile node's care-of address

7.3. Traversal Extension

The Traversal Extension MAY be included by mobile nodes in Registration Requests, and by home agents in Registration Replies. As per Section 3.6.1.3 of [1], the Traversal Extension must appear before the Mobile-Home Authentication Extension. A Traversal Extension is an explicit notification that there are one or more traversal points (firewalls, fireridges, etc) between the mobile node and its home agent. Negotiating access past these systems may imply a new authentication header, and possibly a new encapsulating header (perhaps as part of tunnel-mode ESP) whose IP destination address is the traversal address.

Negotiating access past traversal points does not necessarily require cryptographic techniques. For example, systems at the boundary between separate IP address spaces must be explicitly targetted (perhaps using unencrypted IP in IP encapsulation).

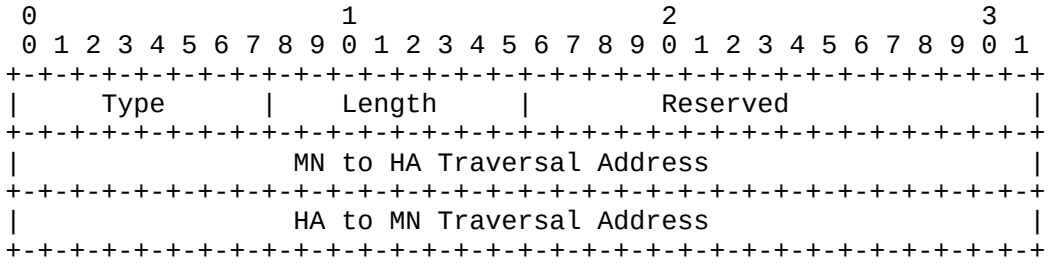
A mobile node SHOULD include one Traversal Extension per traversal point in its Registration Requests. If present, their order MUST exactly match the order in which packets encounter them as they flow from the mobile node towards the home agent.

Notice that there may be additional firewalls along the way, but the list of traversal points SHOULD only include those systems with which an explicit negotiation is required.

Similarly, the home agent SHOULD include one Traversal Extension per traversal point in its Registration Replies. If present, their order MUST exactly match the order in which packets encounter them as they flow from the home agent to the mobile node.

A Traversal Extension does not include any indication about how access is negotiated. Presumably, this information is obtained through separate means. This document does not attempt to solve the firewall discovery problem, that is, it does not specify how to discover the list of traversal points.

As per section 1.9 of [1], the fact that the type value falls within the range 128 to 255 implies that if a home agent or a mobile node encounter a Traversal Extension in a Registration Request or Reply, they may silently ignore it. This is consistent with the fact that the Traversal Extension is essentially a hint.



Type

129

Length

10

Reserved

0

MN to HA Traversal Address

The IP address of the an intermediate system or firewall encountered by datagrams sent by the mobile node towards the home agent. Typically, this is the external address of a firewall or firewall complex.

This field MUST be initialized in Registration Requests. In Registration Replies, it is typically all 0's, otherwise, the mobile node SHOULD interpret it as a hint.

HA to MN Traversal Address

The IP address of an intermediate system or firewall encountered by datagrams sent by the home agent towards the mobile node. Typically, this is the internal address of a firewall or firewall complex.

This field MUST be initialized in Registration Replies. In Registration Requests, it is typically all 0's, otherwise, the home agent SHOULD interpret it as a hint.

8. Data Transfer

Data transfer proceeds along lines similar to the Registration Request outlined above. Section 8.1 discusses data traffic sent by a mobile node to a correspondent node. Section 8.2 shows packet formats for the reverse traffic being tunneled by the home agent to the mobile node.

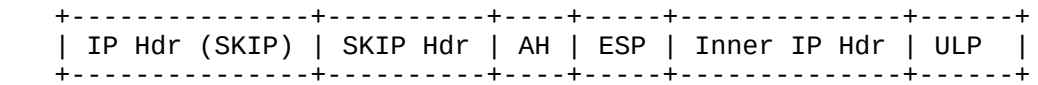
8.1. Data Packet From the Mobile Node to a Correspondent Node

The mobile node composes a packet destined to a correspondent node located within the private network.

The Mobile IP function in the mobile node examines the Inner IP header, and determines that it satisfies conditions "a" and "b1" from Section 7.1. The mobile node requests the proper encryption and encapsulation services from SKIP.

Thus, the mobile node with a co-located address sends encrypted traffic to the firewall, using the following format:

DATA PACKET: FROM THE MOBILE NODE VIA THE FIREWALL



IP Hdr (SKIP):

Source	mobile node's care-of address
Destination	public (outside) address on the firewall

```
SKIP Hdr:
   Source          NSID = 1
                   Master Key-ID = IPv4 address of the mobile node
   Destination     NSID = 0
                   Master Key-ID = none
Inner IP Hdr:
   Source          mobile node's home address
   Destination     correspondent node's address
```

The SKIP Firewall intercepts this packet, decrypts the Inner IP Hdr and upper-layer payload (ULP) and checks the destination address. Since the packet is destined to a correspondent node in the private network, the "Inner" IP datagram is delivered internally. Once the SKIP firewall injects this packet into the private network, it is routed independently of its source address.

As this last assumption is not always true, the mobile node may construct a bi-directional tunnel with its home agent. Doing so, guarantees that the "Inner IP Hdr" is:

```
Inner IP Hdr:
   Source          care-of address
   Destination     home agent address
```

When at home, communication between the the mobile node and certain external correspondent nodes may need to go through application-specific firewalls or proxies, different from the SKIP firewall. While on the public network, the mobile node's communication with these hosts, MUST use a bi-directional tunnel.

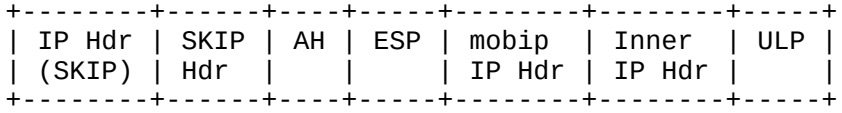
8.2. Data Packet From a Correspondent Node to the Mobile Node

The home agent intercepts a packet from a correspondent node to the mobile node. It encapsulates it such that the Mobile IP encapsulating IP header's source and destination addresses are the home agent and care-of addresses, respectively. This would suffice for delivery within the private network. Since the current care-of address of the mobile node is not within the private network, this packet MUST be sent via the firewall. The home agent can accomplish this by encapsulating the datagram in a SKIP packet destined to the firewall (i.e. we assume secure channel configuration number 4).

8.2.1 Within the Inside (Private) Network

From the home agent to the private (inside) address of the firewall the packet format is:

DATA PACKET: BETWEEN THE HOME AGENT AND THE FIREWALL



IP Hdr (SKIP):
- Source: home agent's address
- Destination: private (inside) address on the firewall

SKIP Hdr:
- Source: NSID = 0, Master Key-ID = none
- Destination: NSID = 0, Master Key-ID = none

Mobile-IP IP Hdr:
- Source: home agent's address
- Destination: care-of address

Inner IP Hdr:
- Source: correspondent node's address
- Destination: mobile node's address

ULP: upper-layer payload

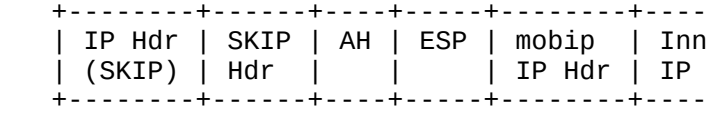
The packet format above does not require the firewall to have a dynamic binding. The association between the mobile node's permanent address and it care-of address can be deduced from the contents of the "Mobile-IP IP Hdr" and the "Inner IP Hdr".

Nevertheless, a nomadic binding is an assurance that currently the mobile node is, in fact, at the care-of address.

8.2.2. On the Outside (Public) Network

The SKIP firewall intercepts the packet, and recovers the Mobile IP encapsulated datagram. Before sending it out, the dynamic packet filter configured by the original Registration Request triggers encryption of this packet, this time by the SKIP firewall for consumption by the mobile node. The resultant packet is:

DATA PACKET: BETWEEN THE FIREWALL AND THE MOBILE NODE



IP Hdr (SKIP):
- Source: firewall's public (outside) address
- Destination: mobile node's care-of address

SKIP Hdr:
- Source: NSID = 0; Master Key-ID = none
- Destination: NSID = 1; Master Key-ID = IPv4 address of the mobile node

Mobile-IP IP Hdr:
- Source: home agent's address
- Destination: care-of address

Inner IP Hdr:
- Source: correspondent node's address
- Destination: mobile node's address

ULP: upper-layer payload

At the mobile node, SKIP processes the packets sent by the firewall. Eventually, the inner IP header and the upper-layer packet (ULP) are retrieved and passed on.

9. Security Considerations

The topic of this document is security. Nevertheless, it is imperative to point out the perils involved in allowing a flow of IP packets through a firewall. In essence, the mobile host itself MUST also take on responsibility for securing the private network, because it extends its periphery. This does not mean it stops exchanging unencrypted IP packets with hosts on the public network. For example, it MAY have to do so in order to satisfy billing requirements imposed by the foreign site, or to renew its DHCP lease.

In the latter case it might filter not only on IP source address, but also on protocol and port numbers.

Therefore, it MUST have some firewall capabilities, otherwise, any malicious individual that gains access to it will have gained access to the private network as well.

Acknowledgements

Ideas in this document have benefited from discussions with at least the following people: Bill Danielson, Martin Patterson, Tom Markson, Rich Skrenta, Atsushi Shimbo, Behfar Razavi, Avinash Agrawal, Tsutomu Shimomura and Don Hoffman. Jim Solomon has also provided many helpful comments on this document.

References

[1] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[2] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[3] A. Aziz and M. Patterson, Design and Implementation of SKIP, available on-line at http://skip.incog.com/inet-95.ps. A previous version of the paper was presented at INET '95 under the title Simple Key Management for Internet Protocols (SKIP), and appears in the conference proceedings under that title.

[4] Leech, M., Ganis, M., Lee, Y, Kuris, R., Koblas, D., and L. Jones, "SOCKS Protocol Version 5", RFC 1928, March 1996.

[5] Leech, M., "Username/Password Authentication for SOCKS V5", RFC 1929, March 1996.

[6] Atkinson, R., "IP Encapsulating Payload", RFC 1827, August 1995.

[7] Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.

[8] Stephen Kent, message to the IETF's IPSEC mailing list, Message-Id: <v02130500ae569a3e904e@[128.89.30.29]>, September 6, 1996.

[9] Tom Markson, private communication, June 12, 1996.

[10] A. Aziz, T. Markson, H. Prafullchandra. Encoding of an Unsigned Diffie-Hellman Public Value. Available on-line as http://skip.incog.com/spec/EUDH.html.

Authors' Addresses

Gabriel E. Montenegro
Sun Microsystems, Inc.
901 San Antonio Road
Mailstop UMPK 15-214
Mountain View, California 94303

Phone: (415)786-6288
Fax: (415)786-6445
EMail: gabriel.montenegro@Eng.Sun.COM

Vipul Gupta
Sun Microsystems, Inc.
901 San Antonio Road
Mailstop UMPK 15-214
Mountain View, California 94303

Phone: (415)786-3614
Fax: (415)786-6445
EMail: vipul.gupta@Eng.Sun.COM

Full Copyright Statement