Report # I733-040R-2007
Date: 09/19/2007

A Filtering Strategy for Mobile IPv6

Enterprise Applications Division
of the
Systems and Network Analysis Center (SNAC)

Information Assurance Directorate

Author
Casimir A. Potyraj, I733
(410) 854-5723
cas@thematrix.ncsc.mil

National Security Agency
Attn: I733
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704
(410) 854-6191

This page intentionally blank

Table of Contents

1 Introduction

A firewall filtering strategy for Mobile IP traffic in IPv6 is presented in this document along with supporting analysis and rationale.

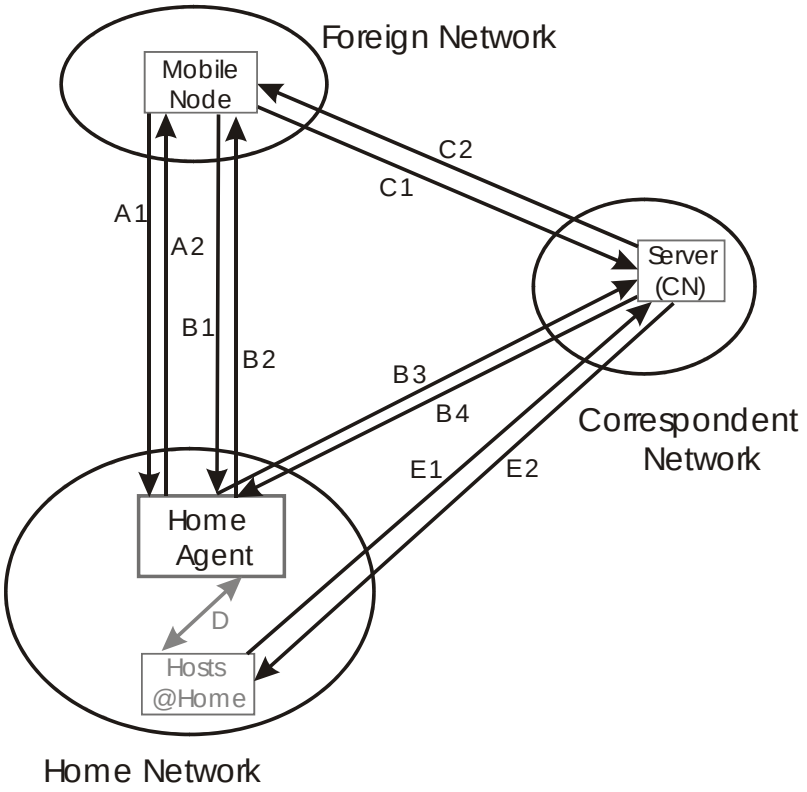
1.1 Basic Mobile IP Traffic Flows

Mobile IP traffic is exchanged between three participating sites: Home Network, Foreign Network, and Correspondent Network, as opposed to only two sites involved with "normal" (i.e. non-mobile) IP. Refer to Figure 1. When a mobile node is at home, traffic flows between the Home Network and a Correspondent Network and is identical to the normal IP scenario. A server on the Internet, for example, could be a correspondent node and the server's network would be referred to as the Correspondent Network. When the mobile node moves to a new site, it connects to a link at a Foreign Network and begins the unique mobile IP traffic scenario. The mobile node first communicates with the Home Network, then with the correspondent node via the Home Network, and finally (and optionally) with the correspondent node directly. These three flows are indicated by the letters A, B, and C, respectively in Figure 1. The numbers 1 and 2 are used to distinguish the two directions of traffic flow. Furthermore, flow B1 is paired with B3 and B2 is paired with B4 to represent the traffic that flows through the Home Network to the Correspondent Network. Flow D is mobility-related internal traffic that is not seen by any firewall. Flow E represents normal IP traffic and also Mobile IP correspondent binding de-registration, which occurs when the mobile node returns home. Since each of the three sites will likely employ a firewall, this document accommodates the expected traffic cases in a manner that both allows mobile IP operation and maintains site security.

1.2 Mobile IP and IPsec

The Mobile IP specifications mandate a very specialized usage of IPsec for the protection of critical communications. A very important distinction must be made between this limited use of IPsec to protect Mobile IP and the more typical use of IPsec to implement a full Communication Security (COMSEC) model. Mobile IP requires IPsec only for a bare minimum set of critical enabling packets between a mobile node and its home agent at the Home Network. This brings Mobile IP up to roughly the same level of security as that of normal (non-mobile) unprotected (no IPsec) IP. Furthermore, the current RFCs[1, 2] for Mobile IP do not specify how the protocol would work in the case where all traffic *must be* fully protected by IPsec. A network architect can choose mobility or full IPsec but not both, and if mobility is chosen, IPsec is used in a very limited way on certain packets to/from the home agent.

The issue of providing Mobile IP in a secure (fully IPsec protected) environment is deferred to separate analysis. The firewall configuration guidance provided here assumes the currently specified Mobile IP scenarios only. The detailed analysis of the specified IPsec support (e.g. configuring IPsec, security associations, the coexistence of IPsec and mobility headers, etc...) is also deferred. The guidance here is specifically on determining the best firewall filtering to accompany the currently specified Mobile IP design.



Mobile Node's Traffic

A1:	To Home Agent	C1:	Route Opt To CN
A2:	From Home Agent	C2:	Route Opt From CN
B1-B3:	Reverse tunneling To CN	D:	Mobility-related traffic not seen by a firewall
B2-B4:	Reverse tunneling From CN		
B1-D:	Tunneling To Home	E1:	Normal Traffic and de-register
D-B2:	Tunneling From Home	E2:	Normal Traffic and de-register

Figure 1: Mobile IPv6 Traffic Flows

2 Going Mobile or Not

The first security-related issue is whether or not "going mobile" is allowed. All three networks have a different perspective on this issue and users should contemplate it as well. These perspectives are discussed below from a theoretical standpoint. The practical matter of firewall configuration and packet filtering details are contained in section 4.

2.1 Home Network Perspective

Individual networks in an IP-based internet[A], have ownership (or at least temporary rights) over certain address prefixes referred to as their allocated address space. Owners of these networks have a reasonable expectation that "their" traffic will be delivered to

[A] The lowercase "i" is deliberate and implies any IP internet, not the public Internet in particular.

them and not somewhere else. This is *reasonable* in as much as the basic integrity of the internet's routing system is relied upon.

Home networks in a Mobile IP scenario should be able to have this same level of control over their home addresses. A system administrator should be able to decide which of his users can "go mobile" with the same confidence that he has in knowing that traffic is delivered to/from one of his own addresses in normal IP. Mobile IP should not be any weaker than normal IP in this respect.

The design of Mobile IP supports this goal by requiring cooperation of the Home Network, by means of a home agent, in order for a node to go mobile. When a node is mobile, it uses its home address to receive packets at some foreign link. Nodes cannot decide to do this on their own without a home agent enabled back at the Home Network.

Mobile IP does not interact with IP routing protocols such as RIP or BGP. This is a significant point and a good decision by the standards body because it allows the routing system to maintain the same level of integrity with or without mobility enabled. Hence Mobile IP doesn't work by tweaking routes or routing tables with alternate information, an approach that would have been too slow to converge anyway. Instead, special purpose IPv6 headers are used to swap in/out the home address just after/before the packet is delivered. The mobile node, in this manner, appears to use its home address while the routers see an address relevant to the node's current location at the Foreign Network. Mobile IP is designed to **only** allow this swapping if a binding is established, and a binding can **only** be established through the cooperation of the home agent.

In conclusion, the Home Network is certainly concerned with the decision of whether its nodes can go mobile and the decision can be completely controlled by the presence/absence of a working home agent. The Home Network's security strategy, therefore, should have the ability to either prevent any home agent operation (if Mobile IP is to be disabled) or to prevent/detect any unauthorized home agents from being set up in the Home Network (if Mobile IP is enabled).

2.2 Foreign Network Perspective

The concern with Mobile IP at the Foreign Network is with the basic function of link access control. A foreign link will likely want some means of verifying whether a visiting node is authorized to be on-link. Unauthorized users would consume valuable resources and would clearly be a greater security threat as an insider even without using Mobile IP at all.

Link access control can be accomplished at the link layer or potentially at the IP layer if changes are made to the IPsec architecture. Once a node is authorized to be on-link, the IPv6 Neighbor Discovery and Address Auto-configuration protocols act to establish a local IP address. At this point, the foreign link likely will not care whether the visiting node chooses to activate Mobile IP to utilize its home address.

Practically speaking, a foreign link in a *true* mobile scenario must be wireless. True mobility involves a mobile node continuously on the move such that dealing with physical connections are too sluggish and slow. Technically speaking, however, the

Mobile IP protocol is not dependant on any specific type of link layer technology and could be utilized from a wired foreign link. When a mobile node registers at a foreign link once (i.e. not continuously hopping to new links) the result is more of a Remote Access scenario than a mobile IP scenario.

A wireless link already raises the concerns for link access control independent of the Mobile IP protocols. Security mechanisms at the link layer are currently the best means of imposing this control. Wired links typically achieve link access control through physical security, building access, and other measures over human activity in the network's physical space.

It is possible to imagine scenarios where a wireless network specifically wants to allow visiting nodes but to prohibit them from using Mobile IP. Say a mall has a free wireless access network intended for shoppers, but motorists on a nearby roadway frequently use it as a mobile hop when they drive by. The mall owners may want to thwart these drive-by users by disabling Mobile IP. Although such scenarios seem far-fetched, the task of disabling the Foreign Network characteristics from a network will be included in the filtering guidance of this document in case it is needed in the future.

Mobile IP hides the home address within a Destination Option header of outbound traffic from a mobile node that is away from home. The mobile node uses its foreign link IP address (called the care-of address) as the source IP address, therefore ingress filtering[3] can be performed normally on the foreign link without disrupting Mobile IP.

In conclusion, the main concern at the Foreign Network is link access control which requires a technical solution for wireless links regardless of Mobile IP. In most cases, Mobile IP will not prompt any additional firewall filtering, though in rare cases it may be desired to disable Mobile IP for visiting nodes. Ingress filtering is not adversely affected by Mobile IP.

2.3 Correspondent Network Perspective

Administrators or data owners at a Correspondent Network may *want* to restrict access to a server based on whether the remote client is mobile. Since access to some servers in normal IP is restricted to a set of allowable source addresses, it seems logical that the mobility of these allowed users may be unacceptable to some Correspondent Networks. They may take the position: "You can access my data but not from a remote location". A mobile user can present a higher risk when the access point is wireless or when in a region of the world where even the wired traffic is at a greater risk. The problem with this viewpoint is that there **is no way for a Correspondent Network to know for sure if a remote client is mobile or not.**

Although the Correspondent Network does participate in address binding operations using the Mobile IP protocol and specialty headers, this is only for the optional Route Optimization method that allows more efficient routing of Mobile IP traffic. The default, less efficient method (called reverse tunneling), consists of tunneling packets through the home agent. Once these packets are decapsulated out of the tunnel, there is no way to distinguish them from normal IP that would have originated from a non-mobile node at

the Home Network. A Correspondent Network, therefore, cannot expect to have a firewall policy that is sensitive to whether or not the accessing client is mobile or not.

Given this reality, the Correspondent Networks should focus on how to handle traffic when the mobility protocol and Mobile IP specialty headers *are* present. It is not recommended to punish nodes for using this more efficient Route Optimization method since that would result in more mobile users turning it off and less efficiency overall. Correspondent Networks shouldn't block users who use the Mobile IP specialty headers or they will simply fall back to tunneling through the home agent and get through anyway.

The source address in normal IP provides a weak WHO-WHERE property to the packet. The WHO refers to a specific node or user that owns the address and the WHERE refers back to the basic integrity of the routing system that provides reasonable expectation of delivery to a specific destination network. This is not usually thought of as a geographical WHERE but an access point somewhere in the internet[4]. The word "weak" is used only to indicate that these properties are not cryptographically enforced and therefore may be spoofable.

Mobile IP makes use of both a home address and care-of address. A good way of thinking about this is to consider that the WHO-WHERE property of a normal IP address has now been split into a WHO address and a WHERE address. The home address indicates WHO is sending the packet and the care-of address indicates his/her present location in the internet. If the default reverse tunneling method of Mobile IP traffic is used (i.e. not route optimization), the care-of address is stripped off when the packet emerges from the tunnel. The correspondent node receives only the inner packet and sees only the home address. If route optimization is used, then the correspondent node verifies a binding between the home and care-of addresses, after which it can directly receive traffic containing both addresses: the care-of address as the source and the home address hidden in a specialty header.

In conclusion, Correspondent Networks should base firewall filtering on the home address (the WHO) regardless of whether the packet is received via the route optimization method or not. This implies a capability in firewalls for processing the specialty mobility headers, which may or may not presently exist. Few (if any) IPv6 filtering frameworks have the ability to filter a home address when route optimization is in use. If the firewall does not yet have this capability, there are some workarounds that will be discussed in section 4.3.

2.4 User Perspective

Finally, individual users should be aware of the fact that going mobile may present a greater security risk to the mobile node itself.

First off, a mobile node is most likely wireless and therefore has a greater chance of having its traffic collected at a foreign site. Using wireless access protocols on the home link presents similar concerns, but going mobile increases the threat greatly because there are more sites and less chance of knowing who might be listening. IPsec is used to protect the bare minimum of critical packets between the mobile node and home agent,

but all other traffic to the home agent may or may not be IPsec protected. Furthermore all traffic from the mobile node directly to the correspondent node (i.e. Route Optimization in use) would not have IPsec applied according to the current Internet Engineering Task Force (IETF) specifications.

Secondly, a mobile node visiting a foreign link may not receive the same protections as provided by the Home Network. For example, filtering for viruses or malicious code may be weaker; Intrusion Detection System (IDS) protection is likely not applied to links where mobile users are constantly coming and going.

Finally, a mobile node visiting many Foreign Networks is at a higher risk simply from the increased exposure to different links. Statistically speaking, connecting to more links brings greater risk.

3 Traffic Cases for Mobile IP

A filtering strategy for Mobile IP must address security issues at each of the three sites (Home, Foreign, and Correspondent Networks). The firewall must contend with the traffic cases presented in this section when Mobile IP is in use.

There are three IPv6 header types exclusively associated with Mobile IP: the Home Address Destination Option Header, the Mobility Header, and the Type 2 Routing Header[5]. The occurrence and visibility (encrypted or not) of each of these headers is important to the firewall strategy.

The Mobility Header is defined as a separate IPv6 extension header (i.e. not an option contained within one of the two Options extension headers) and is used to send a variety of different Mobile IP messages. The specification requires that the "next header" value[6] of a Mobility Header must be *0x3B* indicating that there is no next header or upper layer protocol. Essentially the Mobility (extension) Header functions as a standalone IP protocol.

The Home Address Destination Option is used in some messages sent by the mobile node as a means of delivering the home address when it is inappropriate to use the home address directly as an IP source address. This option is also used as a data field in Binding Update operations.

The Type 2 Routing Header is used in some messages returning back to the mobile node. It delivers the home address when it is inappropriate to use the home address directly as an IP destination address.

The following figures show the messages that occur in a Mobile IP scenario for each of the labeled paths shown back in Figure 1. The legend and list of abbreviations below apply to all of the figures.

Legend and Abbreviations:

(IP header fields)
s: or d: -Source or Destination IP address
(possible address values)
Co -Mobile node's care-of address
H -Mobile node's home address
HA -Home Agent's IP address
CN -Correspondent Node IP address
ac -an IPv6 anycast address within the home network
h* -any host within the home network other than the Home Agent

(Protocols)
IP -Internet Protocol version 6
ICMP -Internet Control Message Protocol version 6
(ICMP message types)
HA disc Req -Home Agent Address Discovery Request, (RFC 3775, sec 6.5)
HA disc Reply -Home Agent Address Discovery Reply, (RFC 3775, sec 6.6)
Prefix Solicit -Mobile Prefix Solicitation, (RFC 3775, sec 6.7)
Prefix Adv -Mobile Prefix Advertisement, (RFC 3775, sec 6.8)

UDP -User Datagram Protocol version 6
IKE -Internet Key Exchange Protocol (IPsec key exchange)

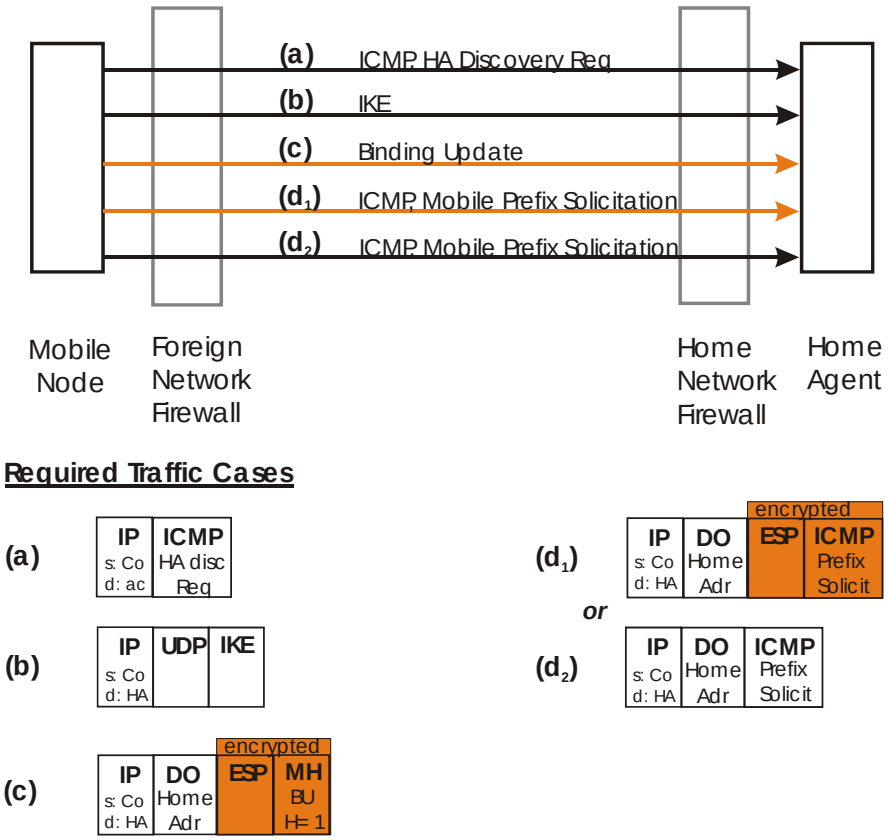
(IPv6 Extension Headers)
DO -Destination Options
(Destination Option types)
Home Adr -Home Address Destination Option, (RFC 3775, sec 6.3)

ESP -Encapsulation Security Payload (IPsec encryption)
RH -Routing Header
(Routing Header types)
Type 2 -Type 2 Routing Header, (RFC 3775, sec 6.4)

MH -Mobility Header
(Mobility Header types)
BU H=1 -Binding Update with H-bit set, (RFC 3775, sec 6.1.7)
BU H=0 -Binding Update with H-bit cleared, (RFC 3775, sec 6.1.7)
Bind Ack -Binding Acknowledgement, (RFC 3775, sec 6.1.8)
Bind Error -Binding Error, (RFC 3775, sec 6.1.9)
Bind Rfrsh -Binding Refresh Request, (RFC 3775, sec 6.1.2)
HoTI -Home Test Init, (RFC 3775, sec 6.1.3)
Ho Test -Home Test, (RFC 3775, sec 6.1.5)
CoTI -Care of Test Init, (RFC 3775, sec 6.1.4)
Co Test -Care of Test, (RFC 3775, sec 6.1.6)

3.1 A1 Traffic Cases

The A1 set represents packets sent by a mobile node (while away from home) to a home agent within the Home Network.



The Home Agent Discovery Request message (A1-a) is an optional ICMP message that will probably not be widely used since it requires an anycast address to be set up in the Home Network. Instead, mobile nodes will likely leave home with the knowledge of its home agents' addresses. In any event, this message should not be considered security sensitive.

Internet Key Exchange (IKE) messages (A1-b) may or may not occur. They will not occur if IPsec security associations (SAs) are manually configured for the mobile node/home agent pair. Even if dynamic SA generation is used, IKE will not be needed at every foreign link, but only when the established SAs have expired. These SAs are established with respect to the mobile node's home address and therefore remain valid at new Foreign Networks.

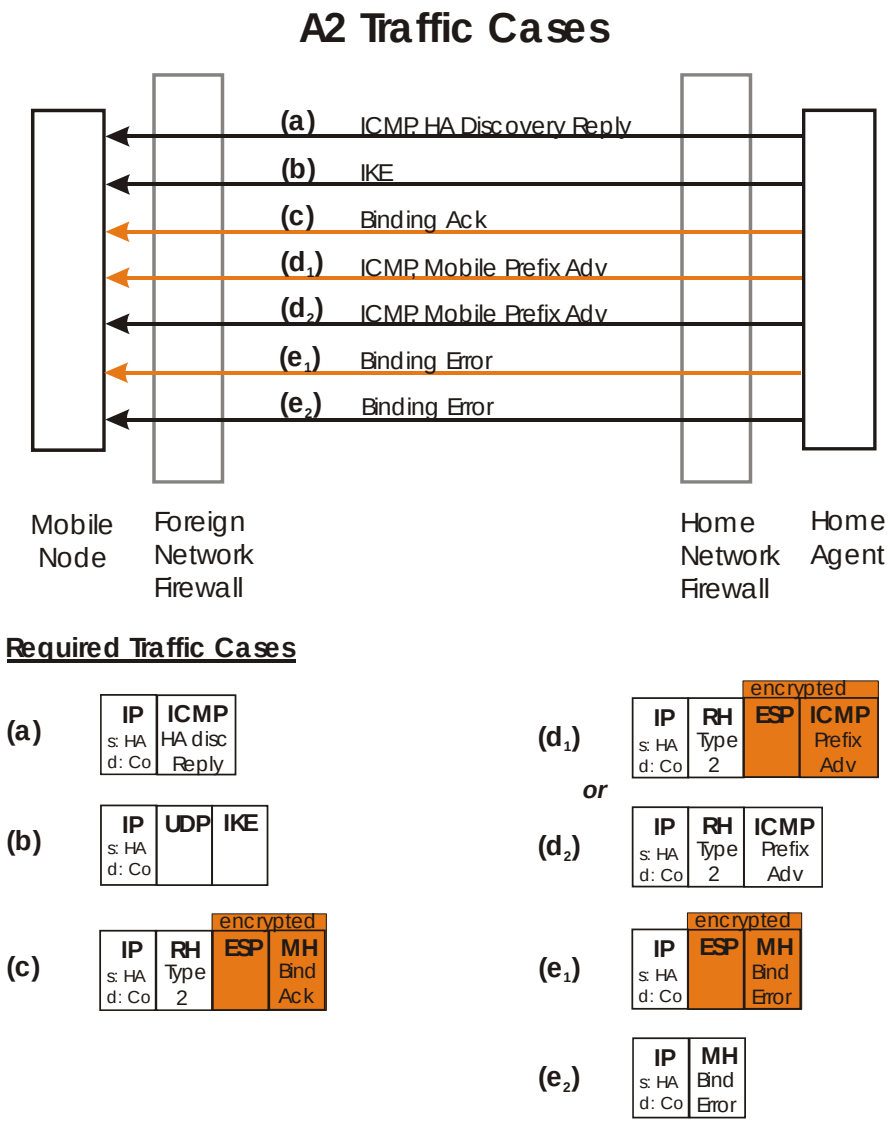
The Binding Update message (A1-c) to the home agent is important from a security standpoint. This message must be encrypted according to the Mobile IP standards[7] and will have the Home Address Destination Option present[8]. The H flag within the Binding Update message will be set to 1, though this will not be visible to the firewall due to the applied encryption.

Mobile IP specification states that Mobile Prefix Solicitation messages SHOULD be IPsec protected but does not say MUST[9]. Therefore, either A1-d_1 or A1-d_2 will be observed, but not both. These messages contain the address prefixes used by the Home Network and therefore MAY be security sensitive. For example, an adversary could

discover all address prefixes used by the Home Network (i.e. map the network). Though this is not a compromise in itself, it could help in the efforts to mount other attacks. If there is only one address prefix being used by the Home Network, the Mobile Prefix Solicitation messages cause no security concern. The prefix in that case would already be visible via the home addresses in use.

A2 Traffic Cases

The A2 set represents packets sent by a home agent to a mobile node that is away from home. This is largely response traffic to the A1 cases but can also be initiated by the home agent such as with unsolicited Mobile Prefix Advertisement messages.

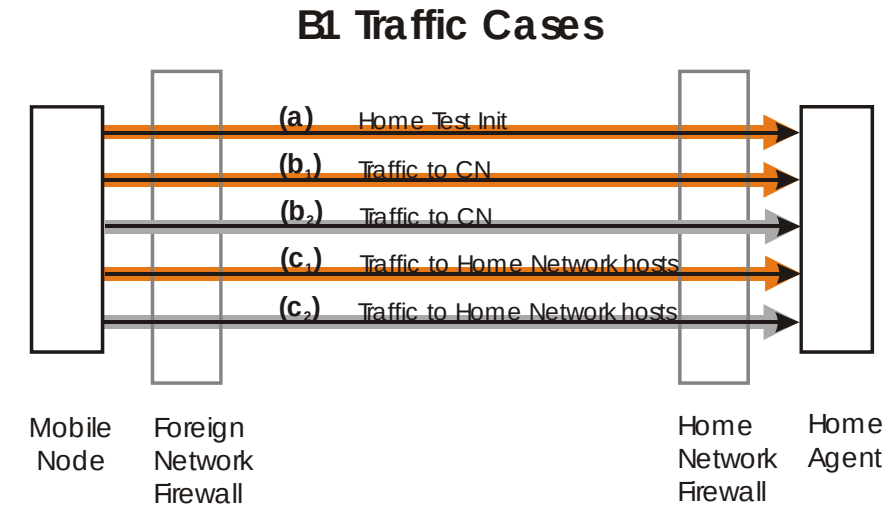


As with the Mobile Prefix Solicitation, the Advertisement also may or may not be encrypted.[10] The Type 2 Routing Header is required.[11]

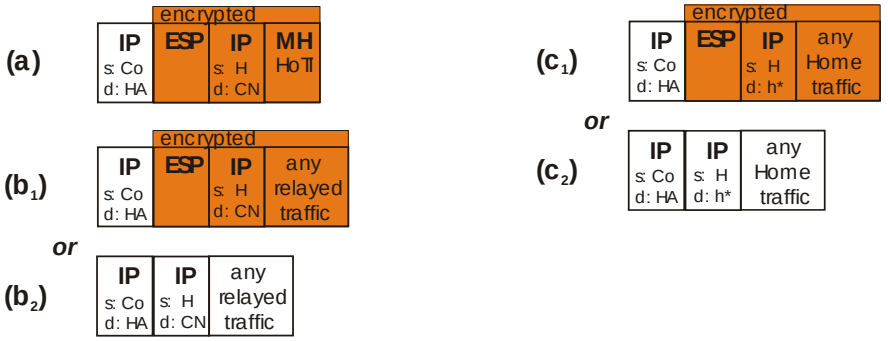
In rare occurrences a Binding Error message could be sent to the mobile node from the home agent.[12] The Binding Error will likely be unencrypted as shown by format A2-e_2. The encrypted format (A2-e_1) is technically possible though would require a separate IPsec security association (from that used for A2-c) since these messages are sent to the care-of address, not the home address. It is easier to leave the Binding Error messages in the clear and there are no foreseen security threats from doing so.

3.2 B1 Traffic Cases

The B1 set represents packets that are tunneled through the home agent by a mobile node that is away from home. This includes traffic relayed to a correspondent node via Mobile IP's reverse tunneling mode of operation and any traffic destined for nodes inside the Home Network.



Required Traffic Cases



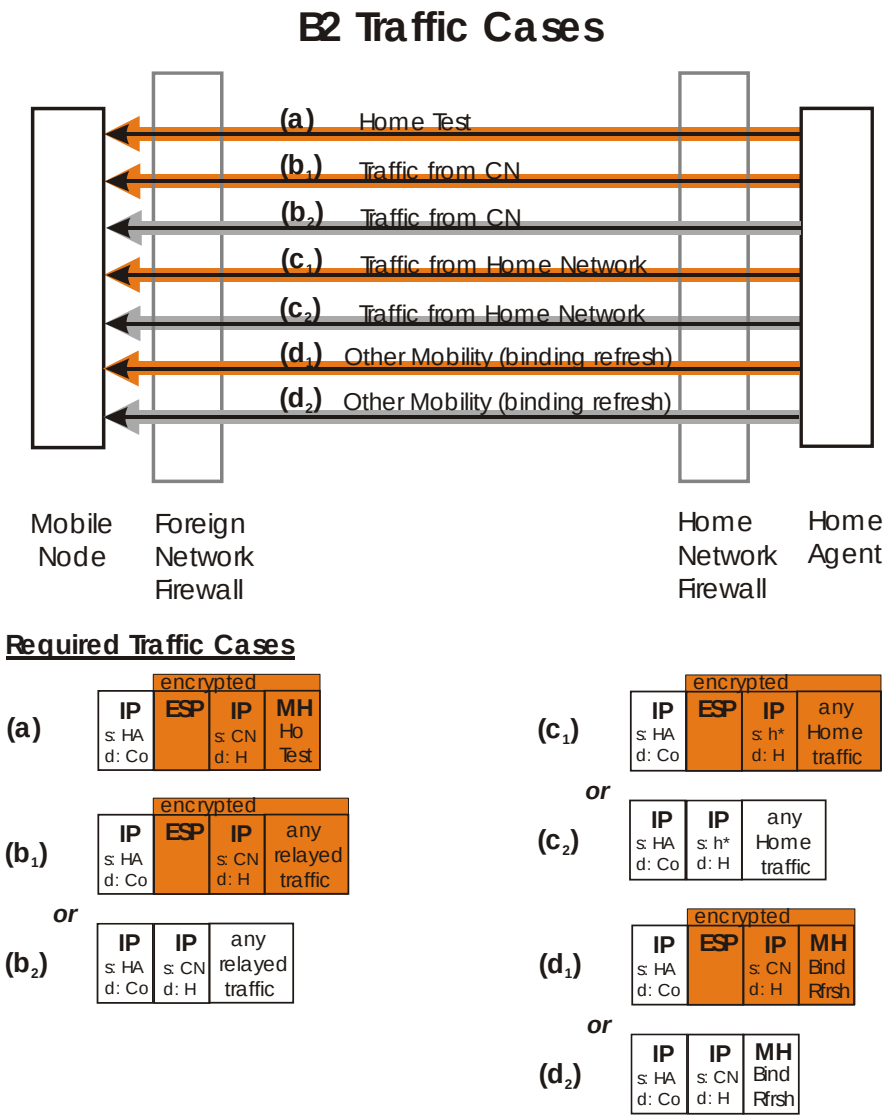
The B1 encrypted messages do not have the Home Address Destination Option as with the A1 cases. Tunnel-mode SAs bound to the care-of address are used here[13] and therefore must be automatically modified with each hop made by a mobile node to a new foreign link. Some IPsec implementations may not have this capability and should be avoided.

The choice between (B1-b_1 or B1-b_2) and between (B1-c_1 or B1-c_2) reflects the option in the standards that this traffic MAY be encrypted (i.e. it doesn't say MUST)[14].

B1-c_1 and B1-c_2 refers to traffic from the mobile node that is destined for nodes within Home Network rather than a Correspondent Network. Note that **h*** is used in the figures to indicate a destination address in the home network other than the home agent.

3.3 B2 Traffic Cases

The B2 set represents the tunneled packets sent by a home agent to a mobile node that is away from home. This is largely traffic in response to the B1 cases but in general can be any traffic that is addressed to the mobile node[15]. Neighbor Discovery traffic on the Home Network is serviced by the home agent on behalf of the mobile node, not forwarded to the mobile node.

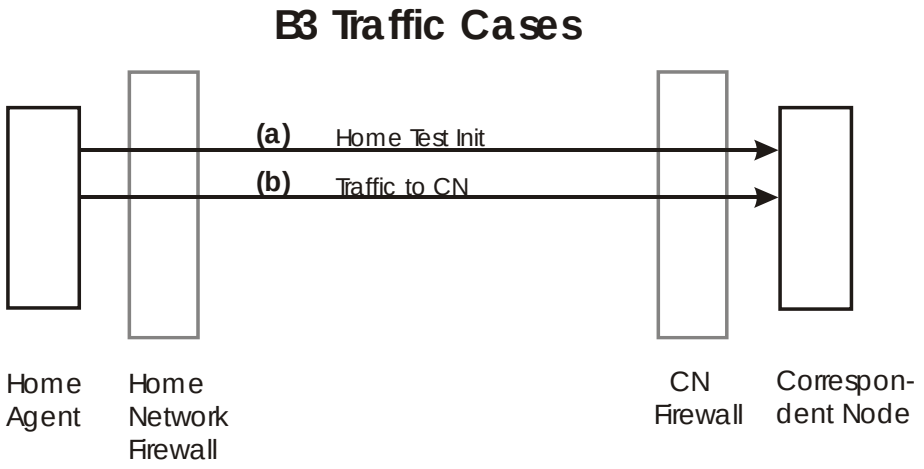


Mobile Prefix Advertisement messages can be in response to a Solicitation (B1 case), but can also be initiated by the home agent as an unsolicited Advertisement to inform a mobile node of new address information on the home link.

Binding Refresh messages are always sent to the home address since they are sent at a time when the state of the binding is uncertain[16]. Therefore, they can only appear here and not as C2 cases.

3.4 B3 Traffic Cases

These packets are the inner IP layer of the respective B1 tunnel cases. These packets exit the tunnels and are forwarded to the appropriate correspondent node.



Required Traffic Cases

(a)

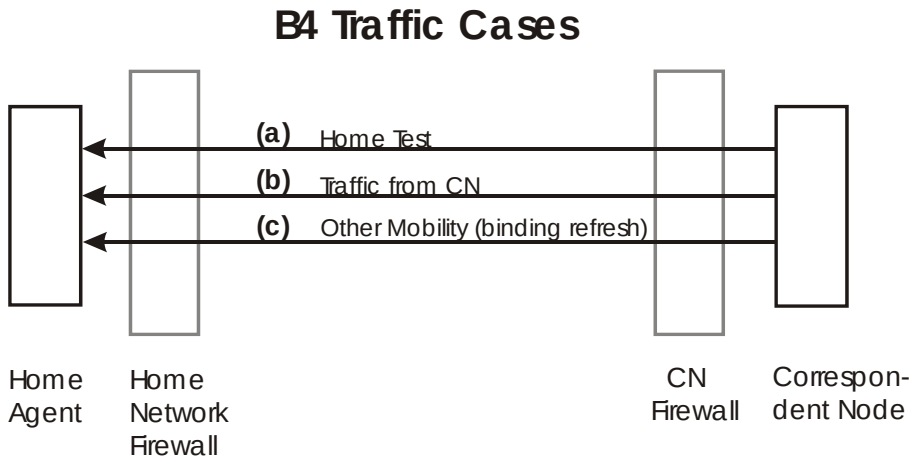
IP s: H d: CN	MH HoTI

(b)

IP s: H d: CN	any relayed traffic

3.5 B4 Traffic Cases

These packets become the inner IP layer of the respective B2 tunnel cases. These packets arrive from correspondent nodes and are tunneled to the mobile node whenever the mobile node is away from home and registered with the home agent.



Required Traffic Cases

(a)

IP	MH
s: CN d: H	Ho Test

(b)

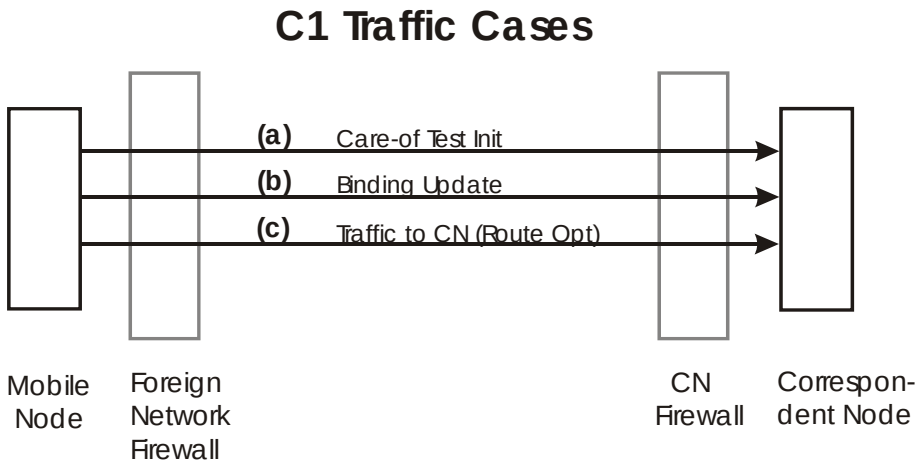
IP	
s: CN d: H	any relayed traffic

(c)

IP	MH
s: CN d: H	Bind Rfrsh

3.6 C1 Traffic Cases

The C1 set represents packets sent by a mobile node (while away from home) directly to a correspondent node.



Required Traffic Cases

(a)

IP	MH
s: Co d: CN	CoTI

(b)

IP	DO	MH
s: Co d: CN	Home Adr	BU H= 0

(c)

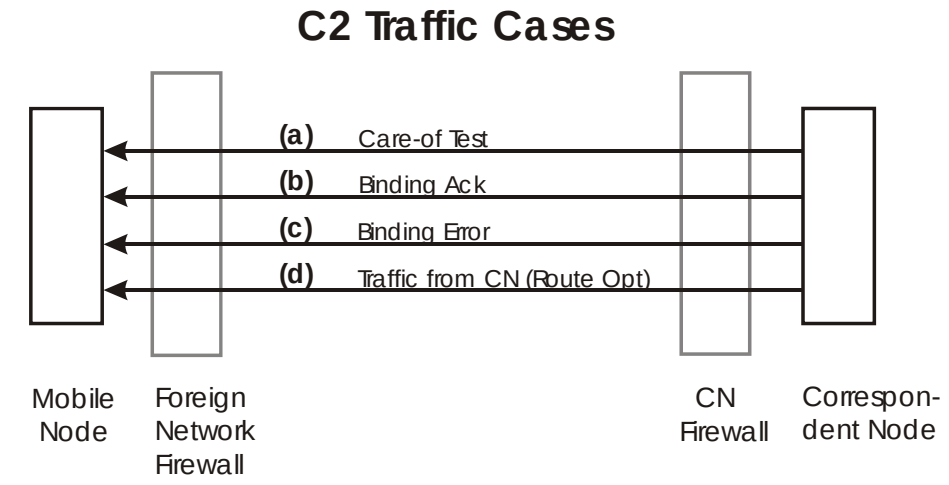
IP	DO	
s: Co d: CN	Home Adr	any traffic (Rt Opt)

Binding Updates (C1-b) to correspondent nodes must have the H flag=0.[17] This is an important characteristic for firewalls to detect because it distinguishes home agent registration from normal correspondent node registration.

An assumption is made here that when a mobile node is away from home, it will always use the Home Address Destination option to send binding updates directly to a correspondent node, whether for registration, extension, or deletion of a binding. Therefore these messages are shown here as C1-b and not as an option in the B1 to B3 path[18].

3.7 C2 Traffic Cases

The C2 set represents the packets sent by a correspondent node directly to a mobile node that is away from home. This is response traffic to the C1 cases.



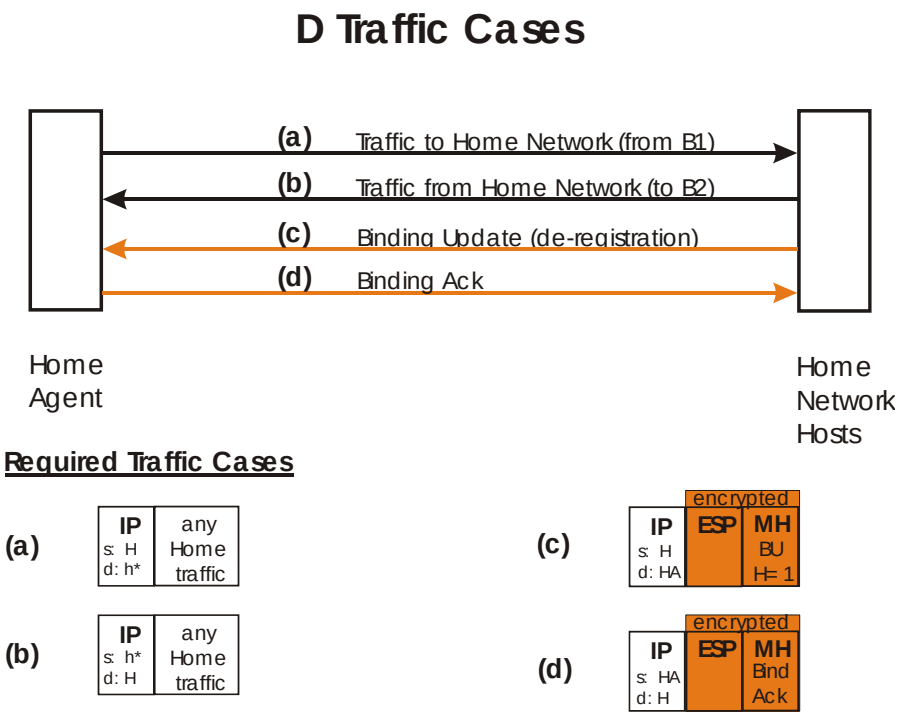
Required Traffic Cases

The Binding Ack message (C2-b) is the typical response to a Binding Update message and includes error reporting in which no binding is established. The Ack therefore is not always an acknowledgement of a successful binding operation.

The Binding Error message (C2-c) is primarily used to report attempts to use the Mobile IP Route Optimization without establishing the necessary binding first.

3.8 D Traffic Cases

The D cases represent the traffic between the home agent and the local Home Network. This traffic is not seen by any of the three firewalls discussed in this analysis but is identified for discussion purposes.

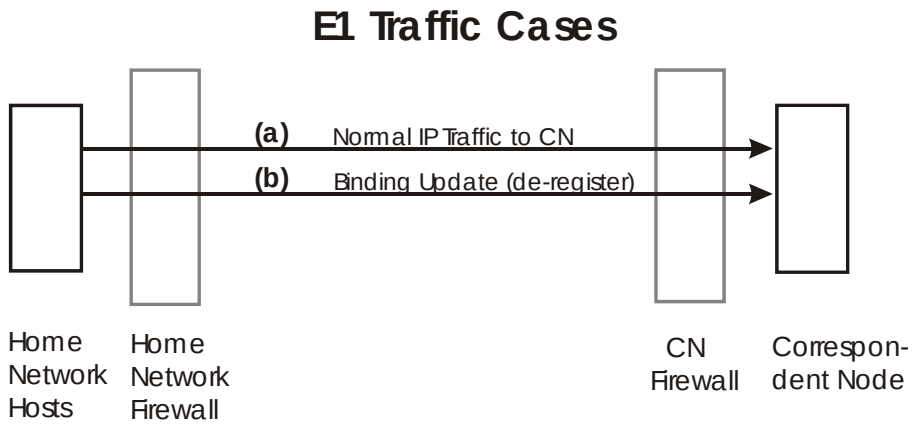


Case D-a represents traffic from the mobile node (while it is away from home) that exits the tunnel from case B1-c_1 or B1-c_2. Similarly, Case D-b traffic returns into the tunnel represented by B2-c_1 or B2-c_2.

Cases D-c and D-d represent the mobile node's de-registration process once it has returned home. At this time, the mobile node becomes part of the Home Network again and must command the home agent to stop acting on its behalf.

3.9 E1 Traffic Cases

The E1 cases represent the traffic sent by a mobile node (while at home) to a correspondent node.



Required Traffic Cases

(a) IP (s: H, d: CN) | any traffic

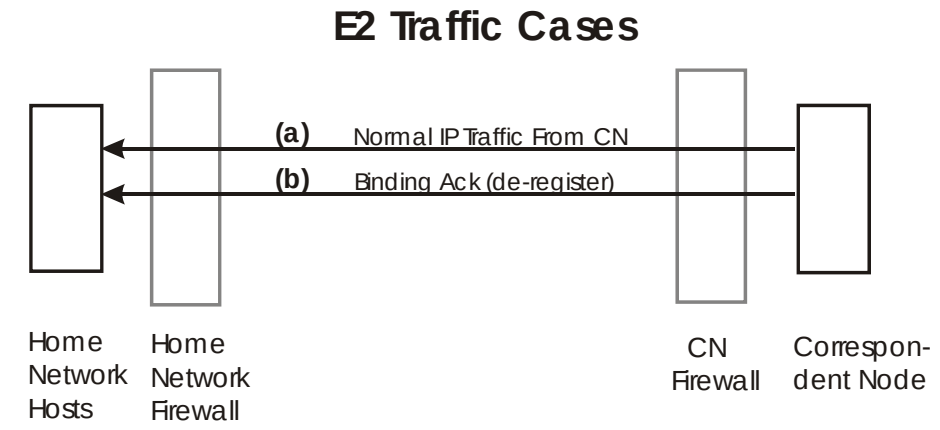
(b) IP (s: H, d: CN) | MH BU H=0

E1-a is normal (non-mobile) IP traffic.

Case E1-b refers to a Binding Update with a correspondent node that may be performed to de-register a binding once the mobile node has returned home.

3.10 E2 Traffic Cases

The E2 cases represent the traffic sent by a correspondent node to a mobile node that is presently at home.



Required Traffic Cases

(a)

IP s: CN d: H	any traffic

(b)

IP s: CN d: H	MH Bind Ack

E2-a is normal (non-mobile) IP traffic.

Case E2-b is the response to traffic E1-b used to confirm the de-registration of a binding.

4 Filtering Policies for Mobile IP

In this section, filtering policies are recommended for firewalls at each of the sites: Home Network, Foreign Network, and Correspondent Network. Combinations are also discussed, for example, a site may act as a Home Network for its own mobile users and as a Correspondent Network with respect to other networks' mobile users. Such a site needs to account for both types of traffic within a single firewall policy. Refer to Chapter 5 for a summary of each policy in pseudo-code format.

4.1 Home Network Only

As shown in Figure 1 (see section 1.2) inbound traffic to the Home Network firewall consists of traffic cases: A1, B1, B4, and E2. Firewall filtering rules at the Home Network must not drop any of this legitimate traffic.

Per section 2.1, the Home Network should be concerned about unauthorized home agents being set up by mischievous users. To prevent this, the firewall must be able to block at least one essential home agent packet from all nodes except the authorized home agents. The obvious choice is the Binding Update packet, which is needed to register (enable) the home agent for a given mobile node. As shown in the A1 traffic cases, valid Binding

Updates to the home agent are encrypted. The firewall can target packets containing both a Home Address Destination Option and ESP (encryption) header, and only allow this combination to legitimate home agents. This drops all Binding Updates (A1-c) and encrypted Mobile Prefix Solicitations (A1-d_1) going to unauthorized destinations in the Home Network. All other IPsec packets are unaffected since they do not contain a Home Address Destination Option.

Next, the firewall should drop any unencrypted binding updates[19]. The Mobile IP standards require binding updates to the home agent to be encrypted[20] but the Mobile IP code itself may not be able to enforce this requirement. IPsec is a separately specified function with a configurable security policy that determines what gets encrypted (or must be received encrypted). Once IPsec processing is complete (decrypt), the receiving application typically has no evidence of whether the packet was encrypted or not.

It isn't clear how (or if) an implementation (Mobile IP code) will guarantee that Binding Updates to the home agent are received encrypted. Will the IPsec design signal to the Mobile IP code that the packet was encrypted? Will the home agent application refuse to start if the IPsec policy is not properly configured? Or will Mobile IP blissfully carry out its processing of Binding Updates *assuming* that they have been properly decrypted through IPsec? This uncertainty is the reason for recommending that firewalls drop unencrypted Binding Updates as a precaution even though they technically aren't allowed by the standards. To protect against the unauthorized installation of home agents, it must be assumed that someone might try to deliberately set up a home agent without enabling the "required" encryption.

The B1 cases also present some security concerns to the Home Network. The standards allow an optional use of IPsec for the tunneled traffic as indicated by the choices (B1-b_1 or B1-b_2) and (B1-c_1 or B1-c_2)[21]. Furthermore, the nature of these packets presents unique problems for an IPsec design, namely that the care-of IP address is associated with the security policy database entry and the security association for the ESP header. A special solution is required to allow these characteristics to be updated and updated *only* in response to a secure Binding Update packet. Some implementations may not have the capability to protect this tunneled traffic with IPsec, and these implementations would still be technically compliant since that function is optional. Implementations that cannot protect the mobile node's tunneled traffic to the home agent should be avoided if at all possible.

The Mobile IP specification tries to make the case that unencrypted reverse tunnel traffic is made safe by requiring the home agent to check the source addresses of the inner and outer IP layers against the current binding for that mobile node[22]. It states: "This simple check forces the attacker to know the current location of the real mobile node and be able to defeat ingress filtering". Although this is true and does help to prevent just anybody anywhere from using a mobile node's tunnel, it misses the most likely avenue of attack. Instead of trying to attack a mobile node from some arbitrary point in the internet, attackers would more likely sit on a foreign link and wait for mobile users to arrive. Since the foreign link is (likely) wireless, it is easy for attackers to collect and inject packets using another's IP address[23]. The above check is defeated since the attacker does in fact "know the current location of the real mobile node"; it's on the same link as the attacker.

The attacker would allow the mobile node to set up the tunnel and then use it to reach the mobile node's Home Network (case B1-c_2) or some Correspondent Network that the attacker wouldn't normally be able to reach (case B1-b_2). The attacker might use this opportunity to reach restricted sites or conduct illegal activities, since it would appear to an observer that the legitimate mobile user was doing these things.

When the tunneled traffic to a home agent is not encrypted, the Home Network firewall should apply restrictions to this traffic. Most importantly, the firewall must greatly restrict the reachable destinations inside the Home Network. This traffic must be treated as if it were from an outsider. The attacker must not be allowed access to anything through the mobile node's tunnel that he wouldn't otherwise be able to reach on his own. This also restricts the real mobile node from reaching destinations on his/her own Home Network, but that is the price for not encrypting this traffic. The relayed traffic to other Correspondent Networks should also be filtered or monitored. This is harder to specify and may be more appropriate for an IDS to look for suspicious usage (i.e. mobile users visiting unauthorized sites etc...). A firewall needs the ability to filter tunneled (IP in IP) traffic to fulfill these security measures. If the firewall does not have this capability the filtering may be achievable on the home agent's inside interfaces[24].

Finally, since this section recommends filtering for a Home Network **only**, some measures may be wanted to prevent the site from being used as a Correspondent Network or Foreign Network.

The Correspondent Network activity is already thwarted by dropping unencrypted Binding Updates as recommended above. The firewall could also drop inbound Care-of Test Init packets, but this is probably better handled by disabling the Route Optimization functionality on inside servers and allowing the specified ICMP error message to be sent back to any mobile nodes attempting to set up a binding. Since the Binding Updates are dropped, the binding would not occur anyway. If there are IPv6 servers that do not allow Route Optimization to be disabled, it is better to drop the inbound Care-of Test Init and Home Test Init messages along with the Binding Updates[25].

Disabling Foreign Network characteristics from the Home Network may be wanted at a Home Network. These networks have a wireless access LAN to support the coming/going of their own mobile users, not other networks' mobile users using it as a hop. Of course, the link access control function is the first line of defense here, but the firewall can provide additional protection by specifically dropping traffic types of visiting mobile nodes. The Foreign Network characteristics can be disabled from the Home Network by dropping all inbound packets containing the Type 2 Routing Header and/or all outbound packets containing a Home Address Destination Option header. These packets, in this direction, only occur at a Foreign Network. These headers in the opposite direction must be allowed since they appear in A1 and A2 cases. These filtering rules will not disrupt the local mobile users that have returned home.

4.2 Foreign Network Only

The Foreign Network has no concerns with the Mobile Node's traffic other than verifying that the node is welcome there in the first place. This must be accomplished by some link access control feature and is not relevant to the firewall filtering strategy. As a Foreign

Network **only**, the firewall should prevent the site from being used as a Home Network or Correspondent Network.

The Home Network characteristics can be prevented by dropping all inbound packets containing a Home Address Destination Option. This rule applies regardless of whether the packet contains an ESP header or not. The firewall must also drop any unencrypted Binding Update messages[26].

Disabling the Correspondent Network characteristics is enforced by dropping the inbound unencrypted Binding Updates (above). Additionally, the site should drop inbound Care-of Test Init and Home Test Init messages if there are servers for which Route Optimization cannot be disabled.

4.3 Correspondent Network Only

The Correspondent Network receives inbound traffic cases B3, E1, and C1. The main concern is with case C1-c, which is traffic received via the Route Optimization method. Cases E1-a and B3-b appear to the Correspondent Network as normal IP traffic and there is no special handling required. In fact, as mentioned in section 2.3, the Correspondent Network will not be able to distinguish between cases E1-a and B3-b and therefore cannot know for sure if the mobile node is at home or away. The other cases are the necessary support traffic that must occur prior to case C1-c traffic being sent[27].

The unique Mobile IP format (case C1-c), must not be allowed to subvert the filtering performed on normal IP packets. More specifically, the packet now has a care-of address (WHERE) and a home address (WHO) instead of a single source IP address (WHO-WHERE) as in normal IP. As explained in section 2.3, the primary access control filtering should be based on the WHO that corresponds to the home address of the packet. For case C1-c, this means that a firewall would need to extract the home address out of the Home Address Destination Option and treat it as if it were the source address. The entire filtering rule set would then be applied to this altered data set[28]. Ideally, firewalls will offer this as an option, but in reality it may or may not yet be available. Filtering can also be done on the actual source address of the packet (i.e. the home address is not swapped in place of the source address), though it should be considered of secondary importance. Such filtering could be used to completely reject Foreign Networks that are known to be undesirable (i.e. in dangerous countries, known hacker sites, etc...).

Filtering on the home address (as if it were the source address) does not give attackers any special advantage beyond what they already have in normal IP. An attacker can always spoof a source address to pass a firewall filter. The difficulty is in getting the return traffic which goes to the real location of that spoofed IP address. Using case C1-c traffic, the attacker can still spoof a source via the Home Address Destination Option, and the Correspondent Network will refuse to send the return traffic. In this case, no return traffic is sent because there is no binding established which can only occur with the cooperation of the real Home Network. The risk is the same with C1-c and normal IP traffic.

First and foremost, the Correspondent Network should avoid dropping the C1-c traffic outright as an attempt to avoid mobile users if at all possible (e.g. do not drop all packets

containing a Home Address Destination Option). Mobile users will simply revert to the B3-b case and get through anyway.

If the present site security policy (for normal IP) requires no filtering on source addresses of incoming packets (i.e. everyone is treated equally) then Mobile IP case C1-c traffic is a "don't care" situation. The mobility header and Mobile IP specialty headers only serve swap out source addresses of inbound packets and these are not being filtered by the policy. This simple case requires no adjustment to the existing firewall policy.

If the present filter set *does* filter on source address to restrict access to some internal destinations, it may still be possible to avoid dealing directly with the C1-c packet case. If the source-sensitive filtering rules are purely to block certain source addresses and allow everything else through, this filtering rule will cause Home Test Init messages (B3-a) to be dropped thus rendering the corresponding (unwanted) C1-c packets useless. More likely they would never be sent[29]. Again, in this case, no adjustment to the existing firewall policy is necessary.

If the source-sensitive filtering rules allow only certain acceptable source addresses (with acceptable ports/protocols) through and block everything else, the approach above won't work because the C1-c packets of allowed users will be dropped. In this case, the best solution is to have a firewall that can automatically filter on the home address extracted from the Home Address Destination Option as discussed earlier. If no such firewalls are available, a work around would be to treat **all** packets with a Home Address Destination Option (i.e. C1-c packets) as if they had acceptable source addresses (i.e. filter the protocol/ports values), allow **all** Care-of Init Test messages through regardless of the source address, and drop all other packets that do not have an acceptable source address. This would still drop the Home Test Init messages from unwanted sites, thereby rendering useless any unwanted C1-c packets that get in. This is tolerable, but less than optimal since it allows some unwanted traffic to get in, only to be rejected by the Mobile IP processing on the servers. Refer to the pseudo-code representation of this logic in section 5.3 for a better understanding.

The scenarios above filter the Home Test Init messages to restrict mobile traffic from certain sources (home addresses) into the site or to specific destinations within the site. Packets from prohibited source addresses are dropped and packets from allowed source have all remaining filters applied (e.g. restrictions on protocols and ports). If a finer granularity is needed such that some allowed sources can use protocol/port set A and other allowed sources can use protocol/port set B, this **cannot be achieved** via the above Home Test Init filtering approach. The only alternatives here are to use a firewall that can extract/filter the home address from the Home Address Destination Option or to drop all traffic with the Home Address Destination Option present[30].

As a Correspondent Network **only**, it may be desirable to prevent the site from being used as a Home Network or Foreign Network.

The Home Network characteristics can be prevented by dropping any inbound encrypted packets containing a Home Address Destination Option and dropping any unencrypted Binding Update messages **with the H flag =1**. Note this additional constraint on the H flag from the rule in section 4.1 is needed to distinguish between the unwanted home registrations and the wanted correspondent registrations. These rules apply to all source addresses, therefore these packets would be dropped regardless of whether the real source address or extracted home address were filtered.

The typical Correspondent Network will likely **not** be concerned with the Foreign Network characteristics, since it probably doesn't have wireless access links. If the Correspondent Network *does* have wireless links, the protection against being used as Foreign Network is the same as in section 4.1. Drop all inbound packets containing the Type 2 Routing Header and/or all outbound packets containing a Home Address Destination Option header.

4.4 Combination Home Network and Correspondent Network

Most likely, a Home Network will also operate as a Correspondent Network for other networks' mobile users. That is to say, the Home Network has servers willing to participate in the Route Optimization method for remote mobile users.

This is largely a combination of filtering from sections 4.1 and 4.3 with a few changes. First, when dropping unencrypted Binding Update messages, only those with the H flag set to 1 can be dropped since the H=0 case is now a legitimate packet supporting correspondent node registration.

A new filtering action should be added to prevent the Home Network's own mobile nodes from (intentionally or accidentally) establishing correspondent-style bindings with nodes inside the Home Network. When a mobile node is away from home it should establish a binding with the home agent and tunnel (preferably an IPsec tunnel) traffic to the Home Network as shown in case B1-c_1 or B1-c_2. It should not be allowed to perform Route Optimization with inside servers. The reasons are that tunneling home is safer assuming IPsec is used and secondly the route optimization procedure is a lot of extra work for very little gain in this case (i.e. the tunnel home is already an optimal path for these destinations). Applying this filtering may vary depending on the capabilities of the firewall and home agent router. One good way to enforce this rule is to prevent any Home Test Init messages to inside nodes that are from locally owned home addresses.

See Figure 2 below. No such packet should be allowed to emerge from any of the case B1 tunnels. Another way of stating the same thing is to say that none of the case D-a packets can be a Home Test Init message. This filtering would have to be applied on the appropriate interface of the home agent.

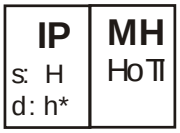


Figure 2: A Bad Home Test Init Packet

If the above Home Test Init filtering is not practical, a firewall with the ability to extract/filter the Home Address Destination Option could be used. In this case, drop any inbound packet with a home address that is a local home address **except** for packets destined for a legitimate home agent.

Real world scenarios may contain more complexity at the Home Network and may require the filtering recommendations in this document to be adjusted accordingly. For example, no attempt is made here to show users and servers segregated by a DMZ. The goal of this document is to identify the basic security concerns with respect to the reference system shown in Figure 1, and assume that administrators can adapt the filtering to their own situation.

4.5 Combination Home Network, Correspondent Network, and Foreign Network

This scenario is the same as 4.4 above except that no action is taken to disable the Foreign Network traffic. Everything else is the same.

4.6 Combination Foreign Network and Correspondent Network

This scenario is the same as 4.3 above except that no action is taken to disable the Foreign Network traffic. Everything else is the same.

5 Filtering Policy Configuration Summaries

Each filtering policy from Chapter 4 above is summarized below in a pseudo-code format for clarity. The pseudo-code should be considered an ordered list of actions, hence an action to "drop all packets of type X" means all remaining packets not already dropped by previous actions in the list.

5.1 Summary: Home Network Only

```
Inbound Filtering:
        If Dest IP address < > authorized home agent, Then
                If packet contains: a Home Address Destination Option header AND an ESP
                header, Then Drop packet
                Endif
        Endif
        Drop all packets containing a Mobility Header with a Binding Update message.
        If Mobile IP tunneled traffic is unencrypted (i.e. B1-b2 and B1-c2) Then
                Filter traffic to the Home Network (B1-c2) in the same manner as traffic
                from an untrusted outsider.
                Filter (or monitor via IDS) all relayed traffic (B1-b2) for suspicious
                activity and unauthorized destination sites.
                (Filtering may need to be done on a home agent router's interface if the
                firewall cannot filter inside tunnels.)
        Endif
(opt)   If there are reachable IPv6 destinations inside the Home Network that can not
        be configured to disable Mobile IP Route Optimization, Then
                Drop all packets to these destinations containing a Mobility Header with a
                Care-of Test Init message
                Drop all packets to these destinations containing a Mobility Header with a
                Home Test Init message
                (This filtering is optional, but will prevent inside servers from wasting
                resources on these messages.)
        Endif
        Drop all packets containing a Type 2 Routing Header[B]

Outbound Filtering:
        Drop all packets containing a Home Address Destination Option header[B]
```

5.2 Summary: Foreign Network Only

```
Inbound Filtering:
        Drop all packets containing a Home Address Destination Option. (applies
        whether or not an ESP header is present)
        Drop all packets containing a Mobility Header with a Binding Update message.
 (opt)  If there are reachable IPv6 destinations inside the Foreign Network that can not
        be configured to disable Mobile IP Route Optimization, Then
                Drop all Care-of Test Init messages
                Drop all Home Test Init messages
                (This filtering is optional, but will prevent inside servers from wasting
                resources on these messages.)
        Endif

Outbound Filtering:
        (None)
```

[B] Both of these are recommended, though either one is sufficient to disable Foreign Network functionality.

5.3 Summary: Correspondent Network Only

For simplicity, the word "SWAP" is used below to refer to the function discussed in section 4.3, where a firewall exchanges the source IP address with the home address contained in the Home Address Destinations Option and applies all filtering to this new data set. The term "Non-SWAP" is used to refer to a special filtering rule defined by the firewall to apply to the real source address when the Home Address Destination Options header is present. These are proposed firewall capabilities and may or may not exist in any particular product at this time.

```
Inbound Filtering:
        Drop all packets containing a Home Address Destination Option header AND an
        ESP header.
        Drop all packets containing a Mobility Header with a Binding Update message
        that has the H flag =1.
        If filtering for normal IP is dependent on source addresses, Then
                If filtering is of the form: "drop all traffic from Set_A sources and
                filter protocol/ports on the rest", Then
                        Done (no changes required for C1-c packets)
                Elseif filtering is of the form: "filter protocol/ports on all traffic
                from Set_A sources and drop the rest", Then
                        If firewall can SWAP, Then
                                Drop all packets from unwanted Foreign Sites using Non-SWAP
                                rules
                                Enable SWAP and filter protocol/ports on Set_A, drop all
                                non-Set_A.
                        Else (no firewall has SWAP)
                                Assume any packet containing a Home Address
                                Destination Option header is in Set_A. Filter
                                protocol/port.
                                Allow any packet containing a Mobility Header with a
                                Care-of Test Init message to pass through
                        Endif
                Elseif filtering is of the form: "filter protocol/ports 1 on Set_A
                sources, protocol/ports 2 on Set_B sources, etc... , Then
                        If firewall can SWAP, Then
                                Drop all packets with source address from unwanted Foreign
                                Sites using Non-SWAP rules
                                Enable SWAP and filter protocol/ports 1 on Set_A,
                                protocol/ports 2 on Set B etc...
                        Else (no firewall has SWAP)
                                Drop all packets with a Home Address Destination Option.
                                (This is scenario cannot be met with traditional firewall
                                capability and the only option is to drop the C1-c packets)
                Endif (no more filtering forms)
        Else (filtering for normal IP is not dependent on source addresses)
                Done (no changes required for C1-c packets)
        Endif

        Drop all packets containing a Type 2 Routing Header[C]

Outbound Filtering:
        Drop all packets containing a Home Address Destination Option header[C]
```

[C] Both of these are recommended, though either one is sufficient to disable Foreign Network functionality.

5.4 Summary: Combination Home Network and Correspondent Network

The terms "SWAP" and "Non-SWAP" are defined in the first paragraph of section 5.3.

```
Inbound Filtering:
        If Dest IP address < > authorized home agent, Then
                If packet contains: a Home Address Destination Option header AND an ESP
                header, Then Drop packet
                Endif
        Endif
        Drop all packets containing a Mobility Header with a Binding Update message
        that has the H flag =1.
        If Mobile IP tunneled traffic is unencrypted (i.e. B1-b2 and B1-c2) Then
                Filter traffic to the Home Network (B1-c2) in the same manner as traffic
                from an untrusted outsider.
                Filter (or monitor via IDS) all relayed traffic (B1-b2) for suspicious
                activity and unauthorized destination sites.
                (Filtering may need to be done on a home agent router's interface if the
                firewall cannot filter inside tunnels.)
        Endif
        Drop any B1-c1 or B1-c2 packets containing a Mobility Header with a Home
        Test Init message (do not drop B1-b1 or B1-b2 with this message)[D]
        If filtering for normal IP is dependent on source addresses, Then
                If filtering is of the form: "drop all traffic from Set_A sources and
                filter protocol/ports on the rest", Then
                        Done (no changes required for C1-c packets)
                Elseif filtering is of the form: "filter protocol/ports on all traffic
                from Set_A sources and drop the rest", Then
                        If firewall can SWAP, Then
                                Drop all packets from unwanted Foreign Sites using Non-SWAP
                                rules
                                Enable SWAP and filter protocol/ports on Set_A, drop all
                                non-Set_A.
                        Else (no firewall has SWAP)
                                Assume any packet containing a Home Address
                                Destination Option header is in Set_A. Filter
                                protocol/port.
                                Allow any packet containing a Mobility Header with a
                                Care-of Test Init message to pass through
                        Endif
                Elseif filtering is of the form: "filter protocol/ports 1 on Set_A
                sources, protocol/ports 2 on Set_B sources, etc... , Then
                        If firewall can SWAP, Then
                                Drop all packets with source address from unwanted Foreign
                                Sites using Non-SWAP rules
                                Enable SWAP and filter protocol/ports 1 on Set_A,
                                protocol/ports 2 on Set_B etc...
                        Else (no firewall has SWAP)
                                Drop all packets with a Home Address Destination Option.
                                (This is scenario cannot be met with traditional firewall
                                capability and the only option is to drop the C1-c packets)
                Endif (no more filtering forms)
        Else (filtering for normal IP is not dependent on source addresses)
                Done (no changes required for C1-c packets)
        Endif

        Drop all packets containing a Type 2 Routing Header[E]

Outbound Filtering:
        Drop all packets containing a Home Address Destination Option header[E]
```

[D] Other filtering methods may be used to achieve the goal: prevent local Mobile users from using Route Optimization with their own home networks.

[E] Both of these are recommended, though either one is sufficient to disable Foreign Network functionality.

5.5 Summary: Combination Home Network, Correspondent Network, and Foreign Network

The recommended filtering policy for all three network types together is the same as what is listed in section 5.4 **except** for the last two rules that are marked by the footnote E. These rules must be deleted to allow the Foreign Network traffic, all else remains the same:

Delete from Inbound rules:

```
Drop all packets containing a Type 2 Routing Header
```

Delete from Outbound rules:

```
Drop all packets containing a Home Address Destination Option header
```

5.6 Summary: Combination Correspondent Network, and Foreign Network

The recommended filtering policy this combination is the same as what is listed in section 5.3 **except** for the last two rules that are marked by the footnote C. These rules must be deleted to allow the Foreign Network traffic, all else remains the same:

Delete from Inbound rules:

```
Drop all packets containing a Type 2 Routing Header
```

Delete from Outbound rules:

```
Drop all packets containing a Home Address Destination Option header
```

Endnotes

[1] "Mobility Support in IPv6"; RFC 3775; Johnson, Perkins, Ericsson; June 2004
[2] "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents"; RFC 3776; Ericsson, Devarapalli, Dupont; June 2004
[3] Note the terms "ingress filtering" and "egress filtering" are used inconsistently amongst various authors even though they are typically referring to the same thing. Here, as in most cases, the filtering refers to checks that source addresses of packets heading toward the larger internet are of a limited set of valid possibilities. Edge networks would probably call this egress filtering whereas ISPs like to call this ingress filtering (from their customers).
[4] The hierarchical scheme used to distribute IPv6 address prefixes has changed several times via superceding standards (RFCs). First there was a portion of space that would be distributed geographically, then there was a loosely defined TLA/NLA structure, now (via RFC 3587) there is a "global routing prefix" that gets assigned by "Regional Internet Registries (RIR)". The degree to which a physical location in the world can be associated with an IPv6 address keeps changing and one should consult the latest RFCs to get the latest information.
[5] Chapter 6 of RFC 3775 contains the detailed specification of each of these header types.
[6] The specification actually calls it the "Payload Proto" field, uniquely nonconforming with the basic precedent set for IPv6 extension header specification.
[7] RFC 3775, section 5.1, para 1
[8] RFC 3775, section 11.7.1, para 3, bullet 3 for registration and extension. For de-registration while away from home we assume that the Home Address Destination Option is also present per section 10.3.2, para 2, implying that the option **may** not occur if the mobile is at home (which is contained in our case D)
[9] RFC 3775, section 11.4.2, para 2
[10] RFC 3775, section 10.6.3, para 1, bullet 4
[11] Note that the text in RFC 3775, section 10.6.3, paragraph 1 bullet 2 is confusing. It states that the destination address will be the mobile node's home address when the Prefix Discovery Reply is unsolicited. This, however, (we believe) would get adjusted with the application of the routing header such that the final packet has the care-of address as destination and the home address in the RH.
[12] An unencrypted message with the home address and the wrong care-of address would probably cause a Binding Error before it gets rejected by any IPsec policy. Also a message (encrypted or not) with a Mobility Header that has an unknown Type field would cause a Binding Error.
[13] RFC 3776, section 3.2. See also RFC 3775, sections 10.4.6 and 11.6.3. Note that the language in RFC 3775 is less resolute. For example, paragraph 3 of 10.4.6 states that this protection SHOULD be used whereas paragraph 1 already said it MUST be available (so why not use it?). We assume that it will be used.
[14] RFC 3775, section 10.4.5, para 1, bullet2 and RFC 3776, section 4.1, bullet 6.
[15] Since a mobile node is typically the client, most communications are initiated as B1 cases and returned as B2 traffic, but other patterns are possible and allowable such as peer-to-peer networking whereby another user contacts the mobile node.
[16] RFC 3775, section 9.5.5, para 2
[17] RFC 3775, section 6.1.7, Home Registration (H) bit. See also section 10.3.1, para 2 and para 3, bullet 1
[18] This is vaguely supported by the Figure in section 5.2.6 of RFC 3775. It should be noted, however, that there are no requirements in RFC 3775 that would prevent these messages from being tunneled through the home agent, nor are there any requirements that would prevent them from being accepted by the correspondent node in that manner. In other words, sections 11.7.2 and 9.5.1 are flexible enough to allow tunneled Binding Updates though there is no indication that this is the intended method of operation.
[19] Note that dropping *all* unencrypted Binding Updates here is under the assumption that this is a Home Network *only* and not a combination of Home Network and Correspondent Network. In the latter case, only unencrypted Binding Updates with the H flag =1 should be dropped, i.e. only home agent registrations.
[20] RFC 3775, section 5.1, para 1
[21] RFC 3776, section 1, para 4 and section 4.1 bullet 6
[22] RFC 3775, section 10.4.5, para 1, bullet 3
[23] We are assuming that there is no wireless link layer security present.
[24] "Inside interfaces" refers to any interfaces through which the decapsulated traffic passes. Filtering here would not encounter the outer tunnel layer.

[25] RFC 3775, section 8.1, para 1 states that support for Route Optimization by a correspondent node is optional, though it is not a requirement to have a configurable on/off setting for this. Implementations may or may not have a configurable Route Optimization enable setting.
[26] Binding Updates can occur without a Home Address Destination Option (i.e. a de-registration operation), hence the first rule should not be relied on to cover these messages.
[27] Without the support packets, a server will drop the C1-c packets via mandatory Mobile IP packet processing
[28] "altered data set" here means that the firewall is altering the packet data for filtering purposes, but is not changing the actual packet that gets forwarded.
[29] RFC 3775, section 9.4.1, states that a Home test Init messages MUST NOT contain a Home Address Destination Option; therefore it must be sent with the home address as the source.
[30] Dropping all Route Optimization traffic (case C1-c), is listed here as the last resort. It works, it's easy, and it still allows mobile users to get through via reverse tunneling, but it would seriously hamper the deployment of optimized Mobile IP if everyone did this.