NAT Working Group
INTERNET-DRAFT
Category: Informational
Expire in six months

NEC USA
Jeffrey Lo
K.Taniguchi
November,1998

IP Host Network Address (and Port) Translation
<draft-ietf-nat-hnat-00.txt>

Status of this Memo

Abstract

Network Address Translation has become a popular technique that allows private addresses unregistered with Internet Assigned Number Authority (IANA) to be used by organizations within a private routing realm. These private addresses must not be advertised in the public Internet. Hence network address translator (NAT) are placed at the private routing realm border to translate private addresses to globally unique addresses and vice versa before packets are exchanged between the disparate routing realms. These modifications of the packet header by the NAT cause problems with the use of end-to-end security protocols such as IPSec and DNSSEC because network address translation does exactly what the security protocols are trying to prevent.

Host Network Address Translation (HNAT) and Host Network Address Port Translation (NAPT), on the other hand, enable end hosts to carry out address (and port) translations before applying security algorithms. To make dynamic HNAT and HNAPT possible, three conditions are essential. First, there must exist a way for end hosts to discover the IP address of Host-NA(P)T-Server. Second, there must be a way for externally destined packets to be routed in the private domain between the Host -NA(P)T-Client and Host-NA(P)T-Server. Lastly, Host-NA(P)T-Client must

be able to obtain an address (and port) binding from the Host-NA(P)T
-Server dynamically. This draft aims to address these issues to a

considerable extent. Methods suggested are by no means exhaustive in coverage and implementation specifics may vary from vendor to vendor.

1. Introduction

NAT itself takes several flavors, including traditional NAT (basic NAT and Network Address Port Translation (NAPT)), Two-way NAT, Twin NAT, Host NAT and Host NAPT [1]. Traditional NAT only allows outbound session from private to public domains. While basic NAT uses one to one mapping at the private domain border, NAPT allows many private addresses to one global address mapping by utilizing transport level port information, e.g. TCP port and UDP port [2]. In addition to outbound session, two-way NAT also enables inbound session from public to private network. Twin NAT are used in cases when there is an overlap of address assignment between the disparate domains by changing both the source and destination fields. Host NAT and NAPT allow network address (and port) translation to be done by the Host-NA(P)T-Client hence eliminating the traditional NAT limitation of having to do the translation at the border of the private realm.

By using host NAT and NAPT, communicating host are able to exercise end to end security by doing the address (and port) translation before applying security mechanism. This solves the problem of using security mechanisms such as IPSec and DNSSEC in NAT environment. Applications relaying IPv4 addresses and port information in the payload of their messages may find HNAT a valuable alternative to having application specific application-level-gateway (ALG) on the NAT.

In a static HNAT and HNAPT environment, each host-NA(P)T-client needing to establish end-to-end sessions with an entity outside the private routing realm are statically assigned global addresses (and port). After performing the necessary address (and port) translation, packets are tunneled to the Host-NA(P)T-Server by encapsulating it within an internally addressed header. Host-NA(P)T-Server removes the tunneling header before forwarding the packet to the external realm.

In a dynamic environment, in addition to the requirement of routing externally destined packets within the private domain which could be handled by tunneling as proposed in [1], Host-NA(P)T-Client must be able to discover IP addresses of Host-NA(P)T-Servers attached to the private realm. This information could be manually or automatically configured. A scheme has to be devised for automatic configuration to be possible. Host-NA(P)T-Client must also be able to obtain an address (and port) binding from the Host-NA(P)T-Server dynamically through a light weight protocol that enables not only address but port negotiation. We propose Dynamic Bindings Acquisition Protocol (DBAP) to serve this purpose.

2. Terminology

Address Manager
An entity responsible for global address and port assignment to Host-

NAT-Client. The address manager also maintains a private-global address and port mapping of all bindings and other related parameters such as maximum leased time of the binds.

External Entity
An entity physically located within a globally unique routing realm.

Global Address
A globally unique address assigned by Internet Assigned Number Authority (IANA).

Private Address
Addresses used in a private routing realm which are not registered with IANA. Typically but not necessarily, these addresses are within the Range 10.0/8, 172.16/12 and 192.168/16 assigned by IANA. If addresses Other than the range above were used, twin NAT would have to be deployed at the border.

Host-NAT-Client
A host in private network that adopts an address in external realm when connecting to hosts in that realm to pursue end-to-end communication

Host-NAPT-Client
A host in private network that adopts an address in the external realm and port assigned by the address manager when connecting to hosts in that realm to pursue end-to-end communication

Host-NAT-Server
A node that is resident on both private and external realms that can facilitate routing of external realm packets within private realm.

Host-NAPT-Server
A node that is resident on both private and external realms that can facilitate routing of external packets within private realm. In addition, Host-NAPT-Server does one to many mapping of a global address to multiple private address by manipulating transport layer port information.

Inbound Session
A communication session initiated by an external entity.

Outbound Session
A communication session initiated by a Host-NAT-Client.

3. Overview of Dynamic HNAT

In a HNAT environment where global addresses are dynamically assigned, host-NAT-clients obtain global address assignment from the address manager when communication needs to be establish with an

external entity. This address manager may or may not reside on the host -NAT-server. Such a mechanism for dynamically obtaining private to

global address binding is discussed in Section 5. After obtaining a global address assignment, all communications between the two entity use globally unique addresses and would requires no translation by intermediary process.

Certain routing mechanism would be required to route the end-to-end packets within private realm. Such a routing is usually facilitated by the Host-NAT-Server. Two approaches are defined in [1] which are repeated here. One approach would be to embed the packet within an IP packet such that the outer packet is addressed between the Host-NAT -Client's private address and the external peer. Hence NAT router in between could provide transparent routing of the outer packet by translating the outer IP header en-route. A second approach would be to embed the end-to-end packet inside a tunnel while traversing in the private network, such that the tunnel is addressed between Host-NAT -Client's private address and a router resident on both realms.

A Host-NAT-Client has the following characteristics.

1. Aware of the realm to which its peer nodes belong.

2. Assumes an address from external realm when communicating with hosts in that realm. Such an address may be assigned statically or in the case of dynamic HNAT, obtained dynamically from the address manager.

3. Route packets to external hosts using an approach amenable to Host-NAT-Server. In all cases, Host-NAT-Client will likely need to act as a tunnel end-point, capable of encapsulating end-to-end packets while forwarding and decapsulating in the return path.

A Host-NAT-Server has the following characteristics.

1. May be configured with address manager to assign address from external realm to Host-NAT-Client either statically or dynamically.

2. Must be a router resident on both the private and external routing realms.

3. Must be able to provide a mechanism to route external realm packets within private realm. Of the two approaches described, the first approach requires Host-NAT-Server to be a NAT router providing transparent routing for the outer header. This approach requires the external peer to be a tunnel end point.

   With the second approach, a Host-NAT-Server could be any router that can be a tunnel end-point with Host-NAT-Clients. It would detunnel end-to-end packets outbound from Host-NAT-Clients and forward to external hosts. On the return path, it would locate Host-NAT-Client tunnel, based on the destination address of the end-to-end packet and

encapsulate the packet in a tunnel to forward to Host-NAT-Client.

4. Overview of HNAPT

HNAPT is similar to HNAT by allowing Host-NAPT-Client to do network and port translation on behalf of Host-NAPT-Server. Many to one mapping is possible by allowing multiple private addresses to share a single global address, multiplexed base on transport identifiers such as TCP/UDP port numbers and ICMP Query Ids.

Host-NAPT-Clients are identified by a tuple of both address and port assignment. Methods discussed in the previous section could be used to route HNAPT packets within the private routing realm. Since a combination of destination address and transport identifier are used by Host-NAPT-Server to identify Host-NAPT-Client, confidentiality provided by security mechanisms that hide the transport identifier cannot be permitted to work with HNAPT, although authentication and integrity can be attained. Host-NAPT-Client would need to be able to acquire a port or range of port binding from the Host-NAPT-Server. Such requirement could be satisfied by DBAP discussed in section 5.

5. Dynamic Binding Acquisition Protocol (DBAP)

Dynamic Binding Acquisition Protocol (DBAP) provides a way for Host-NA(P)T-Client to dynamically acquire a private address to global address (and port) binding from the address manager. While Port Distribution Protocol (PDP) proposed in [4] solves the issue of dynamic port assignment, the scheme focuses mainly on small-scale implementation of NAT where only a single global unique address is managed by the NAT device. This IP address is also assumed to be static or not to change frequently. Hence there is no way to resolve unique address assignment using PEP, which is fundamental when more than one global address is managed by the address manager. Hence DBAP is introduced as a more generic protocol that enables both dynamic address and port assignment. DBAP request and response could be carried as ICMP type or over TCP or UDP. Six message types are defined at this moment. More message types and functionality will be introduced as the scheme progresses toward a more mature stage of development.

Extension of DBAP to Twin NAT environment will be studied and added in Later version of Internet Draft.

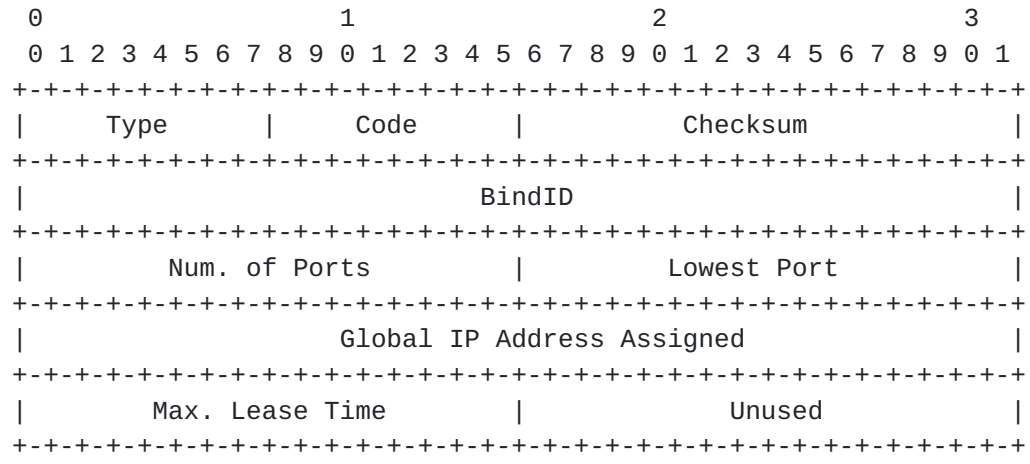
The table below describes the direction of the message :

Message Type	Direction
Assign Request	Host-NAT-Client -> Host-NAT-Server
Assign Response	Host-NAT-Server -> Host-NAT-Client
Free Request	Host-NAT-Client -> Host-NAT-Server
Free Response	Host-NAT-Server -> Host-NAT-Client
ERROR Response	Host-NAT-Server -> Host-NAT-Client

End Notification Host-NAT-Server -> Host-NAT-Client

5.1 ASSIGN REQUEST

Assign Request is used by Host-NA(P)T-Client for requesting a global address (and port) assignments from the Address Manager. In cases when multiple global addresses are required, multiple assign request each with a different BindID [5] must be sent. If an ASSIGN RESPONSE corresponding to an ASSIGN REQUEST is not received from the Host-NA(P)T-Server, Host-NA(P)T-Client may issue another ASSIGN REQUEST with the same BindID after a default timeout, the ASSIGN-WAIT time. Host-NA(P)T-Server receiving more than one successful ASSIGN REQUEST with the same BINDID should discard the subsequent requests and response with ASSIGN RESPONSE. Format of the message is shown below.

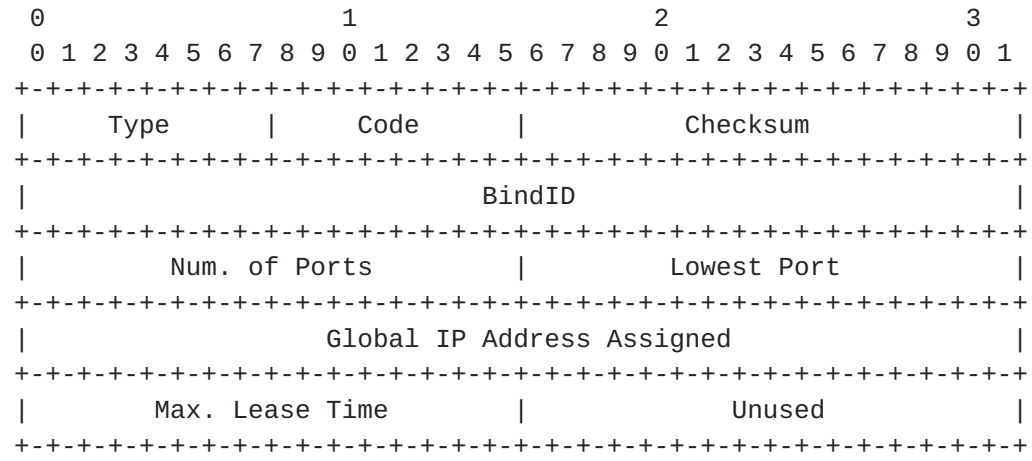


ASSIGN REQUEST Format

Type : to be defined
Code : 0
Checksum : 16-bit 1's complement of the 1's complement sum of the entire request. The checksum itself is set to 0 during computation.
BindID : A randomly generated value in the range 0x1 to 0xFFFFFFFF by Host-NA(P)T-Client during first ASSIGN REQUEST pertaining to a BIND. This value should be included in every DBAP exchanged pertaining to that BIND and would be maintained by the Host -NAT-Server as a binding identifier.
Num. of Port : Number of port requested. This field is 0 when no port Translation is used.
Lowest Port : Must be set to 0
Global IP Address Assigned : Must be set to 0
MaxLeaseTime : Maximum time interval in second that Host-NAT-Client wishes the Host-NAT-Server to reserve the BIND. This value should be 0 if it is not used.
Unused : Must be set to 0.

5.2 ASSIGN RESPONSE

ASSIGN RESPONSE is used to inform requesting Host-NA(P)T-Client of the newly assigned global address, port and other parameters related to the assignment.



ASSIGN RESPONSE Format

Type : to be defined
Code : 1
Checksum : 16-bit 1's complement of the 1's complement sum of the entire request. The checksum itself is set to 0 during computation.
BindID : BINDID of the ASSIGN REQUEST that this response corresponds to.
Num. of Ports : Total number of ports allocated to the host, when no port translation is used, this field must be zero.
Lowest Port : Lowest port number allocated in the block, when no port translation is used, this field must be zero.
Global IP Address Assigned : This field contains the global IP address assigned by the NAT device. Even if only one global address is managed by the Host -NA(P)T-Server, this field must be filled with that address.
MaxLeaseTime : Maximum time interval Host-NAT-Server allocates for this BIND. This value should be 0 if it is not used.
Unused : Must be 0

In case of port translation, Address manager is free to allocate a number of port less than that requested by Host-NAT-Client. At the same time, Host-NAT-Server is free to allocate a smaller lease time than that requested.

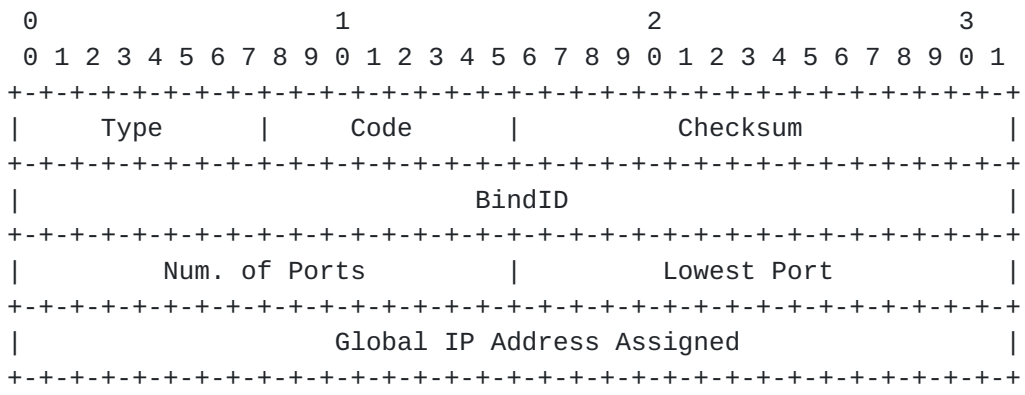
5.3 FREE REQUEST

FREE REQUEST is used by Host-NAT-Client to free an address or port

assignment. If a FREE RESPONSE corresponding to a FREE REQUEST is not received from the Host-NA(P)T-Server, Host-NA(P)T-Client may issue

another FREE REQUEST with the same BindID, address and port information after a default timeout, the FREE-WAIT time. Host-NA(P)T-Server receiving a valid FREE REQUEST for a bind should convert the bind to FIN-WAIT state and wait for a FIN-WAIT time interval before releasing the bind. Host-NA(P)T-Server receiving more than one FREE REQUEST with the same BINDID, address and port information during the FIN-WAIT interval should discard the subsequent requests and reply with FREE RESPONSE. FIN-WAIT interval should be greater than FREE-WAIT interval.

Host-NAPT-Clients are able to free a subset of the port range reserved. Port ranges not freed should be freed by subsequent FREE REQUEST or would be deleted when Maximum Lease Time elapses. If Host-NAT-Clients try to free a port range that exceeds the range of the bind, Host-NAT -Server must return ERROR RESPONSE with error code Incorrect Port Range and keeps the bind intact. Although BDAP does support subset port range release, we do not recommend this practice since it would greatly complicate Host-NAT-Server side implementations.

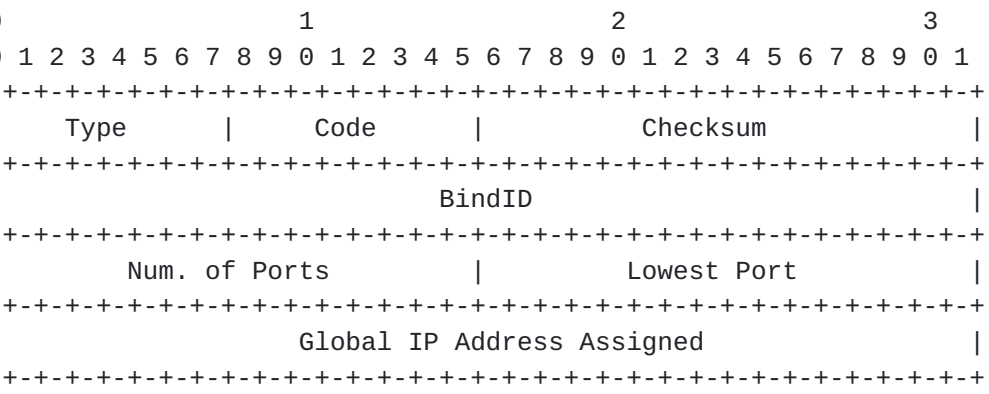


FREE REQUEST Format

Type : to be defined
Code : 2
Checksum : 16-bit 1's complement of the 1's complement sum of the entire request. The checksum itself is set to 0 during computation.
BindID : BINDID of the ASSIGN REQUEST that this request corresponds to.
Num. of Ports : Total number of ports in the block to be freed, when no port translation is used, this field must be zero.
Lowest Port : Lowest port number in the block to be freed, when no port translation is used, this field must be zero.
Global IP Address Assigned : Global address to be freed

5.4 FREE RESPONSE

FREE RESPONSE must be sent by Host-NA(P)T-Server for every valid FREE REQUEST processed.



FREE RESPONSE Format

Type : to be defined
Code : 3
Checksum : 16-bit 1's complement of the 1's complement sum of the entire request. The checksum itself is set to 0 during computation.
BindID : BINDID of the ASSIGN REQUEST that this response corresponds to.
Num. of Ports : Total number of ports in the block freed, when no port translation is used, this field must be zero.
Lowest Port : Lowest port number in the block freed, when no port translation is used, this field must be zero.
Global IP Address Assigned : Global address freed by Host-NA(P)T-Server.

5.5 ERROR RESPONSE

ERROR RESPONSE are sent by Host-NA(P)T-Server to Host-NA(P)T-Client in response to any error conditions that my arise.

ERROR RESPONSE Format

Type : to be defined
Code : 4
Checksum : 16-bit 1's complement of the 1's complement sum of the entire request. The checksum itself is set to 0 during computation.
BindID : BINDID of the ASSIGN REQUEST that this response corresponds to.
Error Code : Reason for the Error. Vendor specific error codes could be

introduced.

Error Codes	Error
0x01	Bad Request
0x02	BindID Not Found
0x03	Wrong BindID
0x04	Out of Port
0x05	Out of Address
0x06	Unauthorized
0x07	Incorrect Port Range
0x08	Incorrect Address

Unused : Must be 0.

Bad Request
Request format not understood by Host-NA(P)T-Server

BindID Not Found
BindID in the DBAP message is not found on Host-NA(P)T-Server record.

Wrong BindID
Bind record on Host-NA(P)T-Server specified by BindID on message does not belong to this Host-NA(P)T-Client.

Out of Port
This error code is used in response to ASSIGN REQUEST. Host-NAPT-Server is temporary out of unassigned port range

Out of Address
This error code is used in response to ASSIGN REQUEST. Host-NAT-Server is temporary out of unassigned global address

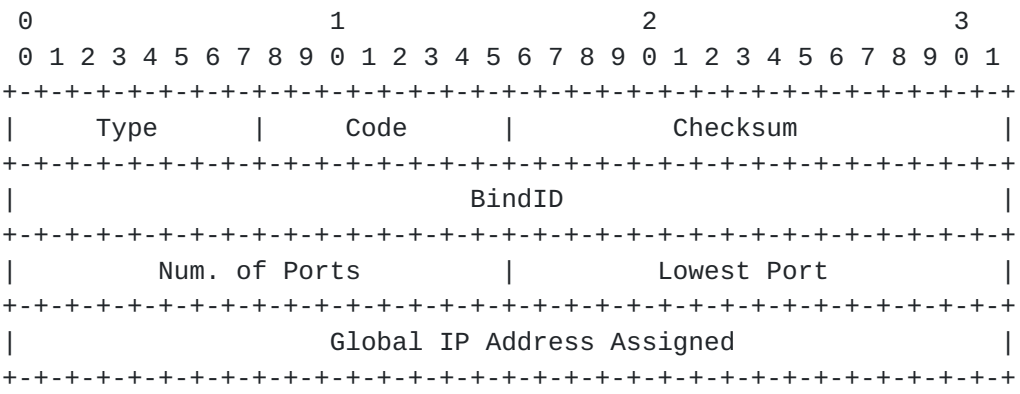
Unauthorized
This error code is used in response ASSIGN REQUEST. Host-NA(P)T-Client is not authorized to obtain bindings with this Host-NA(P)T-Server. This error response could be return after checking with a policy module.

Incorrect Port Range
This error code is used in response to FREE REQUEST. Port range in the FREE REQUEST is not correct for the bind record on Host-NAPT-server.

Incorrect Address
This error code is used in response to FREE REQUEST. Address contained in the FREE REQUEST is not correct for the bind record on Host-NA(P)T-server.

5.6 END Notification

END Notification is sent by Host-NA(P)T-Server for informing Host -NA(P)T-Client of the expiration of a particular bind. Again, Host-NA(P)T-Server must wait for FIN-WAIT interval before releasing the bind.



END Notification Format

Type : to be defined
Code : 5
Checksum : 16-bit 1's complement of the 1's complement sum of the entire request. The checksum itself is set to 0 during computation.
BindID : BINDID of the ASSIGN REQUEST that this notification corresponds to.
Num. of Ports : Total number of ports in the block to be ended, when no port translation is used, this field must be zero.
Lowest Port : Lowest port number in the block to be ended, when no port translation is used, this field must be zero.
Global IP Address Assigned : Global IP address this notification refers to .

Host-NA(P)T-Clients are not expected to acknowledge receipt of this notification. After FIN-WAIT interval elapsed, data packets received pertaining to this bind will be responded with an ICMP host unreachable response.

6. Scenarios

The scenarios quoted are common examples of how HNAT and DBAP could be exploited in real life. In scenarios pertaining to DNS lookup DNSSEC is assumed to be implemented on all DNS servers. Although the mechanism could be extended to all end-to-end security mechanism, IPsec is used in the examples due to its popularity today. Private routing realms are assumed to have global routing capabilities, that is, addresses from external domains are advertised by the NAT router in the private domain but not the other way round. At least one DNS server within the private realm is responsible in handling queries from external entity and, for simplicity, such DNS servers are assumed to be statically assigned a global address each. Security Association (SA) negotiation using Internet Security Association and Key Exchange Protocol (ISAKMP) in NAT Environment is outside the scope of this document. This issue may be addressed in the work-in-progress Internet Draft [6]. Hence for

simplicity, end hosts are assume to have the security association (SA) negotiation completed using ISAKMP and details of ISAKMP negotiation, particularly ISAKMP SA establishment and Internet Key Exchange (IKE),

are omitted. These scenarios illustrate address translation without port translation, cases of port translation could be extended without too much effort.

6.1 Outbound Data Session with End-to-End Security (IPSEC)

Here we consider the outbound data stream of a session between an External entity X and an internal host A with IP security. IP tunneling is used to route the packet in private realm.

1. First of all, host A request a global address from Host-NAT-Server using DBAP. It sends a DBAP ASSIGN REQUEST with a randomly generated BINDID field and "Lowest Port", "Num. of Port" and "Assigned address" fields filled with 0s. It may optionally include a maximum lease time value. When this DBAP request reaches the Host-NAT-Server, a global address, say U, is pulled from the address pool and assigned to A. The binding timer is started and Host-NAT-Server replies to host A with DBAP ASSIGN RESPONSE with "Lowest Port" and "Num. of Port" fields set to zero, and "Assigned Global Address" field set to U.
2. Host A then computes the cryptographic algorithm using address of X as destination address and this assigned global address U as the source address. Before sending the packet out to the private network, host A encapsulates the packet with an internally addressed IP header and tunnel it to the Host-NAT-Server.
3. When the packet reaches the Host-NAT-Server, it is decapsulated and routed in the external realm to X.

6.2 Inbound DNS Name Lookup Query with DNSSEC

In this scenario, we say that an external entity X wishes to perform a name lookup for an internal host A. DNSSEC is applied to all DNS servers. These are the sequence of events.

1. Host X does a DNS query to its local DNS server
2. DNS of X.external.com queries the root DNS server
3. Root DNS server replies with a referral to DNS server of the private network
4. DNS server of X.external.com sends a query to DNS server of private network
5. When the query reaches DNS server of private network, it does a lookup on "A.private.com" and find A's local address, say 10.0.0.1.
6. DNS then obtains a global address for A using DBAP. It sends a DBAP ASSIGN REQUEST with "Lowest Port", "Num. of Port fields" and "Assigned Global Address" fields filled with 0s and a randomly generated BINDID. When this DBAP request reaches the Host-NAT-Server, a global address, say U, is pulled from the address pool and assigned to 10.0.0.1. The bind timer is started and Host-NAT-Server replies to DNS with DBAP ASSIGN RESPONSE with "Lowest Port" and "Num. of Port"

fields set to zero, and "Assigned Global Address" field set to U. DNS of private network then encrypt U in DNS response payload and sends it back to DNS of X.external.com. The response traverse the

Host-NAT-Server unchanged. No DNS-ALG [3] is required at the NAT.
7. DNS of X.external.com replies Host X with address U assigned to Host A by NAT router.

7. Architectural Enhancement on Host-NAT-Server and Host-NAT-Client

To be discussed in later drafts.

8. Impact on Application and Application Level Gateway

To be discussed in later drafts.

9. Security Considerations

To be discussed in later drafts.

10. Acknowledgement

We wish to acknowledge Dr. Takeshi Nishida for his valuable comments that had been very helpful in the writing of this draft.

11. References

[1] P. Srisuresh, Matt holdrege, "NAT : Terminology and Considerations" <draft-ietf-nat-terminology-01.txt>, Work-in-progress

[2] P.Srisuresh, K. Egevang, "Traditional IP Network Address Translator" <draft-ietf-nat-traditional-01.txt>, Work-in-progress

[3] P.Srisuresh, G.Tsirtsis, P.Akkiraju, A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)" <draft-ietf-nat-dns-alg-01.txt>, Work-in-progress

[4] M.Borella, David Grabelsky, Ikhlaq Shdhu, Brian Petry, "Distributed Network Address Translation" <draft-borella-aatn-dnat-01.txt>, Work-in-progress

[5] P.Srisuresh, "IP Network Address Translator Application Programming Interface" <draft-ietf-nat-api-00.txt>, Work-in-progress

[6] P.Srisuresh "Security for IP Network Address Translator (NAT) Domains" <draft-ietf-nat-security-00.txt>, Work-in-progress

12. Authors' Address

Jeffrey Lo
NEC USA, Inc.
110 Rio Robles
San Jose, California 95134
Voice : (408) 943 3033
Fax : (408) 943 3099
Email : jlo@ccrl.sj.nec.com

Kunihiro Taniguchi
NEC USA, Inc.
110 Rio Robles
San Jose, California 95134
Voice : (408) 943 3031
Fax : (408) 943 3099
Email : taniguti@ccrl.sj.nec.com