UNDERSTANDING HOLE PUNCHING

MANUSH PANDYA

ICT, GANPAT UNIVERSITY

ABSTRACT

In todays day and age devices make communication with each other via their IP constantly. In the case that a firewall is applied, the device behind the firewall has to initiate the communication. Hole Punching is a method that allows a communication in case both devices are behind firewalls using the concept of network address translation (NAT). In the case of hole punching a node outside NAT with a public static IP is used, this acts as a rendezvous server that forwards the messages to the device. Nodes on both ends behind different NAT's are used to try and create a direct communication method. This kind of communication is useful for peer to peer architectures and is used for communication uses such as chat applications, teleconferencing file sharing etc. ICMP hole punching, UDP hole punching and TCP hole punching are various methods of hole punching.

INTRODUCTION

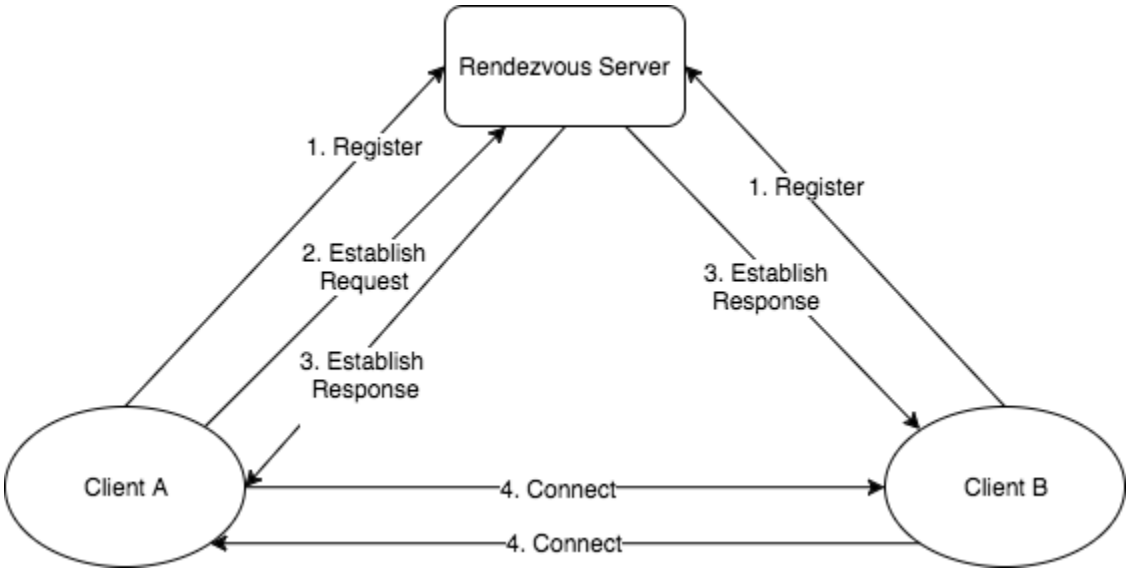

Fig: 1 Hole Punching

Source:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fgithub.com%2Fwilfreddenton%2Fudp-hole-punching&psig=AOvVaw3C15TpXkVf9p8-nzV_OHLO&ust=1619421248653000&source=images&cd=vfe&ved=0CAMQjB1qFwoTCNi8obbsmPACFQAAAAAdAAAAABAO

A NAT is a system that does not allow for outbound communications. Any request sent from a device outside the NAT is immediately rejected. In order to establish a connection, the only way is to send the request from the inside. This kind of methodology is useful for a situation only when one or none of the devices have NAT. this means that in the case where both devices are implementing NAT the communication is not possible. Hole punching solves this problem. It uses one or more servers to establish an outside communication. Fig 1 demonstrates how a communication between two devices can be made where in reality there is no direct connection but using hole punching, a connection similar to direct communication is achieved. Since the communication via the third server creates a gap (hole) in the firewall of the devices this method is termed as hole punching.

VoIP products, gaming software, P2p networking all use hole punching.

NETWORK ADDRESS TRANSLATION (NAT)

“Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. The technique was originally used to avoid the need to assign a new address to every host when a network was moved, or when the upstream Internet service provider was replaced, but could not route the networks address space. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.”

Source: https://en.wikipedia.org/wiki/Network_address_translation

ADVANTAGES OF NAT

- Prevents depletion of IP addresses
- Provides additional layer of security by making original source and destination address hidden
- Provides increased flexibility when connection to public internet
- Allows the use of private IPv4 system and prevent internal address changes upon change of service provider

DISADVANTAGES OF NAT

- High usage of resources as it needs to translate incoming IPv4 addresses and outgoing IPv4 datagrams for transaction details.
- Delay in IPv4 communication
- Loss of end to end device compatibility.
- Some technologies and network application may not function correctly under NAT

ICMP HOLE PUNCHING

ICMP hole punch is employed so as to keep the ICMP parcel stream going. NAT traversal techniques are needed for client-to-client networking applications on the net involving hosts connected in private networks, ICMP hole punching establishes connectivity between 2 hosts communicating across one or more network address translators in either a peer-to-peer or client-server model. Third party hosts on the general public transit network are accustomed to establish UDP or TCP port states that will be used for direct communications between the communicating hosts, absolute information within the packet expected by the NAT permits the packet to reach the destination server.

> "ICMP hole punching sets up availability between two hosts conveying across at least one Network address translation in either a distributed or customer server model. Ordinarily, outsider has on the open travel organize are utilized to set up UDP or TCP port expresses that might be utilized for direct interchanges between the conveying has, anyway ICMP hole punching requires no outsider association to pass data between at least one NATs by misusing a NAT's free acknowledgment of inbound ICMP Time Exceeded parcels.
>
> When an ICMP Time Exceeded bundle arrives at the goal NAT, discretionary information in the parcel expected by the NAT permits the bundle to arrive at the goal server, permitting the goal server to get the customer's open IP address and other information put away in the packet

from the customer." Pooja Pemare - Overview of Hole Punching: ICMP Hole Punching, TCP Hole Punching, UDP Hole Punching.

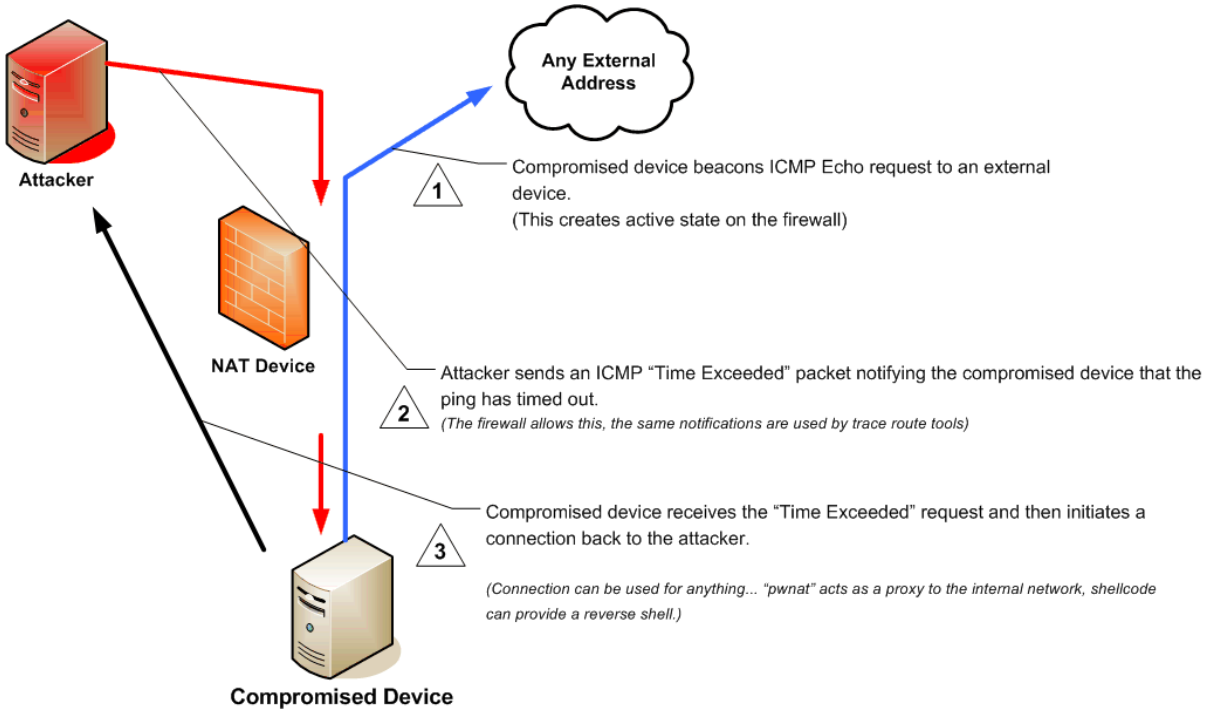

Fig 2: ICMP Hole Punching

Source:

https://www.google.com/url?sa=i&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FICMP_hole_punching&psig=AOvVaw1mpyX0N2aj87Ng7AdJIzRk&ust=1619423118204000&source=images&cd=vfe&ved=0CA0QjhxqFwoTCKCB7rXzmPACFQAAAAAdAAAAABAD

UDP HOLE PUNCHING

UDP hole punching could be an ordinarily used technique used in network address translation (NAT) applications for maintaining User Datagram Protocol (UDP) packet streams that traverse the NAT.

Hosts with network property within a non-public network connected via a NAT to the net generally use the Session Traversal Utilities for NAT (STUN) technique or Interactive connectivity institution

(ICE) to work out the general public address of the NAT that its communications peers need. during this method another host on the general public network is employed to determine port mapping and alternative UDP port state that's assumed to be valid for direct communication between the appliance hosts. Since UDP state typically expires once short periods of time within the varying range of tens of seconds to a couple of minutes, [2] and therefore the UDP port is enclosed the method, UDP hole punching employs the transmission of periodic keep-alive packets, every revitalizing the life-time counters within the UDP state machine of the NAT.

TCP HOLE PUNCHING

The gist of the concept is to use a middle-man server to facilitate the exchange of public information science addresses and foretold ports for each ends of the specified affiliation. Both sides then initiate an affiliation to the other's public information science address-port pair whereas at the same time listening for incoming SYNs. This leads to two SYNs being sent out. At every end, a NAT will produce a bidirectional mapping between the inner host's address-port and an address-port combination on the NAT's external aspect. If the port was foretold properly (and passed to the remote party via the middle-man), the NAT can ultimately forward the remote SYN to the inner host. This leads to either the "simultaneous open" transmission control protocol state transition or a "syn received" transition from the LISTEN state.

CONCLUSION

Hole punching is a powerful and reliable tool for creating peer to peer communications on networks involving NAT. It eliminates the need for expensive tunneling required for direct communication in some cases and is a very useful measure. Telephony software Skype uses hole punching to allow users to communicate with one or more users audibly.

Fast-paced online multi-player games may use a hole punching technique or require users to create a permanent firewall pinhole in order to reduce network latency.

VPN applications such as Hamachi or ZeroTier utilize hole punching to allow users to connect directly to subscribed devices behind firewalls.

Decentralized peer-to-peer file sharing software relies on hole punching for file distribution.

REFERANCES

https://en.wikipedia.org/wiki/Hole_punching_(networking)#:~:text=Hole%20punching%20(or%20sometimes%20punch,network%20address%20translation%20(NAT)

Overview of Hole Punching: ICMP Hole Punching, TCP Hole Punching, UDP Hole Punching , Ms. Pooja Pemare

https://wikivisually.com/wiki/ICMP_hole_punching

https://en.wikipedia.org/wiki/TCP_hole_punching#Methods_of_Port_Prediction_(with_predictable_NATs)

https://www.quora.com/What-is-TCP-hole-punching