Solving the Incompatibility between NAT and IPSec

Connectathon 2002
March 6, 2002
Ivan Wallis
SSH Communications Security, Inc.

What is NAT?

- Network Address Translation (NAT) means substituting IP addresses and/or port numbers at a gateway
- NAT is typically used
  - at the boundary of corporate networks (firewall)
  - by ISPs for dial-up,xDSL, and cable connections (to conserve IP addresses and to ease configuration)
  - in homes and small offices, to attach multiple hosts to a single connection

Why is NAT used?

- Fewer public IP addresses needed (saves addresses)
- Easier configuration
- Easier to change service provider
- More freedom in network planning and expansion
- Hides internal network structure (perceived as better security)

Will there be NAT with IPv6?

- IPv6 deployment will increase NAT use during the transition period
  - Various mobile network architectures are based on using NAT
  - Putting dual stacks into mobile terminals/phones is seen as too expensive
  - Extra complexity and cost of configuring, maintaining and debugging two routing systems
  - Not all systems will support IPv6 any time soon
- IPv6 auto-configuration eliminates most need for NAT
- However,people may still want to e.g. hide internal network details

IPSec NAT issues (IPv4)

- IPSec has not worked across NAT
  - NAT devices drop AH &ESP
  - AH MAC mismatch
  - TCP checksum mismatch
  - SPI conflicts
  - Several local networks using same private addresses
- Most NATs are port NATs
- IPSec standard ignores NATs
- NATs have become the most critical problem for wide-scale IPSEC deployment

NAT Traversal requirements

- No changes to NAT devices - must be implemented at tunnel endpoints
- No user interaction, configuration or understanding required
- Minimal modifications to existing IPSEC architecture
- Works with any IPSEC transform and any kind (and combination) of NAT
- Efficient, interoperable, and robust

Basic solution (IPv4)

- Detect whether both parties support NAT Traversal (NAT-T)
- Detect whether (and/or what) transformations are taking place
- Tunnel packets within UDP
- Compensate for the transformations if needed

Standardization status (IPv4)

- Consensus was reached on the specification
- Internet draft exists,past last call
  - Some protocol numbers still to be obtained from IANA
  - Awaiting IESG approval
- Recently, new problems have been encountered with broken NAT devices and firewalls

Broken NATs and firewalls

- Microsoft tested eight NAT devices from different vendors, most of them where broken
- Common problems:
  - NATs that don't pass fragments at all
  - NATs that can't handle fragments in wrong order
  - NATs that do IKE cookie mapping (how brain-dead!)
- Many firewalls have similar problems

  E.g., Cisco IOS NAT does not handle out-of-order fragments correctly; Linux sends them out-of-order by default
- IKE can send large, fragmented UDP packets (large proposals; certificate/CRL payloads)

The sad state of the Internet

- One has to assume NAT (usually broken NAT)
- The consumer Internet has degenerated to only TCP/IP and small UDP packets
  - ”Mobile Internet” activities are trying to degenerate it further into an HTTP-only system
- For most users,TCP/IP connections still work (subject to firewalls)
  - Unless you try to connect to e.g. port 80 (transparent proxies...)
- UDP only works for small (non-fragmented packets)
  - Only some port numbers work,e.g. anything sent to UDP port 500 is corrupted by some NATs
- Nothing else can be trusted to go through

So what's going to happen?

- Need to specify a way to make NAT-T work
- Quick solution: send small proposals and only one certificate if NAT is taking place
- Full solution:
  - Add application-layer fragmentation mechanism in IKE that keeps UDP packets below e.g. 500 bytes
  - Add application-layer fragmentation mechanism in IKE that fragments UDP-encapsulated AH/ESP packets into pieces less than 500 bytes
    - This mechanism needs to run in the kernel
- The problems are fixable, but add more kludges
  - No other way make VPNs work reliably in sight :-(
- Standardization will be delayed by some months

Status of IPv6 NAT Traversal

- Generally vendors are still struggling to get IPv4 NAT Traversal working
- No real standardization work has started at the IETF regarding NAT-T for IPv6
- In principle it is known how to do NAT Traversal for IPv6,both in the IPv6-IPv6 case and in the IPv6-IPv4 case
- Overall IPv6 deployment seems to be getting delayed

IPv6-IPv6 NAT Traversal

- NAT Traversal through a device translating between IPv6 addresses is fairly straightforward
- Differences from the IPv4 method:
  - In IKE negotiation, must be able to pass IPv6 addresses (or hashes of IPv6 addresses)
    - Already supported by current internet drafts
  - In NAT-T encapsulation
    - Already supported by current internet drafts (though not yet tested or fully analyzed)

IPv4-IPv6 NAT Traversal

- Translation between IPv4 and IPv6 will be driven by wanting to avoid dual stacks, dual configuration, dual routing, dual firewall configurations, additional troubleshooting complexity, etc.
  - Dual stacks problematic especially in mobile devices
- Differences from the normal IPv4 method:
  - IKE implementation must be able to compute checksums properly even if IP address type changes
  - Tunnel mode encapsulation changes very little
  - Transport mode encapsulation changes more
    - Must be more clever in updating TCP pseudo-headers
    - May need to pass some fields explicitly in NAT-T header
  - AH compensation is possible but tricky (must rebuild original IP header)

Who is shipping NAT Traversal today?

- SSH ships a version based on the latest Internet Drafts with its SSH IPSEC Express toolkit
  - The technology was originally developed by SSH
- Various vendors ship their proprietary implementations (hopefully converging to the standard in near future)

Conclusions

- Network Address Translation has been a major problem area in IPSEC VPNs
- NAT Traversal is easy to deploy and makes VPNs much more robust
- NAT Traversal is critical in wireless VPNs
- Obviously becoming one of the key requirements in all VPN products
- Ongoing standardization paves the way for wide deployment