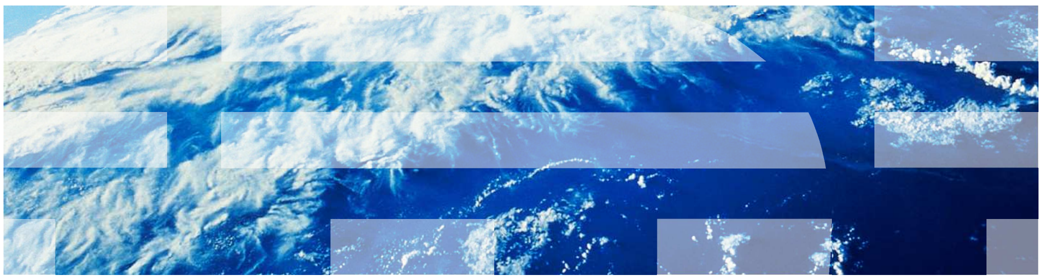
z/OS Communications Server

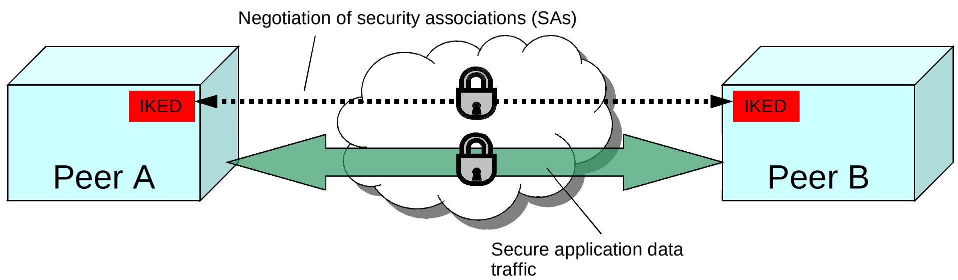
Network address translation traversal support for IKE version 2



This presentation provides an overview of network address translation traversal support for IKE version 2 in z/OS® V1R13 Communications Server.

Background on IPsec

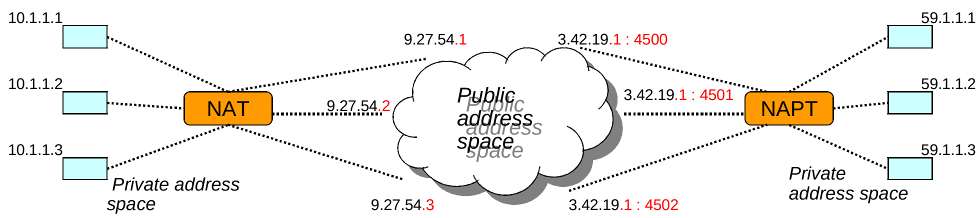
- What is IPSec?
  - An RFC-standardized method of securing communication at the IP layer
  - Provides authentication, encryption and data integrity
  - Two versions of IKE: IKEv1 and IKEv2
  - Transparent to applications



IPSec uses negotiated security associations to encrypt and authenticate IP traffic. IPSec uses security associations (SAs) negotiated by IKE daemons. Phase 1 / IKE SA……IKE protocol provides a secure negotiation channel. Phase 2 / Child SA....AH or ESP protocols provide application data protection.

Background on network address translation

- What is Network Address Translation (NAT)?
  - Translation of private, internal IP addresses to public external IP addresses
  - Alters IP addresses and ports in datagram headers and data payloads
  - Primary purpose is to relieve shortage of globally unique IPv4 addresses



The concept of NAT was developed primarily to address the shortage of globally unique IPv4 addresses. This is not a concern for IPv6. NAT is typically deployed on border routers or firewalls. Another benefit of NAT is the ability to hide internal IP addresses from network segments outside the internal IP address domain. With NAT, there is a one-to-one mappings of private to public addresses. Multiple private addresses can be mapped to a single or limited pool of public addresses. This is called port translation (NAPT, PAT), “IP masquerading”, or “overloading”.

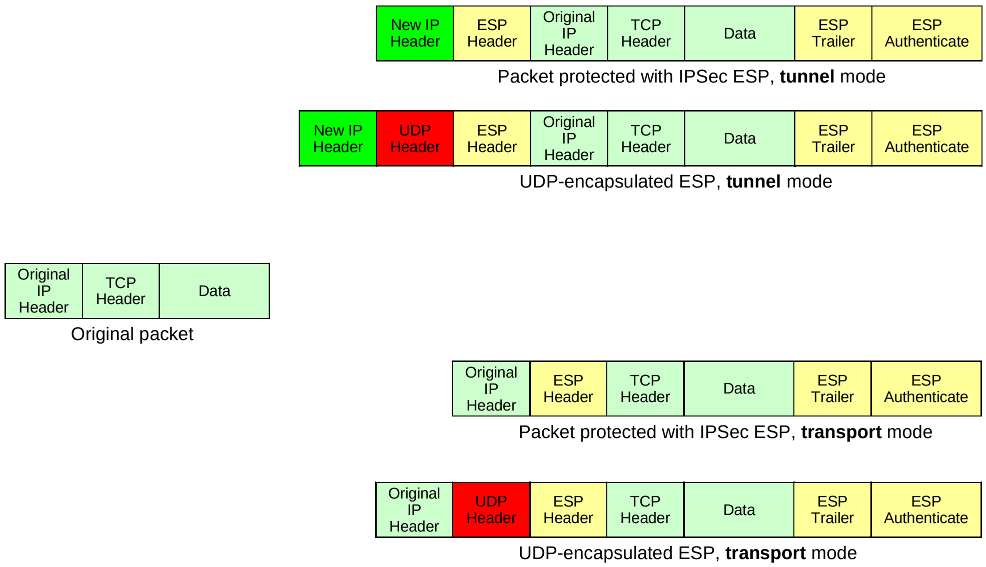
Background on NAT traversal negotiation

- RFC 3715 describes NAT and IPsec incompatibilities
- RFC 3947 describes how IKEv1 negotiates NAT traversal
  - Discover NAT traversal capabilities
  - Detect the presence of NAT devices
- RFC 3948 describes how ESP is UDP encapsulated for NAT traversal
- RFC 5996 describes how IKEv2 negotiates NAT traversal

RFC 3715 describes various fundamental incompatibilities between NAT and IPsec. For IKEv1, these incompatibilities are surmounted using NAT traversal negotiation, which is documented in RFC 3947. NAT traversal negotiation allows for two IKE peers to discover each other's NAT traversal capabilities and to detect the presence of NAT devices between them. This results in the establishment of a UDP-encapsulated ESP security association, the behavior of which is described in RFC 3948.

IKEv2 NAT traversal negotiation, including the detection of NAT devices, is described in RFC 5996. IKEv2 continues to use UDP-encapsulated ESP as described in RFC 3948. z/OS Communications Server supports IKEv2 NAT traversal beginning in V1R13.

Background on UDP encapsulation of ESP



5 July 14, 2011 Network address translation traversal support for IKE version 2

IPsec encapsulates IP packets using either transport mode, which uses the original packet's IP header, or in tunnel mode, which adds a new IP header to the outside of the packet. IPsec normally uses either the AH or the ESP protocol for this encapsulation. NAT traversal uses only ESP; AH is incompatible with NAT traversal.

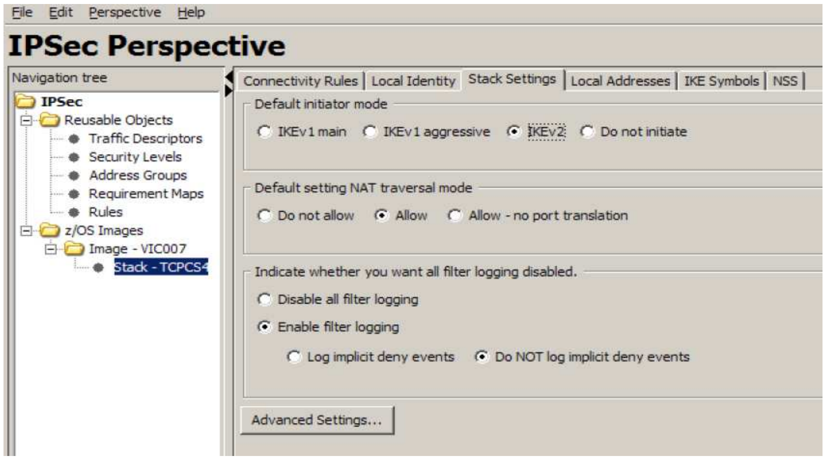
On the left, this slide shows an original IP packet to be encapsulated. At the top right, this diagram shows first the *tunnel*-mode encapsulation of this IP packet using ESP. Note that a new IP header is added to this packet. Second, this packet is further encapsulated using a UDP header for NAT traversal. At the bottom right, this diagram shows first the *transport*-mode encapsulation of this IP packet using ESP. Note that the original IP header is used for this packet. Second, this packet is further encapsulated using a UDP header for NAT traversal.

Overview of support

- Send and receive NAT-detection payloads
- Determine if the peer is z/OS
- Use UDP port 4500 for IKE messages
- Use UDP-encapsulation for ESP security associations
- Detect and respond to NAT remapping

z/OS V1R13 Communications Server adds support for IKEv2 NAT traversal as described in RFC 5996. This support involves several aspects shown on this slide. This includes detecting the presence of a NAT device, accommodating the NAT device, and reacting to changes in NAT mappings. All of these are analogous to the IKEv1 NAT traversal support.

Function externals: Enabling NAT traversal



No new configuration is needed to enable NAT traversal in IKEv2. Beginning in V1R13, z/OS Communications Server supports NAT traversal for IKEv2 using the same configuration as for IKEv1.

If you use the IBM Configuration Assistant, NAT-traversal settings now apply to both IKEv1 and IKEv2. This slide shows the stack-level NAT traversal setting; the Configuration Assistant also allows you to modify NAT-traversal settings for individual connectivity rules using the advanced settings. Filter rules for allowing IKE UDP port 4500 traffic are created automatically for you when using the IBM Configuration Assistant.

If you configure your policy manually, the AllowNAT keyword on the KeyExchangePolicy and KeyExchangeAction statements now apply to both IKEv1 and IKEv2

Function externals: ipsec –k command

- ipsec –k display (phase 1 / IKE SA)

```
CS V1R13 ipsec  Stack Name: TCPCS4  Tue Jan  4 10:17:31 2011
Primary:  IKE tunnel       Function: Display           Format:   Detail
Source:   IKED             Scope:    Current           TotAvail: n/a

TunnelID:                     K11
Generation:                   1
IKEVersion:                   2.0
.
.
.
LifetimeRefresh:              2011/01/04 18:13:57
LifetimeExpires:              2011/01/04 18:16:21
ReauthInterval:               0m
ReauthTime:                   n/a
Role:                         Initiator
AssociatedDynamicTunnels:     1
NATTSupportLevel:             IKEv2_zOS
NATInFrntLclScEndPnt:         No
NATInFrntRmtScEndPnt:         Yes
zOSCanInitiateP1SA:           Yes
AllowNat:                     Yes
RmtNAPTDetected:              No
RmtUdpEncapPort:              4500
```


This slide shows the NAT-traversal-related fields in the ipsec –k display. These fields can now contain information for IKEv2 security associations. Two new NATTSupportLevel values are introduced, IKEv2 and IKEv2_zOS. IKEv2 indicates that NAT traversal was negotiated with an IKEv2 peer, while IKEv2_zOS indicates that NAT traversal was negotiated with a z/OS peer using IKEv2.

The equivalent data in SMF records and network management records for phase 1 tunnels can now be set for IKEv2 security associations.

Function externals: ipsec –y command

- ipsec –y display (phase 2 / Child SA)

```
CS V1R13 ipsec  Stack Name: TCPCS4  Tue Jan  4 10:26:37 2011
Primary:  Dynamic tunnel  Function: Display           Format:
Source:   Stack           Scope:    Current           TotAv

TunnelID:                     Y12
Generation:                   1
IKEVersion:                   2.0
ParentIKETunnelID:            K11
.
.
.
LifetimeRefresh:              2011/01/04 14
LifetimeExpires:              2011/01/04
CurrentTime:                  2011/01/0         7
VPNLifeExpires:               2011/01          :21
NAT Traversal Topology:
  UdpEncapMode:               Yes
  LclNATDetected:             N
  RmtNATDetected:
  RmtNAPTDetected:
  RmtIsGw:
  RmtIsZOS:                     s
  zOSCanInitP2SA:              es
  RmtUdpEncapPort:            4500
  SrcNATOARcvd:               n/a
  DstNATOARcvd:               n/a
PassthroughDF                 Yes
Passthrough                   Yes
```


This slide shows the NAT-traversal-related fields in the ipsec –y display. These fields can now contain information for IKEv2 security associations.

The equivalent data in SMF records and network management records for phase 2 tunnels can now be set for IKEv2 security associations.

z/OS roles

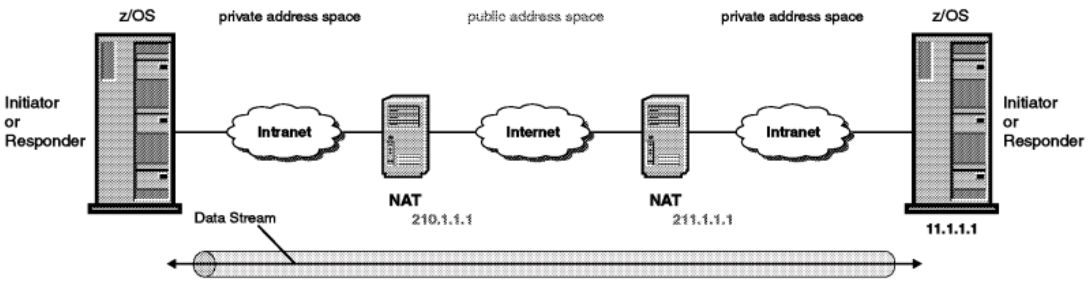
- Topologies supported are the same as for IKEv1
- z/OS in the server role
  – z/OS typically acts as a server, with clients initiating IKE negotiation and application data flows
  – As responder, z/OS provides robust IPSec NAT-traversal responder support
- z/OS in the client role
  – Potential incompatibilities when z/OS initiates IKE negotiation or application data to non-z/OS system
  – See *z/OS Communications Server: IP Configuration Guide* for “Configuration scenarios supported for NAT traversal”
  – IKE issues messages to warn about potential incompatibilities

z/OS supports the same topologies for IKEv2 NAT traversal that it supports for IKEv1.

z/OS is typically deployed in the server role. Robust IPSec NAT-traversal support is provided for the server / responder role. z/OS can be deployed in the client role. A small set of potential incompatibilities exist when z/OS is in the client / initiator role. These are documented in the *z/OS Communications Server: IP Configuration Guide* and on the subsequent slides. When IKE detects a potential incompatibility, it issues messages for IKEv1 (EZD1104I or EZD1105I) and for IKEv2 (EZD1924I or EZD1925I).

Supported z/OS-to-z/OS configurations

- Security association must be host-to-host
- If remote endpoint is behind an NAPT, z/OS must be responder
- Both tunnel and transport mode are supported



This slide details NAT-traversal support when both endpoints are z/OS.

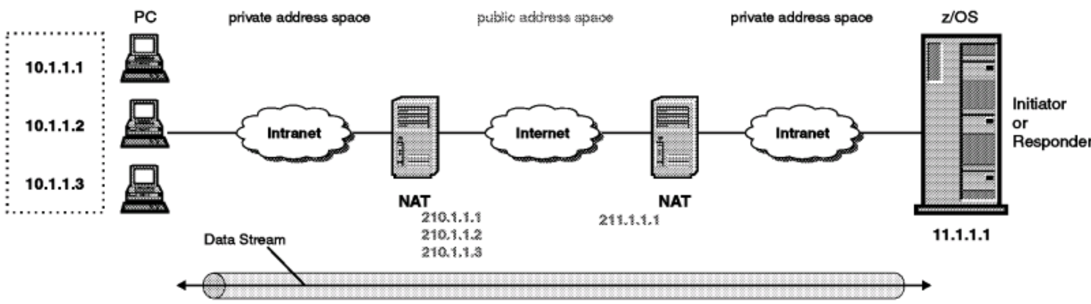
The security associations must be host-to-host; z/OS cannot act as a gateway for NAT traversal.

If the peer is behind a NAT device, z/OS can act as initiator or responder. However, if the peer is behind an NAPT device, z/OS can act only as responder. Phase 1 and phase 2 SAs must be initiated by a peer behind NAPT. Application data traffic must be initiated by a peer behind NAPT.

Both tunnel and transport mode are supported for UDP-encapsulated ESP security associations.

Supported host-to-host configurations

- z/OS as a server: robust responder mode support
- z/OS as a client: results depend on other platforms' implementations
- z/OS must be responder when remote endpoint is behind NAPT
- Both tunnel and transport mode are supported



This slide details z/OS host-to-host NAT-traversal support when one endpoint is not z/OS.

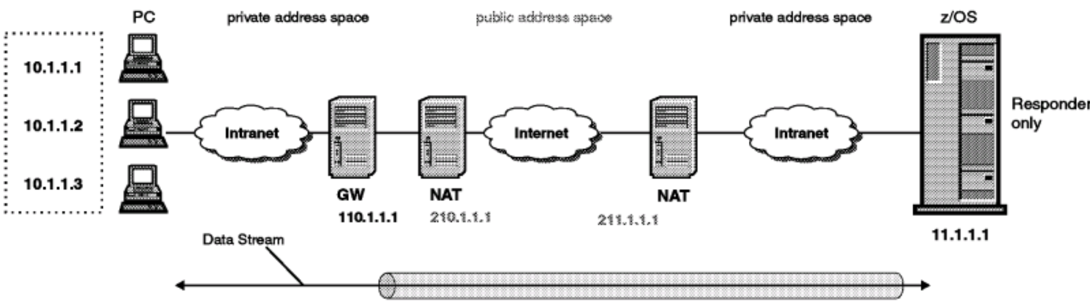
As mentioned earlier, z/OS has robust support when acting as a responder, but potential incompatibilities exist when z/OS acts as the initiator.

If the remote endpoint is behind an NAPT, z/OS must act as a responder. Phase 1 and phase 2 SAs must be initiated by peer behind NAPT. Application data traffic must be initiated by peer behind NAPT.

Both tunnel and transport mode are supported for UDP-encapsulated ESP security associations.

Supported host-to-gateway configurations

- z/OS cannot act as gateway
- When there is a NAT device in front of z/OS, it must be static NAT
- z/OS limited to acting as responder
- Only tunnel mode is possible



13 July 14, 2011 Network address translation traversal support for IKE version 2

This slide details z/OS host-to-gateway NAT-traversal support.

z/OS cannot act as a security gateway for NAT-traversal traffic.

If there is a NAT device in front of z/OS, it must be a static NAT. This is because the remote IPsec gateway needs a predictable address to which to initiate the IKE negotiation.

When the remote endpoint is a security gateway, z/OS is limited to acting as responder. Phase 1 and phase 2 SAs must be initiated by the gateway. Application data traffic must be initiated by the client behind the gateway.

Only tunnel mode is possible for UDP-encapsulated ESP security association that traverse a security gateway.

Diagnosis

- Problem diagnosis
  - pagent.log file for explanation of IPSec policy installation errors
  - IKED syslog output with formatted packet trace
  - If requested by IBM Service, dumps of TCP/IP stack and IKED address spaces with requested CTRACE options
- Common errors
  - Public IP addresses must be used
    - Destination IP addresses on filter rules
    - Remote security endpoint location addresses
  - For IPSec NAT traversal, all security endpoints behind a given NAT or NAPT device must have unique IKE identities

This slide provides information on performing IPSec problem diagnosis.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_NAT.ppt

This module is also available in PDF format at: ../NAT.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information