# CS z/OS Integrated IP Security

## Additional IPSec VPN concepts

# A few additional IPSec VPN concepts - NAT traversal and Sysplex-wide SAs

# IPSec VPN concepts - no NAT devices between security endpoints

- Tunnel mode with AH and/or ESP

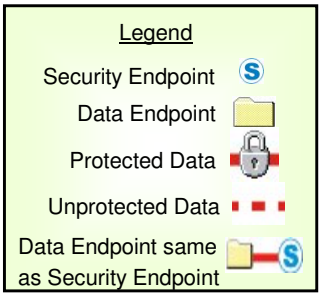
Gateway to Gateway


Gateway to Host


Host to Gateway


- Tunnel or transport mode with AH and/or ESP

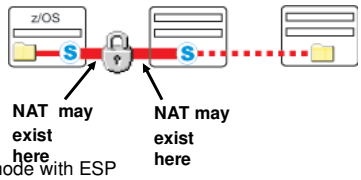
Host to Host

# IPSec VPN concepts - NAT devices between security endpoints

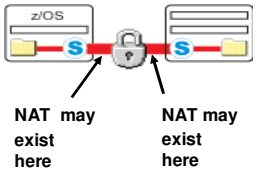
- **If the responder of an SA negotiation is behind a NAT firewall, a static NAT mapping should be used**
- **If z/OS is restricted to responder only, then the data flows must be initiated by the peer as well**
- Tunnel mode with ESP (Responder only)

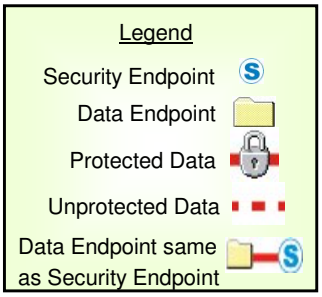
Host to Gateway




- Tunnel or transport mode with ESP

Host to Host



# IPSec VPN concepts - general NAT/NAPT restrictions

- **Only ESP is supported (AH is not allowed by RFC 3947/3948 restriction)**
- **z/OS is optimized for host configuration (does not support acting as a security gateway for SAs that traverse a NAT)**
- **z/OS only supports SAs that traverse a NAT, not SAs that traverse an NAPT**
  - NAPT is a NAT that maps many private addresses to 1 public address by performing port translation (also known as Port Address Translation (PAT)

- Tunnel mode with ESP (Responder only)

Host to Gateway


- Tunnel or transport mode with ESP
  - Potential issues when interoperating with non-z/OS platforms
    - When z/OS initiates an SA for specific ports or protocol
    - When z/OS initiates data on a tunnel mode SA for all ports and protocols

Host to Host


Legend

Security Endpoint

Data Endpoint

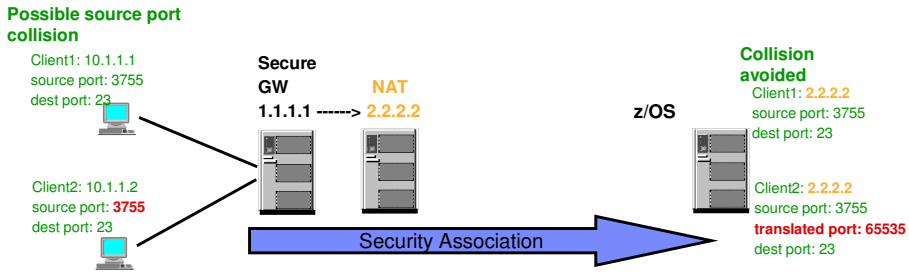
Protected Data

Unprotected Data

Data Endpoint same as Security Endpoint

# IPSec VPN concepts - source port translation for NAT traversal

- **Done when the remote security endpoint is a security gateway behind a NAT**
  - Only done for TCP and UDP packets
  - Since only the public (NAT'ed) address of the security gateway is known to z/OS:
    - Clients that reside behind a security gateway might choose identical source ports
    - z/OS translates source ports to distinguish connections that have a duplicate source port
- **Connection information displayed on z/OS:**
  - Netstat shows translated port
  - ipsec command can be used to show the port mapping (ipsec -o)
  - System logs show when a port translation was performed



# IPSec VPN concepts - NAT keepalive messages

NOTES

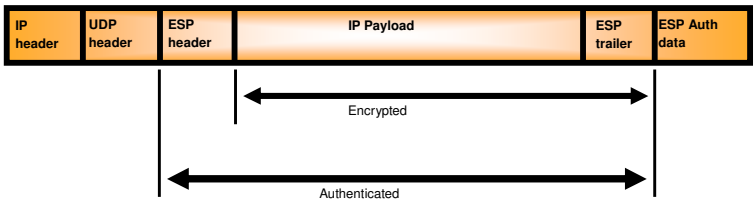
- Intended to prevent NAT mappings from expiring
  - Only required when z/OS is behind a NAT that dynamically assigns IP addresses
- Generated by the stack
  - Only issued when a valid IKE SA exists and IKE is behind a NAT
  - Frequency at which NAT keepalive messages are generated is configurable
    - Defined in the IPSec configuration file
      - Part of Key Exchange Policy
    - Can be turned off
      - Should be turned off if z/OS is behind a static NAT

# IPSec VPN concepts - UDP encapsulation (NAT traversal)

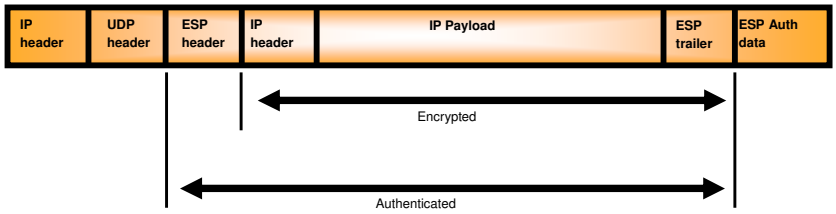
- **Additional encapsulation modes used when a NAT is traversed**
  - UDP-encapsulated transport
  - UDP-encapsulated tunnel
- **Only valid with ESP packets**
  - Normal transport/tunnel mode encapsulation performed
  - Inserts an additional UDP header in front of the ESP header
- **Allows ESP packets to traverse a NAT**
- **On z/OS the decision to use UDP-encapsulation is made by the IKE daemon if a NAT is detected**
- **NAT traversal support can be enabled or disabled in IP security policy**

# IPSec VPN concepts - UDP-encapsulated packets

- **Below shows the format of a UDP-encapsulated transport mode packet**




- **Below shows the format of a UDP-encapsulated tunnel mode packet**



# IPSec VPN concepts - Sysplex Wide Security Association (SWSA) considerations

- **A dynamic VIPA may be the endpoint of an SA - IPSec SAs will be distributed to target stacks of distributed dynamic VIPAs**
  - Used to distribute IPSec-protected workload
  - Used for VIPA takeover
- **Requires the DVIPSEC keyword on the IPSEC statement in the TCPIP profile**
- **Compatibility with z/OS Firewall Technologies IPSec**
  - A FIREWALL stack can be the target of an IPSECURITY stack
  - An IPSECURITY stack can be the target of a FIREWALL stack
  - A FIREWALL stack can be a backup for an IPSECURITY stack
  - An IPSECURITY stack can be a backup for a FIREWALL stack
- **Policies must be consistent on distributing and target stacks**
- **Requires the use of the Coupling Facility EZBDVIPA structure**
- **NAT traversal restrictions - SAs that traverse a NAT:**
  - Cannot be taken over if the remote host is a security gateway
  - Are not supported by z/OS Firewall Technologies IPSec (distributor, target, nor backup)

# Trademarks, Copyrights, and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

| | | | | |
|---|---|---|---|---|
| IBM | CICS | IMS | MQSeries | Tivoli |
| IBM(logo) | Cloudscape | Informix | OS/390 | WebSphere |
| e(logo)business | DB2 | iSeries | OS/400 | xSeries |
| AIX | DB2 Universal Database | Lotus | pSeries | zSeries |

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.