Securing IMS Connect Workloads

Tracy Dean
Product Manager
IBM IMS Tools and z/VM Tools
tld1@us.ibm.com

Agenda

Warning

Importance of IMS Connect

Introduction to IMS Connect Extensions

Multiple methods to secure IMS Connect workloads

Summary and references

IMS APAR PH65117
(Open Telemetry support)
can impact
IMS Connect Extensions

Not marked PE

Wait for PTF for
IMS APAR PH70042

Importance of IMS Connect

IMS Connect

TCP/IP gateway to IMS systems

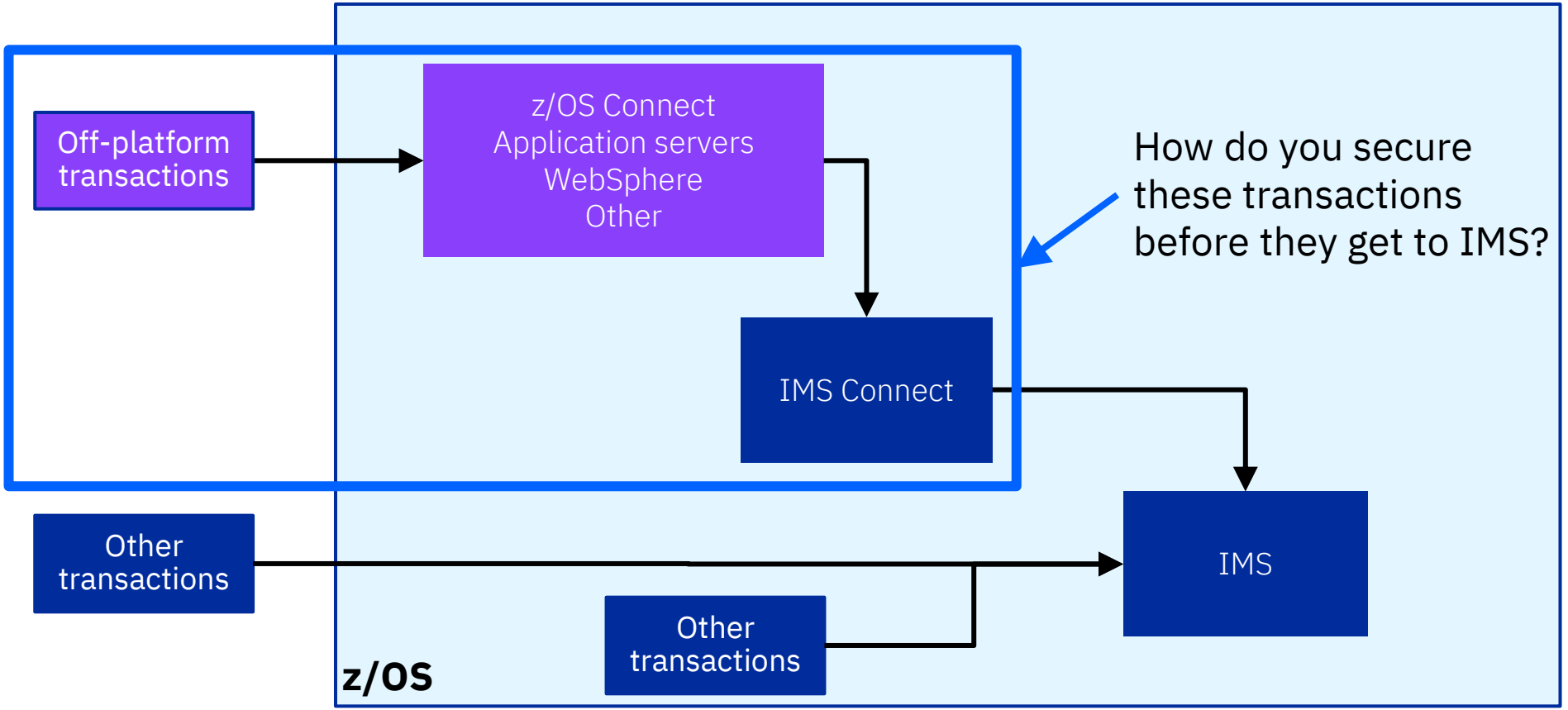
- Clients exchanging requests with IMS Database (via ODBM)
- Clients exchanging requests with IMS Transaction Manager (via OTMA)

Clients can be anywhere

- z/OS Connect
- Application servers
- WebSphere
- Roll-your-own

Clients often administered by multiple teams or organizations

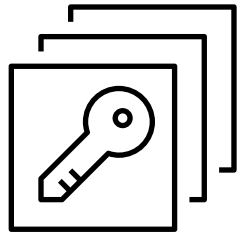
IMS and IMS Connect

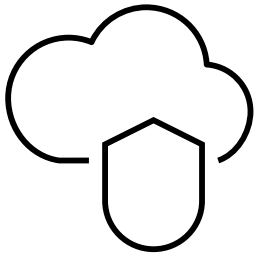


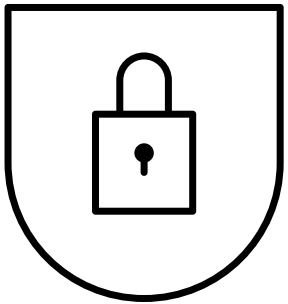
Do I really need to worry about this?

My network is secure – isn't that enough?

- Is one form of security ever enough?
- Human error in network configurations
- Social engineering or hacking







Introduction to IMS Connect Extensions

IMS Connect Extensions

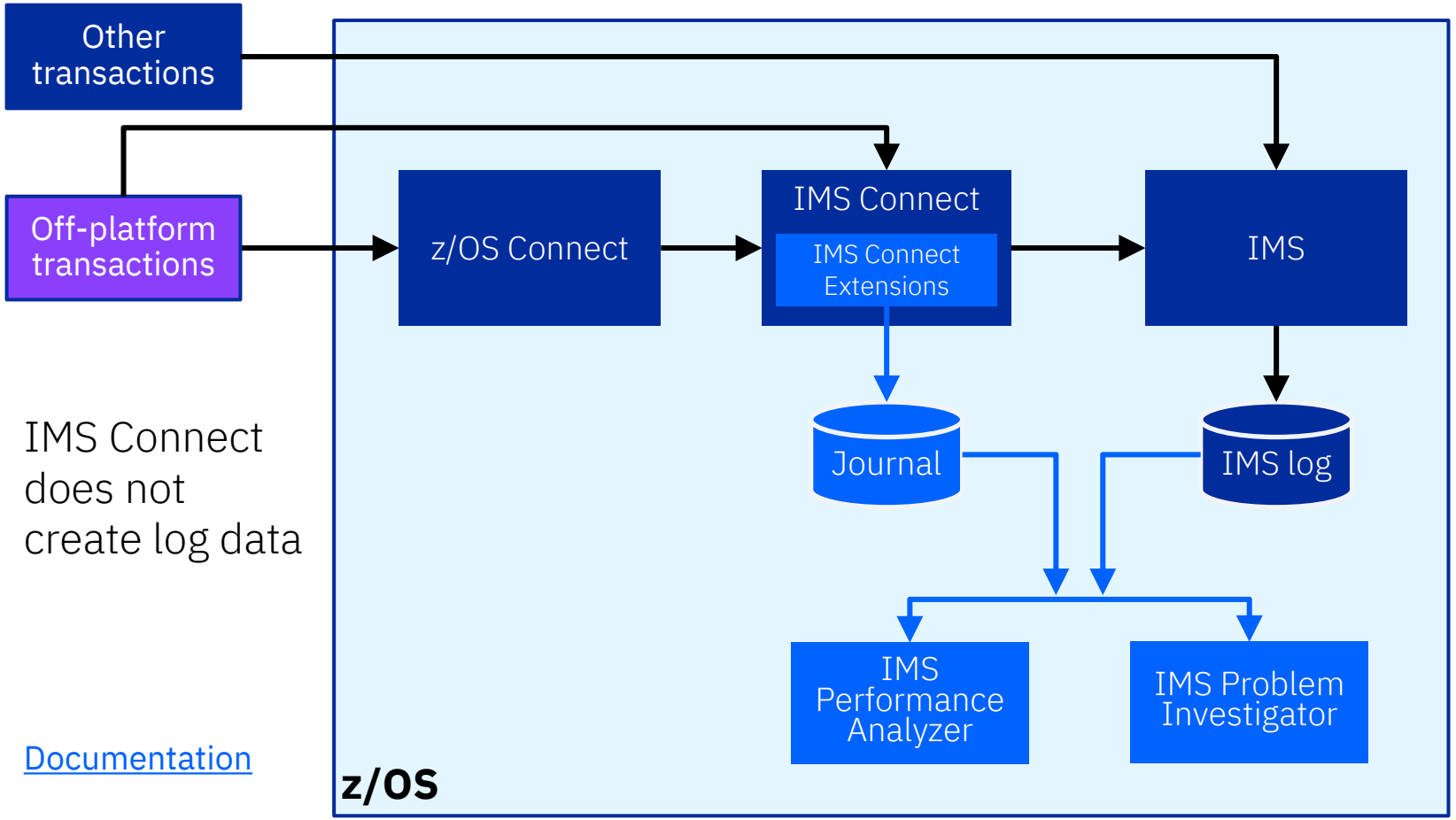
Event collection and streaming instrumentation to analytics

Workload management

Operations management

Security

IMS Connect Extensions – event collection



IMS Connect does not create log data

[Documentation]

Improve availability with workload management

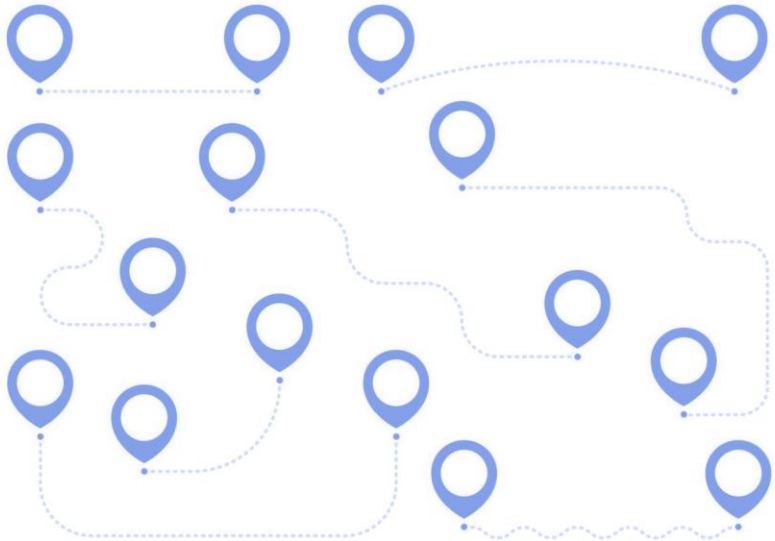
Balance OTMA and ODBM workload across multiple IMS systems

Configure a primary and fallback IMS system

Create custom routing rules/routing plans

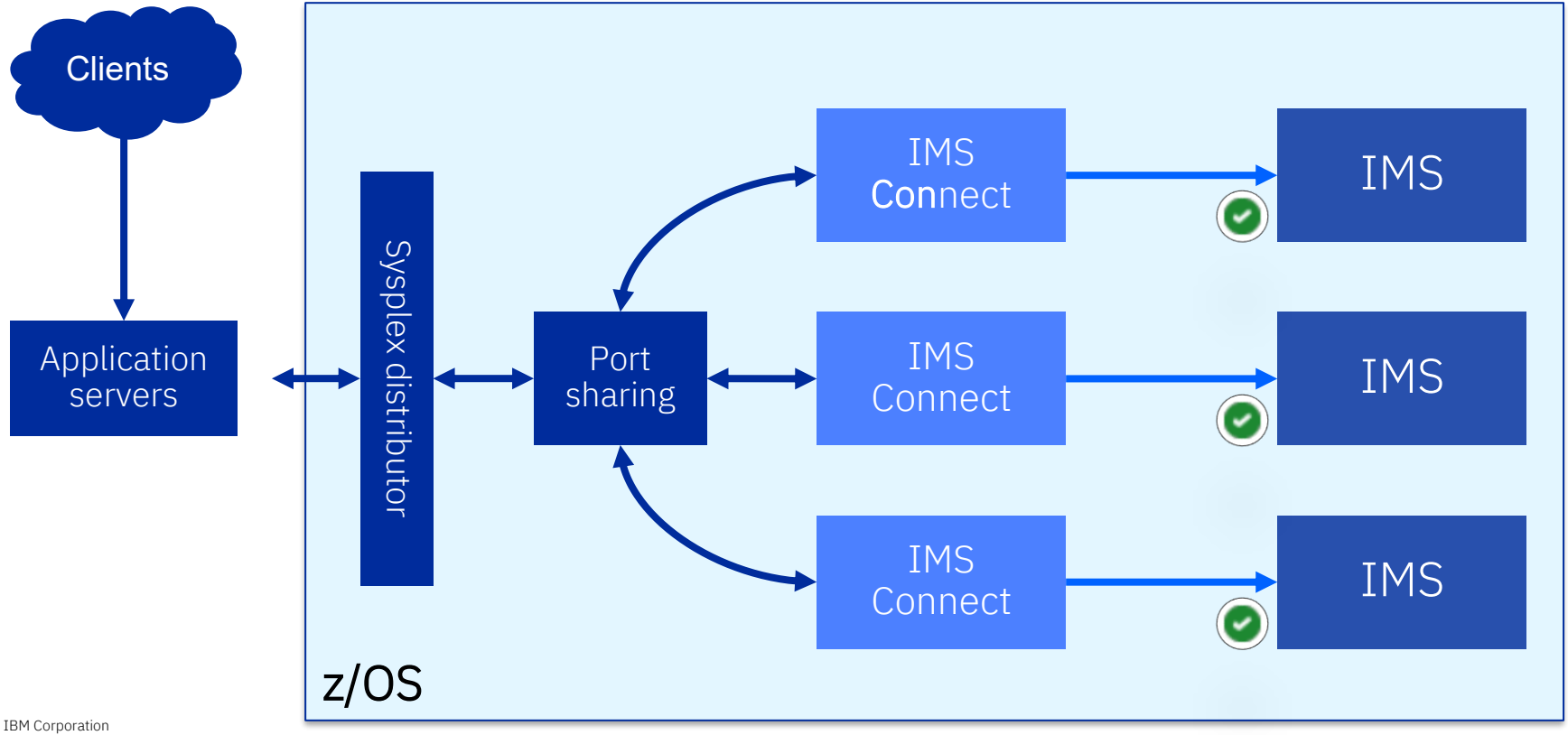
Set up automatic session rebalancing

Schedule or create dynamic changes

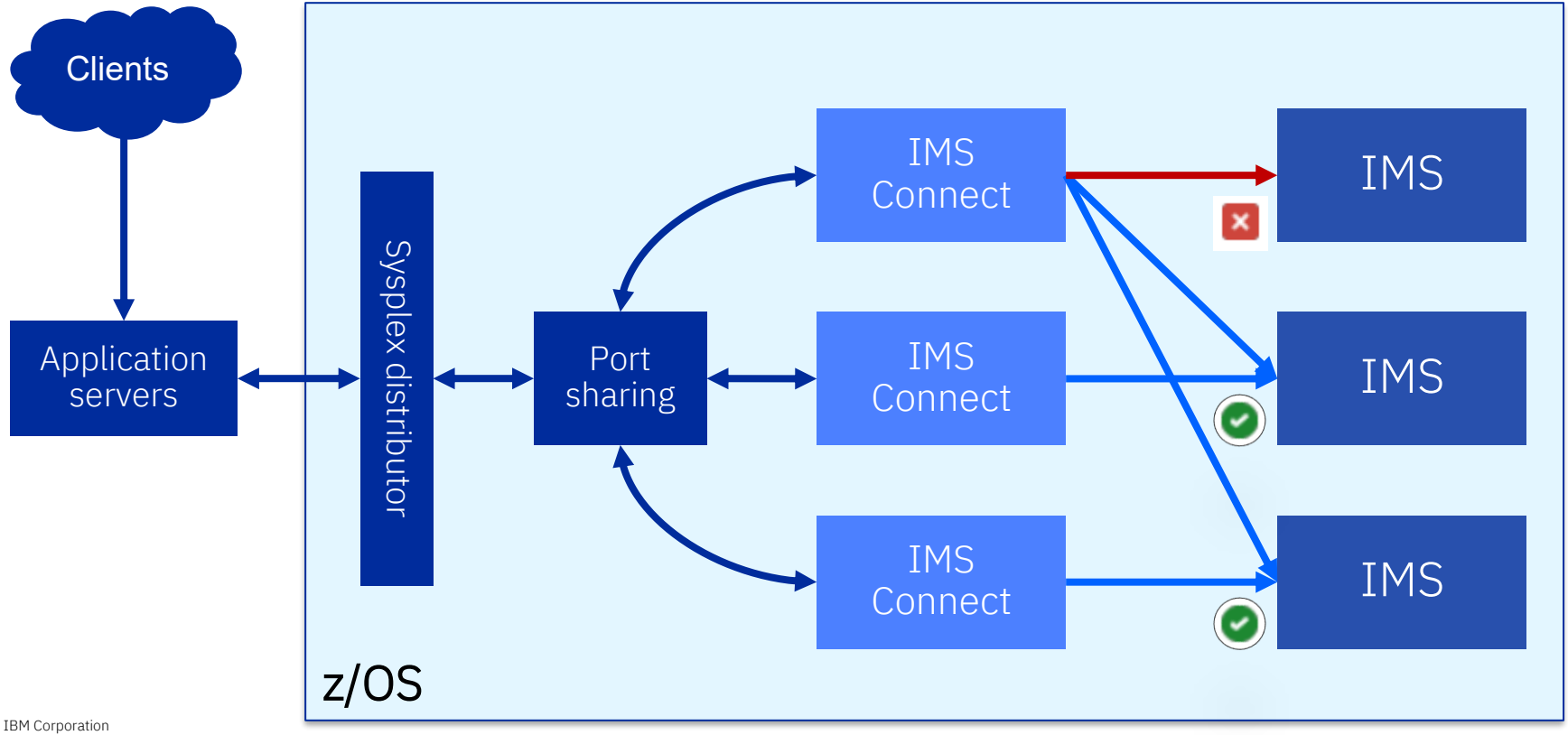


Documentation

IMS Connect Extensions workload management
Simple routing configuration



IMS Connect Extensions workload management
Fallback routing example



IMS Connect Extensions – operations management

- Single point of control (SPOC) for all your IMS Connect systems
- ISPF dialog, Operations Console for z/OS Explorer, or develop your own workflows with Rexx
  - Status monitoring and usage statistics
    - IMS Connect
    - TCP/IP ports
    - DATASTORE connections to IMS
    - ODBMs
    - Active sessions
  - Operations
    - Start/stop/drain a DATASTORE connection to IMS
    - Stop an IMS Connect system
    - Stop/drain an active session
    - Start/stop IMS Connect Extensions trace
    - Change routing plans
    - Dynamically reshape workloads

Documentation

Securing IMS Connect workloads

Securing workloads with IMS Connect Extensions for z/OS

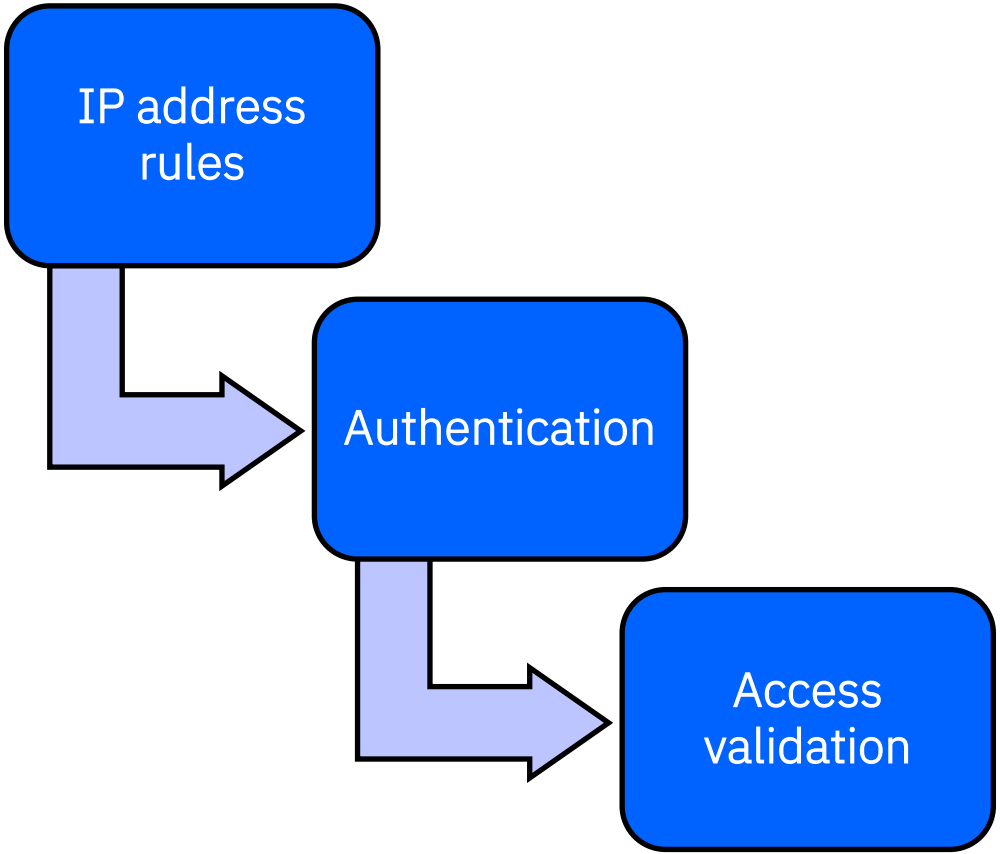
Centrally control and enforce access

IP address rules

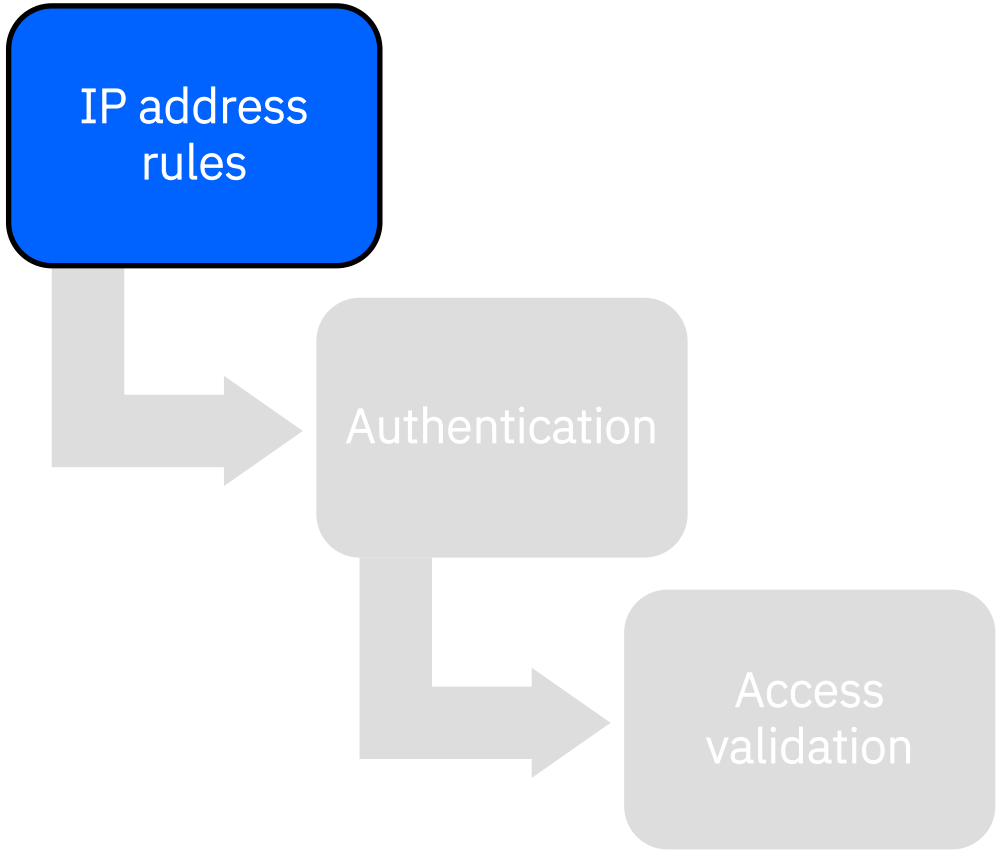
Authentication

Access validation

Order of processing



Order of processing



IP address rules

Requires “Activate IP Address Rules” option to be enabled

Define IP address or range to which the rule applies

- Multiple definitions are allowed
- Dynamically add, modify, delete rules
- IPv4 and IPv6 supported
- Wildcards are supported as trailing characters
- Most specific rule takes precedence
  - Similar to RACF
  - Create a general rule then create overrides with more specific IP addresses

Examples

IPv4	192.23.88.1
IPv6	2001:0db8:85a3:0000:0000:8a2e:0370:7334
IPv4 wildcard	192.55.*
IPv6 wildcard	0:0:0:0:0:ffff:c017:*

IP address rules

Option 1:

Is this IP address blocked?

- Yes: reject request
- No: continue, other rules may apply
- Blocking rule takes precedence

No RACF (SAF) validation

Consider whether this meets your security and audit requirements

Customer use case:

Rogue client on development system

- Looping with invalid user ID
- Flooding IMS log with RACF error messages
- Could block the port but other valid clients using the same port

Solution: Block the IP address

- Dynamically define IP address rule

IP address rules

Option 2:

Override the user ID based on the requester's IP address

- Specify user ID to use as override
- Additional option
  - Only apply user ID override if incoming user ID is blank

Customer use case:

Using customer-written exit to replace user ID based on IP address

- If no IP address match
  - Use a dummy user ID
  - Pass to IMS to fail

Solution: Replace customized exit

- IMS Connect Extensions configuration
- Eliminate maintenance of customized Assembler exit

IP address rules

Option 3:

Do I trust the user ID based on the requester's IP address?

- Yes (set):
  - Set (override) OTMA trusted user flag in OTMA header
    - OMUSR_TRSTUSR in OMUSR_FLAG2 field
- No (clear):
  - Clear OTMA trusted user flag
- Null
  - Leave OTMA trusted user flag unchanged

Customer use case:

Prevent clients from setting the OTMA trusted user flag on incoming requests

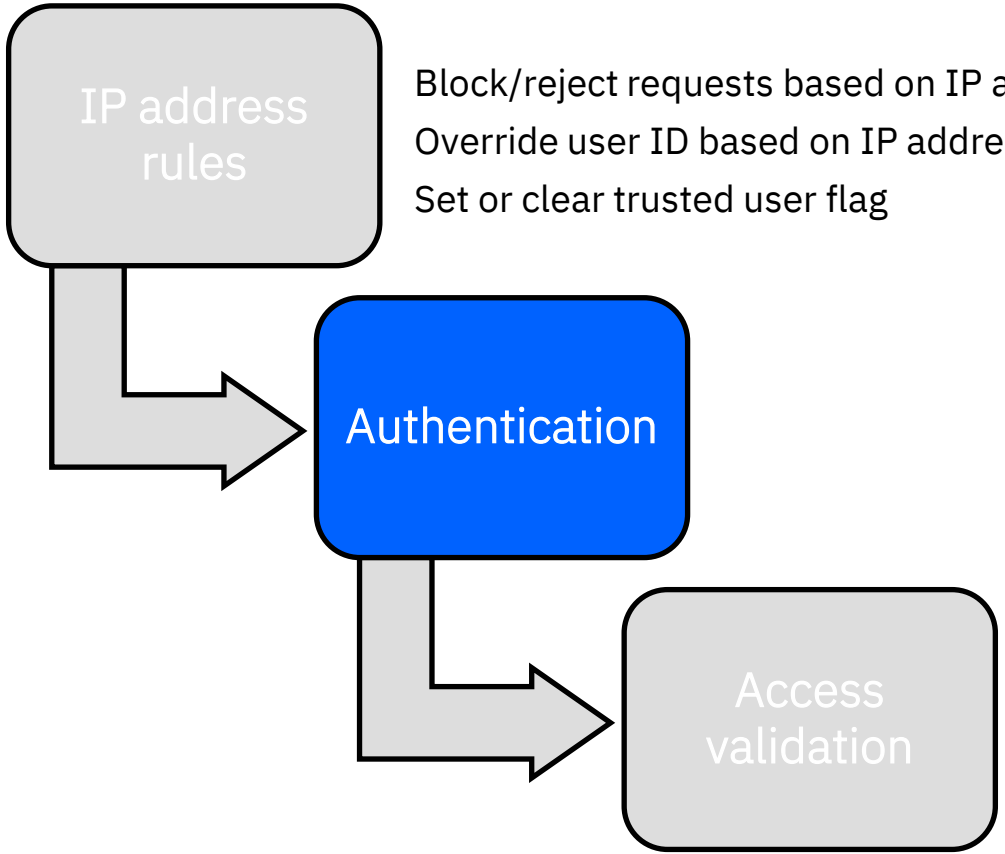
Force the flag off for every request

Remember

You can create one rule for the default and override with other rules

Documentation

Order of processing



Block/reject requests based on IP address

Override user ID based on IP address

Set or clear trusted user flag

User ID authentication

Requires “Activate Security” option to be enabled

Is the request from a valid user ID and authenticator combination?

- Verified through RACF or other External Security Manager
- Supported authenticators: password; passphrase; PassTicket or client certificate for AT-TLS ports (see CLIENTCERT_UID)

What about the overhead of calling RACF so often?

- RACF (or SAF) calls to validate user ID/authenticator pair can be costly
- Option to cache credentials using Accessor Environment Element (ACEE) created by RACROUTE VERIFY
- Specify the aging interval (in minutes)
- Any changes in RACF to authorization levels communicated through ENF 71 events and IMS Connect Extensions clears that user from the cache

Documentation

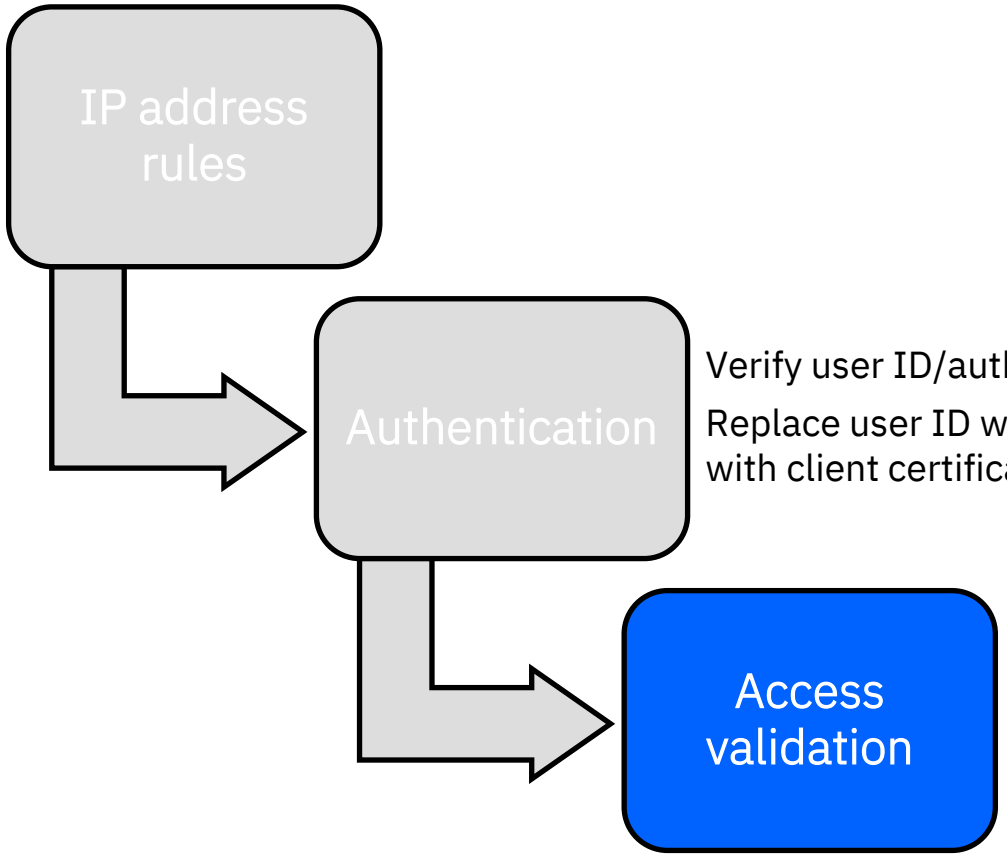
Using client certificates mapped to user IDs

CLIENTCERT_UID option for AT-TLS connections

- In effect when:
  - Client connects to an AT-TLS managed port with an SSL certificate
  - The port is in the CLIENTCERT_UID port list
  - The client certificate has a mapped user ID
- IMS Connect Extensions extracts the user ID and associates it with the request and sets the trusted user attribute
- Certificate option is specified via CLIENTCERT_UID
  - None: Do not check for client certificates, use the user ID provided in the message
  - All: Assign the user ID associated with the certificate for messages received on all IMS Connect ports
  - (*portnum1, portnum2, ...*):
    - For messages received on the listed ports, assign the user ID associated with the certificate
    - For all other ports, use the user ID provided in the message
- In effect regardless of “Activate Security” setting

Documentation

Order of processing



Verify user ID/authenticator pair

Replace user ID with the one associated with client certificate

Access validation

Requires “Activate Validation” option to be enabled

Option 1: Is the user ID authorized to use IMS Connect?

- User ID is credentials of the end user, application server, or TMRA configuration that is used when connecting to IMS Connect
  - Credentials can include password, passphrase, or PassTicket
- User ID must have READ access to the IMS Connect resource (security) class profile in RACF (or other External Security Manager)
- Useful when a limited number of user ID’s issuing requests via IMS Connect

Example using FACILITY class profile:

```
RDEFINE FACILITY ZZSEC01 UACC(NONE)

PERMIT ZZSEC01 CLASS(FACILITY) ID(CEXGRPI) ACCESS(READ)
```

Access validation

Option 2: Is the user ID authorized to use IMS Connect from the client IP address **and** IMS Connect port number?

- User ID must have READ access to a customer-defined resource (security) class profile in RACF (or other External Security Manager)
- Each security class profile name contains the IMS Connect name, a client IP address and IMS Connect port number
  - Typical wildcarding supported in RACF security profile names
  - Wildcards supported in IP addresses as trailing character
- Useful with limited number (or range) of known client IP addresses, IMS Connect port numbers

Access validation

Option 2

Example using XFACILIT class profile:

```
RDEFINE XFACILIT CEX.IPV4.ZZSEC01.129.042.060.030.* UACC(NONE)
RDEFINE XFACILIT CEX.IPV4.ZZSEC01.*.*.*.*.48801 UACC(NONE)

PERMIT CEX.IPV4.ZZSEC01.129.042.060.030.* CLASS(XFACILIT) ID(CEXGRPI) ACCESS(READ)
PERMIT CEX.IPV4.ZZSEC01.*.*.*.*.48801 CLASS(XFACILIT) ID(USRID01) ACCESS(READ)
```

IPv6 also supported

Access validation: Option 2, continued

VALIDATE_TRUSTED option

- No (default): access validation is skipped if OTMA trusted user flag is set to Yes
  - Based on value of OTMA trusted user flag, set by any of:
    - IP address rule
    - Mapped user ID from client certificate
    - Client
      - If no IP address rule or
      - IP address rule did not change trusted user flag
- Yes: access validation (SAF call) is executed regardless of OTMA trusted user flag

Access validation

Option 3: Is the user ID authorized to use IMS Connect from the client IP address, IMS Connect port number **and** Client ID?

- Client ID
  - Unique identifier included in the IMS request message (IRM) for a client application connecting to IMS Connect
    - » Value assigned to a specific dedicated socket connection
  - Can be manually set or automatically generated by IMS Connect
  - Only valid for Commit Mode 0 interactions
- User ID must have READ access to a customer-defined security class profile in RACF (or other External Security Manager)
- Each security class profile name contains a client IP address, IMS Connect port number, and client ID
  - Typical wildcarding supported in RACF security profile names and IP addresses
- Useful with dedicated socket connections from a limited number of known client ID's
- VALIDATE_TRUSTED option – same as Access Validation: Option 2

Access validation

Option 3

Example using XFACILIT class profile:

```
RDEFINE XFACILIT CEX.IPV4.ZZSEC01.129.042.060.030.*.CLIENT1 UACC(NONE)
RDEFINE XFACILIT CEX.IPV4.ZZSEC01.*.*.*.*.48801.CLIENT2 UACC(NONE)

PERMIT CEX.IPV4.ZZSEC01.129.042.060.030.*.CLIENT1 CLASS(XFACILIT) ID(CEXGRPI) ACCESS(READ)
PERMIT CEX.IPV4.ZZSEC01.*.*.*.*.48801.CLIENT1 CLASS(XFACILIT) ID(USRID01) ACCESS(READ)
```

IPv6 also supported

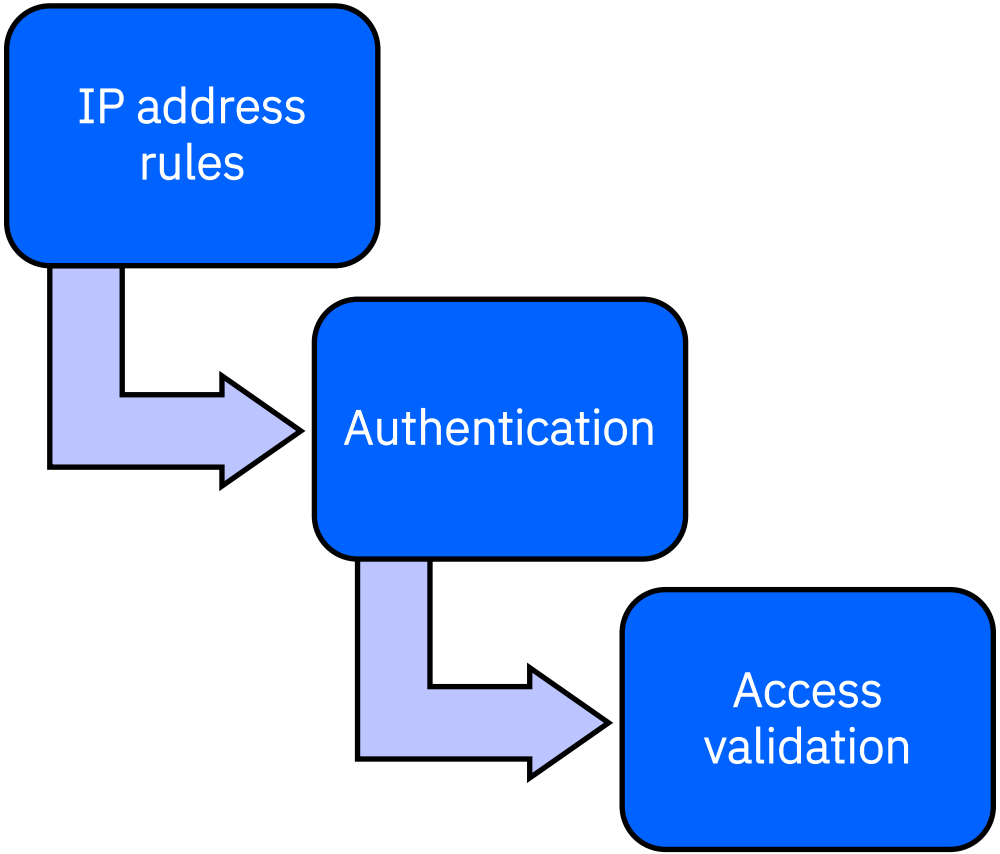
Access validation

What about the overhead of calling RACF so often?

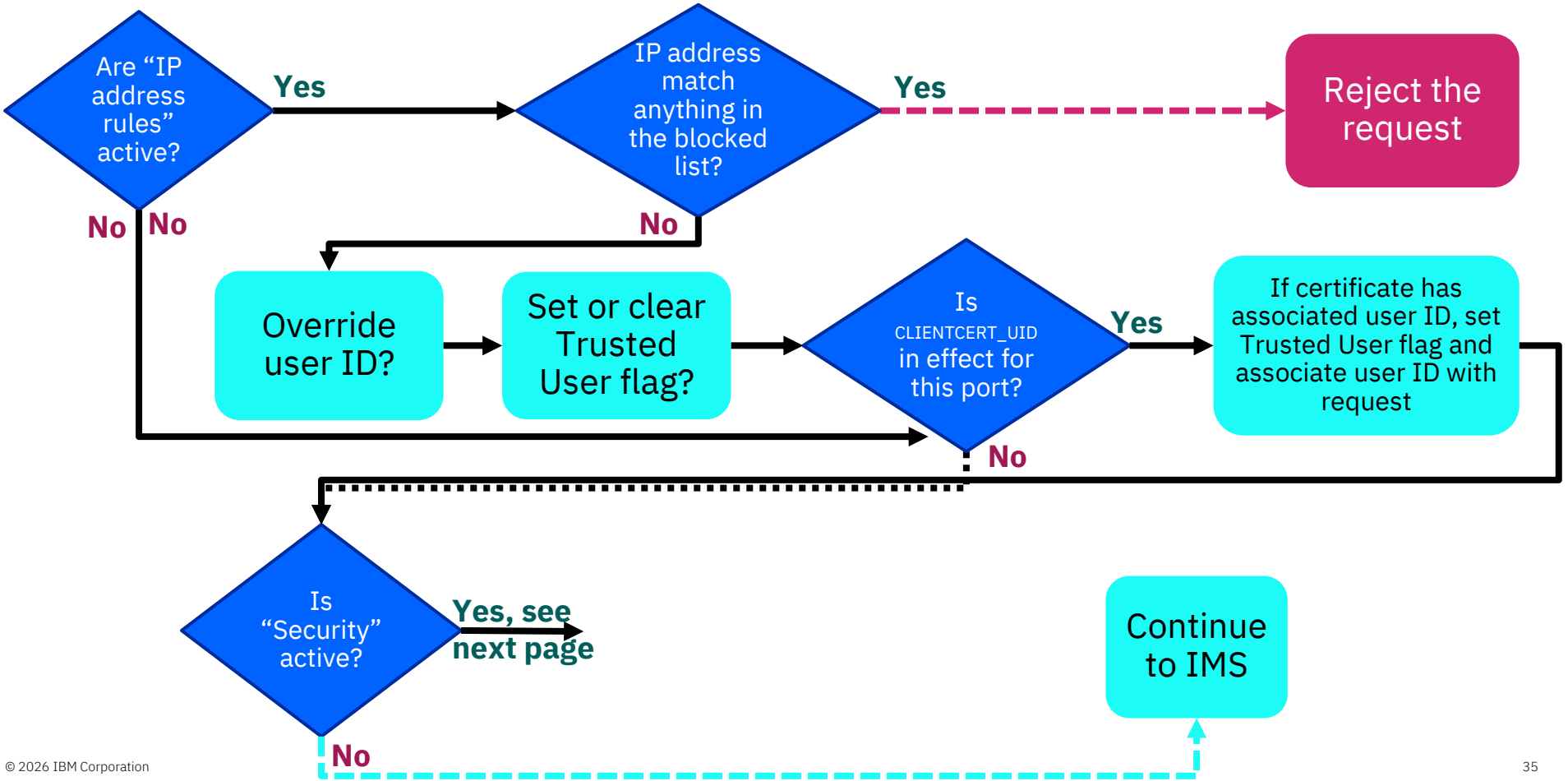
- RACF (SAF) calls to validate access to a profile is not as costly as user ID/password validation
- RACF options implemented in IMS Connect Extensions to reduce time and overhead
  - Preload the appropriate profiles into storage (RACLIST)
  - Issue RACROUTE FASTAUTH

Documentation

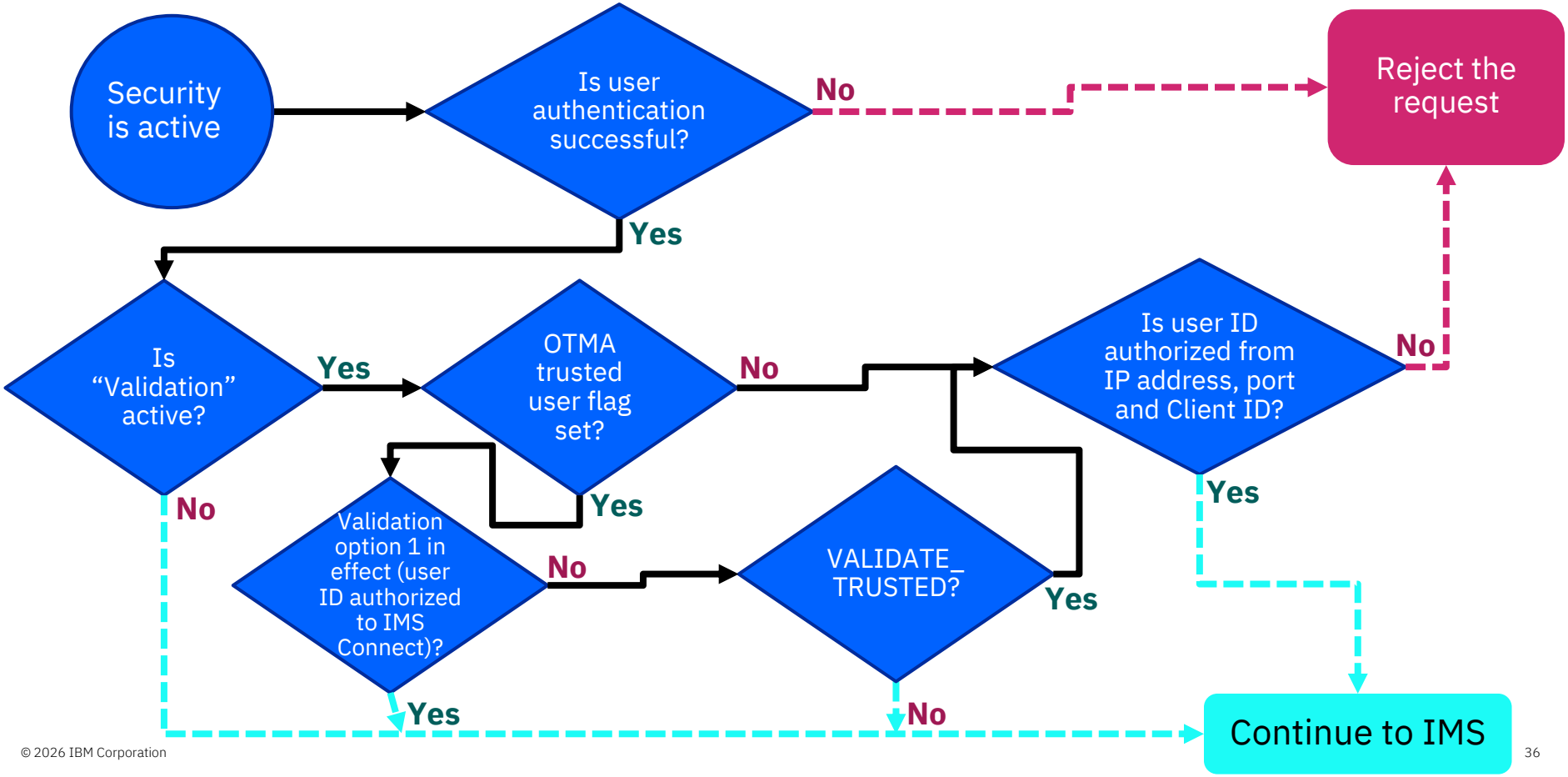
Order of processing



IMS Connect Extensions security flow



IMS Connect Extensions security flow



Case study – securing IMS Connect transactions

z/OS

- Set up all ports to use AT-TLS
- Enable client certificates
  - Implement key and certificate management to provide them to distributed platforms
  - Set up mapping of certificates to user IDs in RACF

IMS Connect Extensions

- Create an IP Address rule to turn off trusted user flag by default
- Turn on VALIDATE_TRUSTED option
- Specify CLIENTCERT_UID ALL
- Implement access validation option 2: user ID authorized to use IMS Connect from the client IP address and IMS Connect port number

Summary and references

IMS Connect is a critical component of IMS for TCP/IP workloads

TCP/IP workloads are increasing

Event data is needed for reporting and problem determination

Workload routing can ensure continuous availability

Security of IMS Connect workloads is crucial

References

IMS Tools website
www.ibm.com/it-infrastructure/z/ims/tools

IBM Z Software Newsletter
http://ibm.biz/zITSMNewsletterSubscribe

IMS listserv
http://imslistserv.bmc.com

Subscribe to notifications about IBM products
https://www.ibm.com/support/pages/my-notifications-subscription-service

IMS Tools support for Data Set Encryption
www.ibm.com/support/pages/ibm-ims-tools-and-data-set-encryption-support

IMS Tools Product Documentation
www.ibm.com/support/docview.wss?uid=swg27020942

IMS Tools new functions
www.ibm.com/support/docview.wss?uid=swg22015506

IMS Tools support for IMS V15
https://www.ibm.com/support/pages/node/7151031

IMS Tools support for Managed ACBs
www.ibm.com/support/docview.wss?uid=ibm10731745

IMS Tools Videos on IBM MediaCenter
ibm.biz/ims-tools-mediacenter

IBM software announcements, end of support dates
https://www.ibm.com/support/pages/lifecycle

IMS Central
https://imsdev.github.io/index.html

IMS Fundamentals videos:
https://mediacenter.ibm.com/playlist/dedicated/122579632/1_b56rpdpt/1_jy8lv5f5

IMS Community (including IMS internship)
https://community.ibm.com/community/user/ibmz-and-linuxone/groups/public?CommunityKey=eba3ada3-db89-4dca-9154-328195f5e560

IMS new functions
https://www.ibm.com/docs/en/ims/15.5.0?topic=enhancements-ims-enhancement-ptfs

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM* IBM Z*
ibm.com
IBM Logo*

*** Registered trademarks of IBM Corporation**

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.
ITIL is a Registered Trade Mark of AXELOS Limited.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
OpenStack is a trademark of OpenStack LLC. The OpenStack trademark policy is available on the OpenStack website.
Red Hat®, JBoss®, OpenShift®, Fedora®, Hibernate®, Ansible®, CloudForms®, RHCA®, RHCE®, RHCSA®, Ceph®, and Gluster® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.
RStudio®, the RStudio logo and Shiny® are registered trademarks of RStudio, Inc.
UNIX is a registered trademark of The Open Group in the United States and other countries.
VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.
Zowe™, the Zowe™ logo and the Open Mainframe Project™ are trademarks of The Linux Foundation.
Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput 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 improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.