z/OS Communications Server

OA49911 - VTAM 3270 Intrusion Detection Services - Overview, Considerations, and Assessment (Prerequisite)

Version 2 Release 2

Note:
Links to related publications are from original documents and might not work. The links to publications are included for reference purposes only.

Contents

Figures

Chapter 1. 3270 IDS overview

The z/OS Communications Server VTAM 3270 Intrusion Detection Services (IDS) function can help alert you to 3270 protocol violations as they occur in real time. This can be useful in identifying potential intrusions that attempt to manipulate 3270 protocol flows with the goal of compromising 3270 SNA applications and data that are deployed on your z/OS systems. This function can detect, in real time, an attempt by a malicious 3270 client emulator to modify protected fields on a 3270 screen. By modifying protected fields, the malicious 3270 client emulator might be trying to subvert the normal processing of the 3270 server application. The effect of such an attempt depends on how well the application guards itself against unexpected changes to protected fields. In the best case scenario, a modification to a protected part of the screen is ignored by the application. In the worst case scenario, it could cause a potentially harmful change in the application's behavior.

Well behaved 3270 client emulator software typically prevents users from entering input into protected parts of the screen. The concern is over malicious users that use 3270 client emulators that do not honor the 3270 protocol and allow changes to protected fields. The 3270 IDS function can detect these types of protocol violations. However, note that SNA 3270 protocol violations might occur without malicious intent. This might be the result of race conditions or lax adherence of the SNA 3270 protocol by software such as 3270 client software emulators, the TN3270 client, session managers, or other SNA based 3270 protocol software. These anomalies might even occur with a regular frequency in your environment and most often go unnoticed as they do not have an impact that is visible to administrators, applications, or users. In some cases, they might cause a temporary error condition on the 3270 client's screen that they can easily recover from. While the 3270 IDS function can flag all detected protocol violations, it cannot determine whether a protocol violation is a malicious attack or an inadvertent anomaly in the 3270 protocol. Additionally, it cannot provide any insight on how a server-side 3270 application deals with these protocol anomalies. In other words, it cannot detect whether an application is vulnerable to a 3270 protocol-based attack or not. The 3270 IDS function simply detects and notifies system administrators of the presence of protocol anomalies, which can be useful as an audit log of potentially suspicious events. In addition to notification, the 3270 IDS function can be configured to take action on the SNA session when a protocol violation is detected, such as terminating the session.

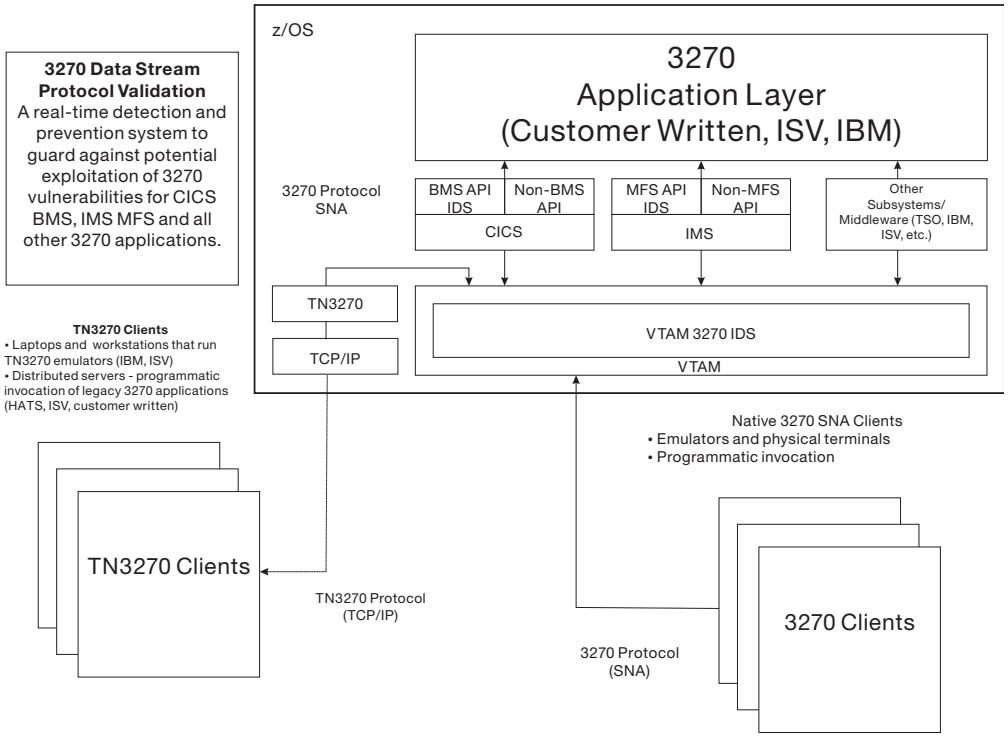

Figure 1. 3270 IDS protection overview

Note: The z/OS Communications Server VTAM 3270 IDS solution is one of several solutions that can provide detection and protection from malicious 3270 attacks.

Figure 1 provides an overview of the following 3270 data stream protocol validation solutions:

CICS basic mapping support (BMS)

CICS provides 3270 IDS detection and protection for any applications that exploit CICS basic mapping support (BMS) interfaces to create and parse their 3270 screens. When this support is activated, CICS monitors the 3270 data streams to detect any attempted modifications to protected fields on the screen. CICS can then provide warnings (log and error message) or prevent the application from processing the data by abending the transaction. See the CICS product documentation through the IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/ for more information on the CICS BMS IDS solution. The CICS BMS IDS solution is available through the following CICS APARs:

- CICS V4R1, V4R2 - PI50363
- CICS V5R1, V5R2 - PI51499 + PI55048
- CICS V5R3 - PI54386

IMS Message Formatting Service (MFS) support

Similar to the CICS BMS, IMS provides 3270 IDS support for any IMS applications that use the IMS Message Format Service (MFS) to format and parse their 3270 messages. When this function is enabled, IMS prevents modifications to protected fields from being passed on to IMS server applications. See the IMS product documentation through the IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/ for more information on the IMS MFS IDS solution. The IMS MFS IDS solution is available through the following IMS APARs:

- IMS V12 - PI51564 - (UI36527 + UI36528)
- IMS V13 - PI46626 - (UI36525 + UI36526)
- IMS V14 - PI51565 - (UI36525 + UI36526)

VTAM 3270 IDS support
The VTAM 3270 IDS support is described in this topic.

ISPF also provides built-in IDS support. ISPF is one of the other subsystems shown in Figure 1 on page 2. Applications that use ISPF services to display their 3270 panels are automatically protected by ISPF. ISPF automatically detects and prevents any modifications to protected areas of the panels from occurring.

The list of 3270 data stream protocol validation solutions is not intended to be an exhaustive list. The other subsystems or other middleware category shown in Figure 1 on page 2 is intended to indicate any other potential application layer 3270 IDS support that might exist but is not identified here.

Note:

- The 3270 client emulators that are used by the 3270 users can use native SNA attachment directly to VTAM or IP attachment through TN3270. The VTAM and middleware 3270 IDS support that is shown in Figure 1 on page 2 covers all 3270 users.
- The terminology in this topic refers to general 3270 validation support, which is different from the specific terminology, such as CICS BMS, IMS MFS, or VTAM 3270 IDS, which refers to validation support within specific products that support the 3270 protocol.

Chapter 2. 3270 IDS considerations and assessment

This topic describes the various factors that you should consider, steps for assessing your exposure to potential 3270 protocol-based attacks, and your potential need for deploying one or more of the 3270 IDS solutions that are described in Chapter 1, "3270 IDS overview," on page 1.

Assessing your environment

If you have workloads that are protected by middleware or native application 3270 validation, evaluate the solutions that are described in Chapter 1, "3270 IDS overview," on page 1 first before you investigate the z/OS Communications Server VTAM 3270 IDS function. Generally, the application solutions have a much lower overhead for IDS processing than the z/OS Communications Server VTAM solution, as they already have existing processing for the processing and handling the 3270 data streams.

The z/OS Communications Server VTAM 3270 IDS function can complement these solutions if you have workloads that you determine are at risk and are not covered by other IDS solutions. As a result, the z/OS Communications Server VTAM 3270 IDS solution is not necessarily required by all z/OS systems or users who have SNA 3270 application workloads. As with any intrusion detection capabilities, you must take careful considerations before you enable a 3270 IDS function. For this reason, the background information is provided here for you to analyze and determine whether this type of IDS function can provide value to your environment. As part of this analysis, you need to understand the z/OS Communications Server VTAM 3270 IDS function, other 3270 IDS options and applicability to your environment, and then assess the risk and cost factors in your environment.

This topic provides information to assist you in your assessment for the potential need of this function in your z/OS environment by evaluating the following aspects:

Applications
: Identify candidate applications and perform a careful analysis of need. See SNA application applicability criteria.

End users, SNA technology and connectivity
: Evaluate the users, key SNA technologies, and network configuration considerations. See exploitation factors and their implications in "SNA technologies, network connectivity, and environmental factors" on page 8.

Exploitation cost
: Understand the cost to exploit this function. See system resource cost and administrative considerations in Exploitation cost.

Complete this assessment carefully, and then consider moving forward with the exploitation of the 3270 IDS function.

SNA application applicability criteria

Is the 3270 IDS function needed in your environment?

Many factors help determine the need for the validation protection that is provided by the 3270 IDS function. To make this assessment, you need background in securing SNA workloads. See the 3270 Emulation: Security Considerations white paper for initial information.

After reviewing the security information in this white paper, you can continue your assessment by using the following key 3270 IDS considerations.

Carefully evaluate your SNA applications for each z/OS system. This topic provides considerations for your SNA application workloads (per z/OS system).

SNA applications

All z/OS systems have 3270 application workloads. At a minimum, the system administrators use various TSO/ISPF functions to maintain z/OS and often to manage other applications. Beyond the system administrators, various applications can exploit SNA APIs that are related to SNA LU0 and LU2 3270 workloads. The first step in your assessment is to identify all of the 3270 applications on your applicable z/OS systems. To assist with this step, use the VTAM operator display command **D NET,APPLS,SCOPE=3270CAND**. This display provides the following information:

3270 candidate applications
: Displays a list of active VTAM applications that have any LU-LU sessions (since the ACB was opened) that qualify for the 3270 IDS monitoring. The qualifying LU sessions must be LU type LU0 with TS profile 2 or LU2 with TS profile 3. Applications that have qualifying LU sessions are potential candidates for the 3270 IDS function.

LU session count
: A cumulative session count (since the ACB was opened) of the number of qualifying LU sessions.

While all applications in this list are candidates, you should initially focus on the applications with the highest qualified LU session counts. After you identify your candidate 3270 applications, you need to evaluate the application 3270 support for each of those applications.

After you identify the applications to focus on, consider whether the VTAM 3270 applications themselves or the middleware under which they run, for example, IBM middleware such as CICS or IMS, offer any native 3270 protocol related validation or protection. As described in Chapter 1, "3270 IDS overview," on page 1, CICS and IMS provide modes (BMS and MFS) for their applications to exploit 3270 communications that also provide 3270 protocol validation. You should first evaluate the data validation support that is provided by the IBM middleware and possibly by the application programs themselves. You might need to consult with the CICS or IMS application programming staff to understand what modes are exploited. If the VTAM 3270 application does not run under a middleware environment that provides its own 3270 IDS function, you need to consult with the application support staff or supporting documentation for the application.

If protocol validation is offered by the middleware or application, enable its support. The 3270 middleware or application is typically in a better position to

perform this type of protocol validation. With an existing understanding of the 3270 data stream context, middleware and application validation is typically much more efficient than the VTAM IDS approach. The application can also provide for some error recovery, retries, or have the capability to ignore certain anomalies or error conditions.

Figure 2 provides an overview of the candidate application assessment process. For each candidate 3270 application, start your assessment here.

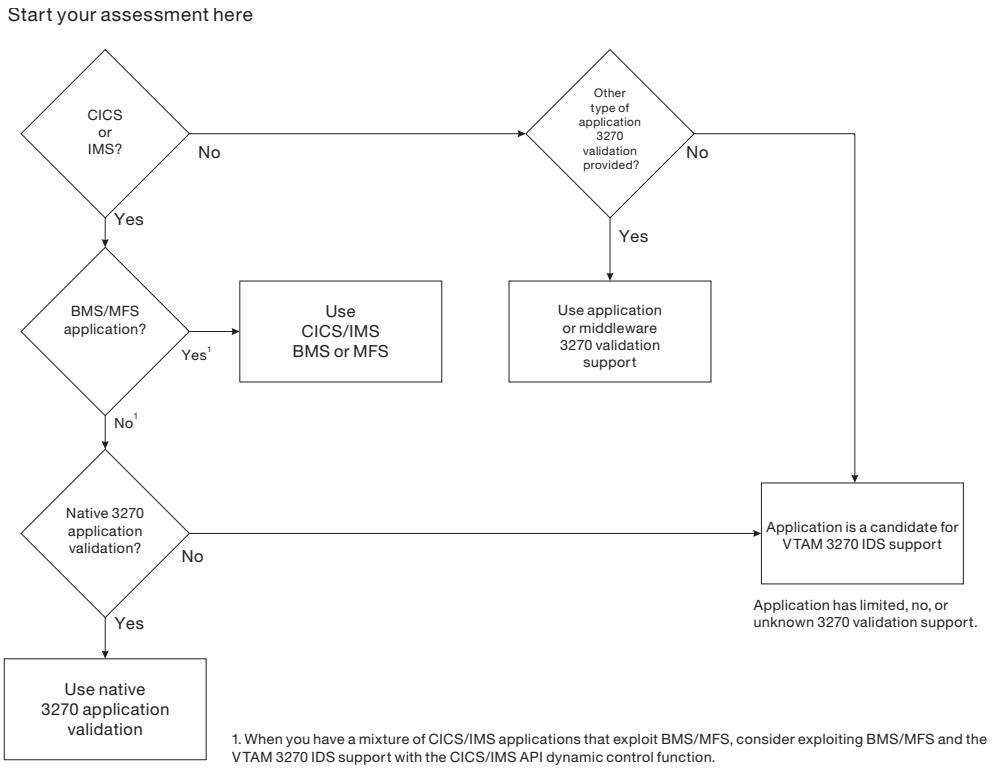

Figure 2. Candidate application assessment process

After you complete your assessment of the candidate applications and their native 3270 validation support, you might determine that the VTAM 3270 IDS validation is not required for your list of identified applications. If you do have a list of candidate applications without coverage or you have a list of potential candidate applications that have unknown validation capability, continue your assessment.

3270 user community of end users

For the identified candidate applications, how well do you understand the configuration and access of your 3270 emulators and the actual end users? For example, who are your end users for each application? Are the users internal or within your company, or are some of them external users? How many users are there?

For the users of each application, what forms of access control and authentication do you have in place for the 3270 users, for example, TLS/SSL, SAF-based, custom written, and so on?

More SNA related aspects are also end user considerations:

- Can you identify or inventory the various SNA components that are used for host access by this set of users?
- What is your level of control and confidence for the security of the following components:
  - TN3270 server products
  - TN3270 client products
  - What products do the SNA session managers support?
  - Do the SNA native connections use TN3270 access? If yes, what 3270 access solutions are being used?

You might not need the 3270 validation for this application, if both the following conditions are met:

- The scope of your end users who have access to your 3270 applications is known and limited.
- The level of control or trust (authentication) you have with the access for those end users (including the control over and integrity of the TN3270 client software and protection it provides) is high.

Consider performing a risk assessment to determine whether the additional protection of an IDS solution is warranted for this application by considering this set of users and the client software used by the users. To complete this part of the assessment, you might need to consult with the 3270 client emulator vendor.

See "SNA technologies, network connectivity, and environmental factors" for more end user related considerations.

SNA technologies, network connectivity, and environmental factors

Figure 3 on page 9 illustrates a typical SNA 3270 network configuration that shows an SNA session manager and a TN3270 server that are located within the same z/OS instance. Several key environmental and configuration aspects are related to identifying and reporting 3270 protocol violations. Some aspects overlap with the previous end user considerations.

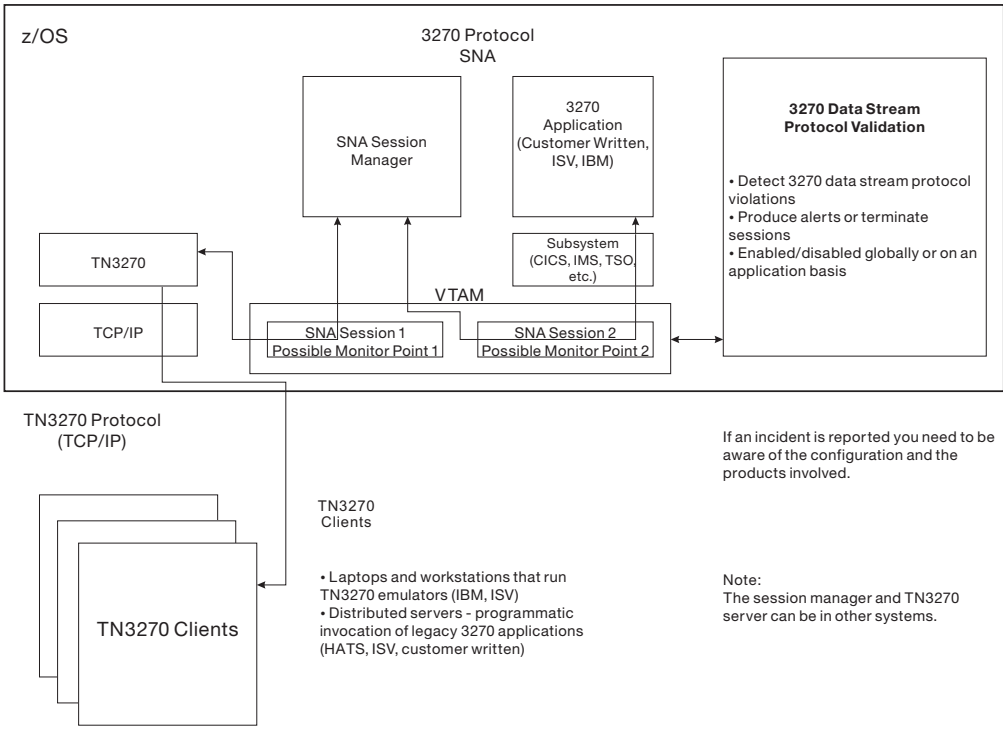

Figure 3. Sample of typical SNA 3270 network configuration

Many variables in an SNA 3270 network can impact the flow of the 3270 data stream. Among these are layers of SNA components, connectivity, and often SNA session management products. The session flow can potentially have an impact on the 3270 protocol validation processing. Consider your unique environmental aspects, for example:

- Systems or network topology: CPU utilization/availability and network topology, network configuration, and network equipment, which can all impact latency that impacts timing.
- Your 3270 related products and vendors, for example, the 3270 application (IMS, CICS, and so on), the TN3270 servers, whether on z/OS or other platforms, the 3270 clients, possible SNA session managers, your end users, and native SNA connectivity when applicable.
- Product compliance, level and compatibility of the SNA LU0 and LU2 3270 protocols, each product in the path of the 3270 data stream, including the 3270 client emulator product, adherence to and implementation of the SNA LU0 and SNA LU2 3270 architecture (including any applicable SNA extensions).
- Your 3270 system and network configuration, physical proximity of resources and IP topology (relative to the 3270 application), the location of the session manager, the TN3270 server and platform, the 3270 client (distance and other network topology aspects) that can all impact timing.

If you have SNA session managers that run on your z/OS system as illustrated in Figure 3, you should disable VTAM 3270 IDS for the traffic between the 3270 clients and the session managers to avoid double validation for the same 3270 data streams. Instead, only perform the validation between the session manager and the actual 3270 application.

It is important to understand that the VTAM 3270 IDS function reports any violation of the 3270 protocol that causes a protected field to be overwritten. The

violation might be the result of malicious activity or the result of unintentional protocol anomalies (inadvertent or transient protocol violations that are caused by things like timing or queuing anomalies).

The VTAM 3270 IDS function cannot make the distinction between a malicious activity versus an unintentional protocol anomaly. Instead, such distinction requires careful analysis of the captured documentation that is associated with the reported incident. In many cases, this type of error can be handled (ignored or retried) by the application.

The frequency of reporting unintentional protocol anomalies varies for each environment. In some environments, the amount or frequency of reporting of unintentional protocol anomalies can be problematic. For each reported incident, you need to perform the initial evaluation to determine the disposition of the IDS incident. If the reported incident is a known unintentional protocol anomaly, that type of incident can be self-managed. If the reported incident is determined to be a malicious attack, you can use the information that is recorded by the VTAM 3270 IDS function to begin your effort to identify the source of the attack. Finally, you might determine that the reported incident is a valid use of the 3270 protocol even though the VTAM 3270 IDS support flagged it. In that case, you might need to work with IBM service to determine the disposition of the incident.

Exploitation cost

System resource cost and other implications of exploitation

Consider system resources (CPU and storage) and administrative costs that are related to the exploitation of the VTAM 3270 IDS function. The actual performance impact of enabling the function varies for each customer environment depending on the scope of the support enabled the application workloads and the type of 3270 traffic.

Processing cost

Internal IBM benchmarks indicate that the IDS analysis that is performed by VTAM 3270 IDS function can result in an increase in CPU use for the SNA application address space, for example, the CICS TOR address space. The amount of increase is impacted by several factors such as the format, complexity, and size of the 3270 screens typically used by the application. The number of LU sessions is another key factor.

If you have SNA session managers that run on your z/OS system, you should disable VTAM 3270 IDS for the traffic between the 3270 clients and the session managers to avoid double validation for the same 3270 data streams. Instead, only perform the validation between the session manager and the actual 3270 application.

Virtual memory cost

Each SNA session that is enabled for the 3270 IDS function allocates approximately 100 K for the session and extra storage for outbound PIU tracking. The VTAM DSCOUNT start option determines how many outbound PIUs to save. The DSCOUNT setting along with PIU (screen) size directly affects the amount of virtual memory that is used to monitor the session. The session-related storage is all 64-bit virtual storage. Total virtual storage can be estimated by multiplying 125 K by total sessions monitored. You need to insure that enough real and virtual memory (paging space) is available before you enable this function on a system. Additionally, insure that system parameters such as MEMLIMIT are set to

appropriate values that do not artificially limit the amount of 64-bit storage that is available to the relevant address spaces.

Administrative cost

Administrative costs are associated with your initial applicability analysis, enablement, and monitoring. Some coordination might be required with the applications administrative staff as well. After the VTAM 3270 IDS function is enabled, each reported incident provides diagnostic data that needs to be evaluated by your staff. This might include network administrators, application developers, other personnel who are familiar with the 3270 data streams in question. If your evaluation concludes that the incident does not reflect any type of protocol violation, you can contact IBM for further assistance.

In some cases, the exploitation of this IDS function might result in persistent and ongoing reporting of similar unintentional protocol anomalies; for example, due to specific vendor products such as TN3270 server, client emulation support, session managers. In such cases, you are required to work with the associated vendor product support staff for a resolution. Pending a resolution, the VTAM 3270 IDS function can be disabled for such workloads.

IBM provides changes for the z/OS TN3270 Telnet Server and the CS Distributed Telnet Server that are related to timing scenarios that can result in reporting of protocol anomalies. For more information about those issues and related changes, see the product support information for those products.

Deployment strategy

After you complete the assessment for each z/OS system and the applicable application workloads on those systems and you believe that your environment can benefit from the VTAM 3270 IDS function, you should consider creating an exploitation plan that enables the support on your systems in a controlled and gradual manner in terms of systems and applications. The objective is to gradually extend the support to the various 3270 application workloads. For example, the support should start with test or development systems for specific applications. After the support is active for a period of time and you have assessed the impact, you can continue expanding the support to other workloads and systems.

Do not code the DSACTION=SENSE option that raises error condition to the z/OS 3270 application or the DSACTION=TERM option that terminates corresponding LU-LU session until you have sufficient experience with a workload and justification for this setting. While you expose more systems and workloads to this validation support, you can assess the impact to your environment and the effectiveness for your workloads.

Known application 3270 solutions provided by IBM

CICS and IMS application 3270 validation support

Both IMS and CICS products provide the following native 3270 validation support:

- CICS BMS data stream protection
- IMS MFS data stream protection

Both of these solutions require less processing and CPU than the VTAM 3270 IDS solution. For more information about the CICS or IMS support, see the CICS or

IMS product documentation for related PTF or base product information.

Application API dynamic control

The VTAM IDS support also provides the capability for applications to dynamically control (enable/disable) the VTAM IDS validation function. With this support, middleware-based IDS solutions can temporarily disable the VTAM IDS function when the middleware IDS solution is actively protecting a session or avoiding dual monitoring of the session when both middleware and VTAM IDS solutions are active for a session. IBM middleware products, such as CICS, IMS, and ISPF, provide this support. For more information about the dynamic IDS exploitation provided by CICS or IMS, see the related product documentation.

TSO/ISPF considerations

TSO users, who are in the ISPF environment, are protected by the ISPF built-in 3270 validation support that is always active. Other TSO environments (non ISPF) need to be investigated and can be a candidate for the z/OS Communications Server VTAM 3270 IDS support. ISPF uses the application API dynamic control when processing ISPF panels.

Index

Numerics

E

S

Printed in USA