3270 Emulation: Security Considerations

Table of Contents

Abstract

3270 data streams have been around since the early days of what has become IBM's z Systems™ family of mainframes. 3270 data streams were originally exchanged between z Systems software and hard wired devices such as display terminals and printers over private connections or closed SNA networks. With the advent of personal computers and workstations, the "dumb terminal" was replaced by software emulators that ran as applications on these "smart" devices. Over time, the traffic between the emulators and the 3270 applications moved from private connections or closed SNA networks to TCP/IP networks, including the Internet. The switch from hardware devices to software emulators introduced the risk of 3270 malware, while the migration to TCP/IP networks greatly increased the risk of unauthorized users attempting to access 3270 applications.

The purpose of this paper is to describe techniques, mechanisms and strategies for minimizing z Systems exposure to the above risks. The paper is organized into the following topics:

1. **Introduction and background**
   describes concepts and background upon which this paper is based.
2. **Controls for protecting TN3270 traffic**
   several chapters that address the following topics:
   - Administrative and network-based controls
   - z/OS® controls
   - z/VM® controls
   - z/VSE® controls
   - A brief discussion about Linux on z Systems and z/TPF
   - Distributed TN3270
3. **Conclusion**
   which summarizes this discussion.

This paper is written for enterprise networking personnel with responsibility for IBM z Systems software platforms. While some basic background is supplied, the reader is assumed to have a basic understanding of TCP/IP, TN3270 and its configuration in the reader's specific environments, SNA, and network security technologies like firewalls, packet filtering, IPsec, TLS/SSL and intrusion detection.

Disclaimer

This paper is provided on an “as-is” basis. IBM makes no warranties or representations with respect to the content hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. IBM assumes no responsibility for any errors that may appear in this document. The information contained in this document is subject to change without any notice.

As always, IBM recommends that z Systems customers subscribe to the IBM z Systems Security Portal (for more subscription information, please visit **http://www.ibm.com/systems/z/solutions/security_subintegrity.html**) and maintain their systems on the latest releases.

Chapter 1. Introduction and background

IBM introduced 3270 data streams in the early 1970s as a way to support display devices and printers much more efficiently than could be done with line-mode terminal protocols common at that time. By allowing terminal devices to send and receive complete screens of information instead of one character at a time, the number of I/O interrupts to the host's CPU was drastically reduced, and the efficiency features of the 3270 protocol greatly reduced the amount of data that had to be transmitted between the terminals and the host. As a result, 3270 display devices became extremely popular and a huge volume of enterprise business applications and systems were written using these devices as their end user interfaces. To this day, a great many of these applications and systems play vital roles in large enterprises. Additionally, the use of "screen scraping" has allowed many existing 3270 data streams to continue to flow unchanged while the associated presentation services have evolved to modern web-based user interfaces.

With the advent of personal workstations, distributed computing, TCP/IP networks and the World Wide Web, large enterprises have evolved away from dedicated 3270-based display terminals, printers, and their related hardware infrastructure. There has also been a migration from native SNA networks (over which much 3270 traffic was carried) to an infrastructure based on TCP/IP networks, 3270 terminal emulators and, of course, web-based technologies.

These changes bring new considerations for system maintenance and network security. For example, carrying SNA traffic over IP networks instead of their native network infrastructure requires prudent use of SNA and IP-based security technologies to secure that traffic (this topic is explained in great detail in the IBM White Paper entitled *Securing an SNA Environment for the 21st century*). Likewise, the use of software 3270 emulators provides new opportunities for malicious software to attempt unauthorized access to 3270 applications. This is especially true when those emulators connect to a z System using the TCP/IP-based TN3270 protocol.

Given this landscape, enterprises need to ensure that only trusted users using trusted emulators have access to a z System's 3270 applications. To this end, enterprises must take care in controlling access to their z Systems 3270 applications, authenticating the endpoints of their TN3270 connections, and maintaining controls over the TN3270 emulator software used to access their systems.

This paper will explore each of these topics and some of the mechanisms available within the different z Systems environments for enforcing these measures. Before we dive into specific measures, however, let's cover some of the important background for our discussion.

IT Security at a glance

Understanding what IT security requirements are and what types of controls are available has become vital in creating a cohesive security strategy. While this paper does not intend to give the reader a deep understanding of all security concepts, the writers do want to convey the basics of IT security to the novice reader.

In general, all IT security falls into one of five categories; physical, policy, platform, application, and network.

Physical Security – Physical security consists of the actual controls that exist to protect the computer hardware system. They can range from low tech measures such as human security guards, to the latest technologies, such as retinal scanners. Within the scope of z Systems, the physical controls deployed should make sure that the production level z Systems hardware systems are protected in a high security area with controlled access. In the past, 3270 terminals were connected through specialized controller devices or LANs over which SNA protocols flowed natively.   As terminal emulators and TCP/IP networks replaced dedicated devices, 3270 traffic flows more in the open, which causes heavier reliance on the four other security categories to ensure 3270 protection.

Policy Security – Policies can be used to restrict resources or data to certain individuals. Security polices allows an enterprise to set limits to the level of access to different resources within the network. This allows an enterprise to protect its resources in a way that relates to the goals of the organization. Within the TCP/IP realm, this could mean defining rules that govern which IP nodes or IP-based applications can communicate with each other across the network. Within the 3270 realm, this could mean defining rules that govern which 3270 clients are allowed to connect with the 3270 services on z Systems.

Platform Hardening - Application platforms are required to deliver data in a secure, reliable fashion, with assurances that data integrity, confidentiality and availability are maintained. One way to achieve this is to ensure the platforms are installed and maintained in a manner that prevents unauthorized access, unauthorized use, or disruptions in service. The process of assuring data integrity, availability, accountability and preventing unauthorized access to resources is called platform hardening. Within the scope of this paper, this could mean strong controls over which 3270 emulation software is allowed on client workstations or preventing unauthorized access to the z Systems host's TN3270 configuration files or datasets.

Network Security – Network security controls protect system resources from external security threats and the data while it is being transmitted. Some examples of network security controls for the IP world include firewall devices, intrusion detection devices, host-based IP filter tables, Virtual Private Networks

(VPN), and proxy servers. When discussing 3270 communications security, this could include (but is not limited to) IPsec VPNs for Enterprise Extender (EE) links, and TLS/SSL security for TN3270 connections.

Application Security – Application security is the step application programmers must take to protect data that is stored or sent by that application. This security is independent of what the operating system is doing. While application security is usually beyond the reach of the infrastructure pieces, each application on each platform should be examined to understand what sort of security mechanism are offered. For 3270 applications this means ensuring security controls are not bypassed by manipulating 3270 input data.

CIA triad of Security – The types of security discussed in the previous section are used to satisfy an enterprise need for the CIA triad of security. CIA stands for Confidentiality, Integrity, and Availability.

- Confidentiality is the assurance that data in any state cannot be understood by those for whom the data is not intended.

- Integrity is the assurance that data is only modified by those authorized to do so, and that it is not unintentionally altered while in transit or while at rest.

- Availability is the assurance that services will be available when an authorized user accesses them. This concept, while not always considered from a pure security perspective, addresses topics like fault tolerance, performance, and protection of system resources from things like denial of service attacks.

Addressing these three fundamental elements provides a solid foundation upon which enterprises can do business securely in today's connected world.

Before we leave this topic, we should note two very important concepts underpin the above fundamentals. The first is *authorization*, which is the process of ensuring that only the users with permission to access or modify a given object are allowed to do so. Access controls are a common mechanism for ensuring authorization. The second of these concepts is *authentication*. In order to enforce authorization rules, we must first be sure that a user really is who they claim to be. Authentication is the process of verifying a user's identity for such purposes. As we explore the various security mechanisms available on z Systems, we will see that each one addresses at least one of the CIA fundamental elements, often incorporating some form of authorization or authentication capability.

3270 data stream overview

While it is beyond the scope of this paper to provide an in-depth description of the 3270 protocol and characteristics of 3270 emulators, it is important to survey the main principles of these topics to provide proper context for readers with little 3270 knowledge. This section provides such a survey.

Fundamentals

The 3270 data stream protocol is based on a connection-oriented half-duplex communication model. It supports a variety of terminal screen geometries (measured in character width and height) and allows full addressability to every portion of the screen using very rich set of instructions. The data streams contain a combination of control instructions, presentation metadata, and the actual data to be displayed or that has been entered by the user.

In a typical sequence, once the 3270 session is established between the terminal and the application:

- The application generates a screen designed to collect user input and sends it to the terminal.
- The terminal receives the stream from the application and displays the screen. It then waits for the user to enter appropriate input values. Once that's done, the terminal packages the user input into a data stream and sends it back to the application.
- When the application receives the input data stream, it attempts to use the input data fields to drive the application's business logic.

While this is an overly simplified example, it illustrates the basic idea model and idea behind the 3270 protocol. The protocol is extremely flexible in the operations, field definitions, screen addressing, and display attributes it supports. Complete details of the 3270 protocol are explained in the following IBM publications:

- *3270 Information Display System - Data Stream Programmer's Reference (GA24-0059).*
- *SNA Formats (GA27-3136)*
- *3174 Establishment Controller Functional Description (GA23-0218)*

While this paper focuses on 3270 display terminals, it should be noted that the 3270 protocol also supports a full set of printing functions as well as the ability to transfer files between 3270 applications (including terminal emulators).

As we already briefly mentioned, 3270 connectivity has evolved quite a bit over time. For many years, 3270 terminals were connected by coaxial cables to a control unit that was connected to the host system over a channel (either natively or using SNA) or a remote (BSC or SDLC) link. While a small number of these connections are still in use today, the original remote access methods have been abandoned in favor of more modern IP-based protocols.

The first terminal emulators used special coaxial adapters to provide connectivity between the personal computer or workstation and the control units. As LAN technologies grew in popularity, IBM introduced LAN-attached control units, eliminating the need for the special purpose coaxial adapters. Later, SNA LU type 2 connectivity made it possible for emulators to connect directly to the host over the LAN, completely eliminating the need for the control units.

Eventually, as IP networks became prevalent, IBM provided two methods for connecting 3270 terminal emulators and hosts over IP: Enterprise Extender, which encapsulates SNA traffic over UDP/IP, and TN3270, which provides for the encapsulation of 3270 data streams over native TCP/IP connections. These are by far the most prevalent connection types in use today.

Given this brief history lesson, the following figure provides a high-level view of today's 3270 connectivity options:

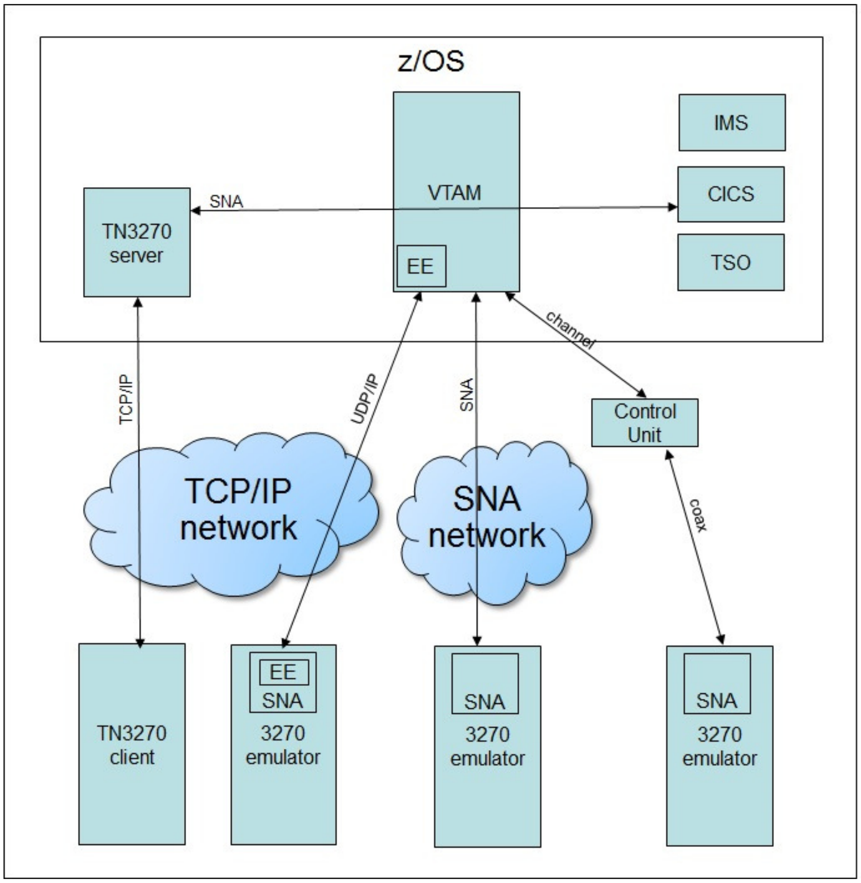


Figure 1 3270 connectivity options

For a discussion regarding the security of pure SNA connectivity (as shown for the three terminals on the right side of the above diagram) as well as

Enterprise Extender connectivity (as shown for the second terminal from the left), refer to the IBM White Paper entitled *Securing an SNA Environment for the 21st century*). Also note that direct channel attachment (as shown for the rightmost terminal) is rarely used nowadays. When it is used, it is usually within the local confines of the data center that houses the z Systems.

For the remainder of this paper, we will focus on TN3270 connectivity.

TN3270

TN3270's purpose is to act as a bridge between the IP and SNA worlds for 3270 terminal emulators. TN3270 servers can reside on the target platform (onboard TN3270) or on an intermediate network node between the emulator and the target system (outboard TN3270). Figure 2 and Figure 3 illustrate the general architecture for inboard and outboard TN3270, respectively, using a z/OS system as the target platform.

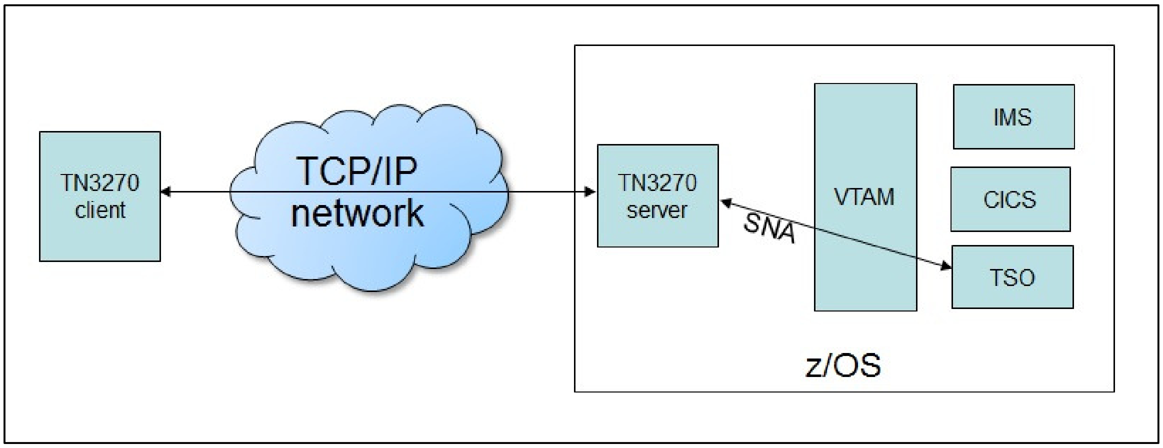


Figure 2 TN3270 inboard architecture

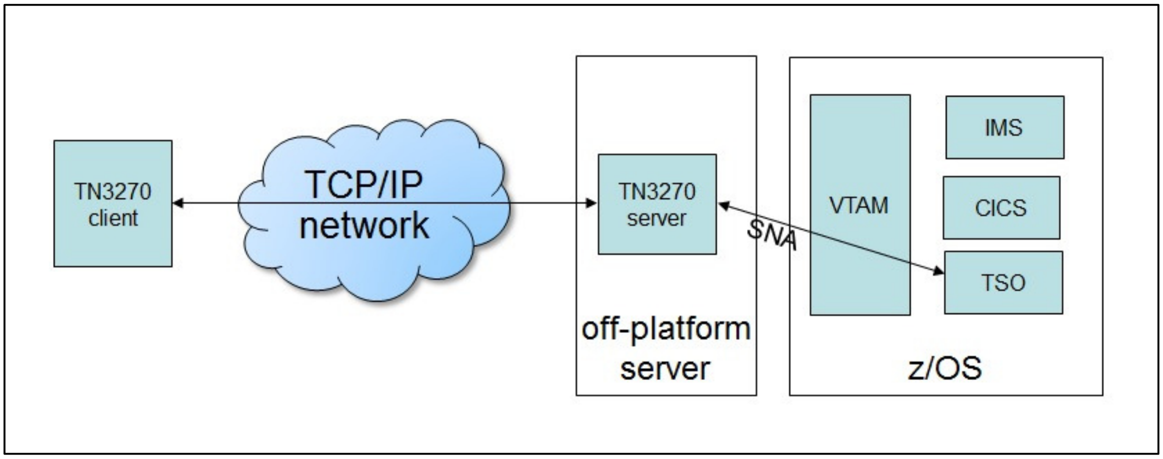


Figure 3 TN3270 outboard architecture

In either architecture, TN3270 clients (the software emulators) connect to a TN3270 server over a TCP/IP network. When a client establishes a new session with the server, the client authenticates itself to the server and identifies the target 3270 application. On the client's behalf, the TN3270 server establishes a proxy connection over SNA to the target application. At that point, the application will often require the end user to authenticate him/herself before allowing the connection to proceed. Once connected, the client and server exchange 3270 data streams that flow natively over the SNA connection between the application and TN3270 server, and over the TCP/IP network between the TN3270 server and the TN3270 client.

While the 3270 protocol was defined by IBM, TN3270 is based upon the standard telnet protocol as described in RFC 854 and its related RFC. Over time, TN3270 was extended beyond as described in the following RFCs:

- RFC 1041 - Telnet 3270 Regime Option
- RFC 1576 - TN3270 Current Practices
- RFC 1647 - TN3270 Enhancements, which describes the protocol sometimes called TN3270D.
- RFC 2355 - TN3270 Enhancements, which obsoletes RFC 1647 and describes the TN3270E protocol.

Chapter 2. Administrative and network-based controls

Before we begin examining the plethora of technology-based protection mechanisms for securing your TN3270 traffic, it is important to consider the administrative measures that enterprises can employ to minimize their exposure to errant or malicious actors.

Software asset management

One of the most effective measures available for controlling your 3270 landscape is to use a comprehensive Software Asset Management (SAM) approach within your enterprise. Specifically, employing software inventory and deployment controls which scan client workstations for installed software and strictly enforce rules regarding which TN3270 emulators are allowed to be installed on client workstations can help ensure that only trusted emulators are being used by your 3270 clients.

Keep in mind that simple executable files can be run from any external drive or USB device and might not need to be installed or registered. As such, taking measures to restrict the installation or execution of programs from external drives or USB devices can be effective in minimizing the risk of an untrusted emulator being used within your enterprise.

Separation of environments

One of the fundamental principles in IT security is keeping systems with different purposes logically separated from each other. In most data centers using z Systems, three types of Logical Partitions (LPARs) are deployed for regular use:

- Production LPARs running the core business for business users
- Development LPARs for development and testing of new applications
- Test LPARs, often deployed in groups, in which system programmers test changes and new software versions before deploying them into production.

Because each type of system caters to a different type of user, they typically have different security requirements. For example, test system users usually have much more access to operational controls on their LPARs than would be given a similar user on a production or development LPAR. It is a good idea to review the user IDs that your users own on systems of various types. For example, do your developers really require user IDs on your production systems?

Enterprise systems should be logically separated from each other such that there is no connectivity between them as so that only users with an appropriate need for access to a given system are permitted that access.

Role-based access controls

Before considering specific access control technologies, an enterprise must have a clear understanding of their user population and the need for access to their 3270-based applications. By assigning users to roles and controlling access based on those roles, the task of ensuring appropriate access to these applications becomes quite manageable.

Firewalls

The use of network-based firewalls is an important component of any comprehensive IP network security strategy, including those that carry TN3270 traffic. Firewall rules should be defined to narrow TN3270 server (both host address and port) access to only those hosts or subnets that require it. The more narrow the rules, the better control you will have over access to the TN3270 server.

IDS/IPS devices

Network-based Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS) are also very powerful tools in protecting your IP networks. These devices perform deep packet inspection on network traffic as it traverses the network looking for a wide variety of attack signatures, from the network layer all the way up to the application layer. To date, however, the number of 3270-related attack signatures supported by these devices is minimal.

Chapter 4. z/OS controls

This chapter provides an overview of the key security features of z/OS Communications Server that can help in securing TN3270 traffic. Note that this chapter only discusses the subset of security features that are specifically relevant to TN3270 – it is not a comprehensive survey of all the Communications Server security functions.

z/OS Communications Server provides a TN3270E server as a standalone started task. This server supports both the TN3270 and TN3270E protocols, is extremely scalable and provides numerous features that help control access to the server and secure TN3270 sessions with clients. Since the z/OS TN3270E server is a component of z/OS Communications Server, the majority of the security-related features are provide by Communications Server components. These features fall into the following categories:

- SAF-based access controls
- IP filter rules (part of the IP security component)
- Cryptographic network security protocols
- Integrated Intrusion Detection Services
- TN3270E server controls

SAF-based access controls

z/OS Communications Server provides three different SAF resources that system administrators can use to control access to the z/OS TN3270 server.

For more information on these z/OS Communications Server SAF resources, refer to the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*, Chapter 3.

NETACCESS resources

EZB.NETACCESS.*sysname.tcpname.zonename* resources control which z/OS user IDs are allowed to access different network zones. *zonename* definitions are specified in the TCPIP profile data set, with each name corresponding to a host, subnet, or network. User IDs with permission to a given NETACCESS profile are allowed to send and receive data to and from the network zone(s) represented by the *zonename(s)* covered by that profile.

NETACCESS controls provide an additional layer of security on top of any authentication and authorization mechanisms that are used in the network or at the peer system by preventing unauthorized users from communicating with the peer network resource.

NETACCESS profiles can be used to limit the network zones with which the z/OS TN3270E server is allowed to communicate. By default, the user ID under which the TN3270E server is running is used for these checks. However, using the NACUSERID parameter of the TELNETPARMS statement, you can specify different user IDs for different TN3270 ports.

Using NETACCESS profiles reduces the visibility of your z/OS 3270-based applications to only those network zones that require such access, and the NACUSERID parameter allows you to control that visibility on a per-port basis.

PORTACCESS resources

EZB.PORTACCESS.*sysname.tcpname.portname* resources determine which z/OS user IDs are allowed to bind to specific TCP ports. User IDs with permission to a given PORTACCESS profile are allowed to bind to the TCP port(s) covered by that profile.

A specific PORTACCESS profile can be used to ensure that only the user ID under which the TN3270 server is intended to run can bind to the configured TN3270 server port. This can help prevent an unapproved z/OS application from attempting to pose as the TN3270 server on the z/OS LPAR.

TN3270-specific resources

There is one TN3270-specific SAF resource. EZB.TN3270.*sysname.tn3270name*.PORT*xxxx* resources control which z/OS users can access the z/OS TN3270 server based on SAF user ID associated with TLS-authenticated X.509 client certificate. This check is made when the TN3270 profile's TELNETPARMS statement specifies SECUREPORT and CLIENTAUTH SAFCERT.

In this case, once the TLS handshake is complete, the TN3270 server queries the z/OS user ID associated with the client certificate. If that user ID is permitted to the PORT*xxxx* resource, then the connection is allowed. Otherwise, the connection is denied.

For more information on the TN3270 profile statements, refer to the *z/OS Communications Server IP Configuration Reference Version 2 Release 1 (SC27-3651)*, Chapter 16.

IP filter rules

z/OS Communications Server's IP security component includes IP packet filtering that controls the flow of IP packets into and out of the z/OS TCP/IP stack. The IP security component is configured through the z/OS Communications Server Policy Agent.

An administrator can define IP filter rules in their IP security policy to permit or deny any type of IP traffic from entering/exiting the TCP/IP stack. Both local and routed traffic are supported. Filter rules can be defined using a wide variety of criteria, most of which are based on the characteristics of the IP packets themselves. For example IP filter rules can be defined to filter packets based on things like source IP address, destination IP address, protocol, source port, and destination port. Address-based criteria can be specified in terms of single IP addresses, ranges of IP addresses, subnets or even complete networks.

IP filter rules are a very powerful tool for controlling which hosts, subnets, or networks are allowed to reach the z/OS TN3270 server. By limiting the IP addresses that are allowed to reach the TN3270 server, you can greatly reduce the visibility of your z/OS 3270-based applications to only those hosts that need to access those applications.

Note that on the surface, the function of IP filter rules and NETACCESS resources seem rather similar. However, there are important differences:

- Since they are SAF-based, NETACCESS resources operate based on the z/OS user ID of the local z/OS application. For TN3270, this is either TN3270 user ID, or a user ID specified on a NACUSERID parameter, which allows different user IDs to be specified for different TN3270 ports. IP filter rules, on the other hand, operate solely on the characteristics of the IP packet with no consideration for user IDs.

- NETACCESS zonenames are defined in the TCPIP profile data set and NETACCESS profiles are maintained in a SAF-compliant external security manager like RACF®. IP filter rules are configured in IP security policy, which is processed by the Policy Agent. The enforcement of IP filter rules is completely contained within z/OS Communications Server.

- NETACCESS rules generate SMF audit records whereas the messages that report results of IP filter checks are logged to syslogd.

IP filter rules and NETACCESS resources can be used independently or in a complementary fashion to provide multiple levels of access controls for your z/OS-based applications and middleware.

For more information on IP filtering, refer to the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*, Chapter 19.

Cryptographic network security protocols

TLS/SSL

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL) are cryptography-based technologies that are applied just above the transport layer, typically under direction of the application program that is generating the traffic to be protected. SSL was originally introduced by Netscape to protect HTTP traffic, but due to its popularity, the IETF standardized the protocol and renamed it TLS. The most common SSL versions are SSLv2 and SSLv3. Both of these, however, are outdated and known to have weaknesses. Therefore, as a best practice, you should use at least TLSv1.0 with a preference toward using the most current TLS version (at the time of this writing, that version is TLSv1.2).

TLS/SSL provides peer authentication through the use of X.509 certificates as well as data authentication, data integrity and data confidentiality protections. There are two “modes” for peer authentication:

- *Server Authentication* mode, in which the server must present its certificate to the client during the TLS handshake in order to prove its identity. This mode is fairly simple in regards to the administrative requirements, but it does not provide a mechanism for the server to authenticate its clients. While this approach is sufficient for many applications, it is not ideal for the enterprise that wants to closely control client access to its TN3270 servers.

- *Client Authentication* or *Mutual Authentication* mode, which builds upon Server Authentication. In this mode, the client, after successfully authenticating the server’s certificate, sends its own certificate back to the server (again, as part of the TLS handshake) to prove its identity to the server. While this mode is more burdensome in terms of the number of certificates that must be issued and managed, it provides a more complete peer-to-peer authentication model. For an enterprise that wants to closely control access to its TN3270 servers, this is usually the preferable approach.

System SSL, a component of the z/OS Cryptographic Services element, implements TLS (versions 1.0, 1.1 and 1.2) and SSL (versions 2 and 3) on z/OS. System SSL can either be invoked directly through its own set of APIs or it can be invoked transparently on the application’s behalf based on z/OS Communications Server Application Transparent TLS (AT-TLS) policies. AT-TLS policies are managed by the z/OS Communications Server Policy Agent.

The z/OS TN3270 is fully enabled for TLS/SSL protection through AT-TLS through the use of the TTLSPORT parameter in the TELNETPARMS statement of the TN3270 profile. It also provides a direct integration with System SSL (by specifying SECUREPORT), but this feature is no longer being enhanced by IBM. Therefore, in order to take advantage of the latest TLS versions and any new features that may be added to System SSL, the best practice is to use AT-TLS to protect your TN3270 traffic.

Because of the protections it provides, good TLS/SSL support is something you should seek out when choosing TN3270 client software. Note that in order to establish a TLS/SSL session, both the client and server must agree on the TLS/SSL version as well as the set of cryptographic algorithms (expressed in *cipher suites* within TLS and SSL) to be used. As such, the TLS/SSL capabilities of your 3270 emulation software will help determine which TLS protocol and cipher suites to use to protect your TN3270 traffic.

For more information on System SSL, refer to *z/OS Cryptographic Services System Secure Sockets Layer Programming Version 2 Release 1 (SC41-7495).* For more information on AT-TLS, refer to *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*, Chapter 22.

IPsec

In addition to IP filtering, Communications Server's IP security function provides a complete IPsec protocol implementation. IPsec is a collection of cryptographic protocols that allow participating peers to establish a wide variety of VPN tunnels between themselves. z/OS applies IPsec protection under the direction of IP filter rules that specify an action of "protect with IPsec."

IPsec provides cryptographic protections that are very similar to those provided by TLS/SSL, and both sets of protocols support a very similar set of cryptographic algorithms.

With its related Internet Key Exchange (IKE) protocols, IPsec provides mutual peer authentication through the use of either X.509 certificates or pre-shared (configured) keys. Of these two approaches, X.509 certificates are much preferred.

IPsec can also provide data authentication, data integrity and data confidentiality protections. The type of protection depends on which specific IPsec protocol is chosen. The recommended protocol is Encapsulating Security Protocol (ESP) since it is the only one that can provide data confidentiality (encryption). The other choice, Authentication Header (AH) provides data authentication and integrity protection, but allows the data to flow in the clear.

Like TLS/SSL, both IPsec peers need to agree on the IKE protocol (there are multiple versions and modes), the IPsec protocol (ESP or AH), and the set of cryptographic algorithms to be used for various purposes. This means that capabilities of the non-z/OS peer IPsec implementation will affect the protocols and cryptographic algorithms you can use to protect your traffic.

IPsec is an alternative to TLS/SSL for cryptographically protecting your TN3270 traffic. However, there are some important differences. Here are a few things to consider when deciding between TLS/SSL and IPsec to protect TN3270 traffic:

1. While both IPsec and TLS/SSL use X.509 certificates for peer authentication, the authentication is performed at very different levels.

   - IKE peer authentication is based on the IP nodes that serve as the tunnel endpoints. For TN3270, this typically means authenticating the peer host – not the user on the host.

   - For TLS/SSL, authentication is done at the application/middleware layer which allows for authenticating the user – not just the host.

2. IPsec is completely transparent to the application and middleware layer. Because of this, TN3270 is unaware when it is being protected by IPsec. Therefore, when IPsec is used to protect this traffic, TN3270 "thinks" it is operating in cleartext mode. In contrast, when TLS/SSL is used to protect TN3270, the client and server are quite aware of the protection and can offer additional security capabilities (like the CLIENTAUTH SAFCHECK capability described earlier) because of it.

3. On z/OS, IPsec operations on data traffic can be executed on a zIIP processor which can significantly reduce the CPU costs associated with the cryptographic protection. The capability does not exist with System SSL or AT-TLS.

4. Unlike TLS/SSL, wherein each session protects a single type of application traffic, the scope of an IPsec tunnel can be defined on the associated IPsec rule by the administrator. Tunnels can be defined to be as narrow as a TLS/SSL session (protecting a single type of application traffic between two specific hosts) or so wide that a single tunnel can protect all of the IP traffic (TCP, UDP, ICMP, etc.) between the local host and the remote tunnel endpoint. If you are interested in protecting a wide variety of IP traffic in addition to your TN3270 traffic, this flexibility could significantly reduce the number of policy rules you need to define.

5. Unlike TLS/SSL, IPsec protects entire IP packets, including IP and TCP headers. TLS/SSL, on the other hand, protects only the data payload contained in those packets. So if cryptographic protection of the IP and TCP headers is important to you, IPsec provides an advantage.

6. Unlike TLS/SSL, which is always established between two application endpoints, IPsec tunnels can be established between two hosts, between a host and a router (called an *IPsec gateway*), or between two routers (two gateways). This can be useful in cases where cryptographic protection is only required while traffic is traversing a specific portion of the network between the two data endpoints. For TN3270, however, end-to-end cryptographic protection between the

client and the server is usually preferred or required, so this feature may not be applicable to your TN3270 traffic.

Note that the preceding list is not comprehensive. As you consider the above points, you will most likely identify other questions and considerations that will factor into your decision between TLS/SSL and IPsec protection.

For more information on IPsec, refer to the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*, Chapter 19.

Integrated Intrusion Detection Services (IDS)

z/OS Communications Server provides an integrated Intrusion Detection Services (IDS) capability for reporting and, in some cases, taking defensive actions, for a wide variety of intrusion-related events. IDS rules are defined in IDS policies which are managed by the z/OS Communications Server Policy Agent.

Note that integrated IDS is not intended to replacement network-based IDS or IPS devices. Rather, it is provided to complement such devices and provide an additional level of detection that is focused low-level network protocols or z/OS-specific resources.

Integrated IDS provides three main categories of services:

- Scan detection and reporting
- Traffic regulation (TR)
- Attack detection, reporting and prevention

For detailed information on z/OS Communications Server's integrated IDS, refer to the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*, Chapter 18. This chapter not only describes IDS capabilities in detail, but it also provides a strategy for enabling IDS, establishing baselines, and tailoring IDS policies based on those baselines.

Scan detection

Scan detection provides notifications when a remote network node demonstrated behavior that is consistent with an attempt to inventory the resources and services provided by the local z/OS LPAR. While not destructive in and of itself, such scans are often a precursor to an attack as they can provide the attacker with information on potential attack vectors on the local host. While scan detection is not specific to TN3270 or any given application or protocol, it can be useful in building a comprehensive set of defenses on your z/OS LPAR.

Attack detection

Attack detection includes a wide range of checks that look for abnormalities and unusual or unexpected behavior in single packets or across multiple packets. These checks are made in both the network (IP, ICMP) and transport

(TCP, UDP) layers of the TCP/IP stack. While none of these checks are specific to TN3270, we suggest that you at least enable a set of basic checks. For a good starting point, consider using the default set of IDS attack policies defined in the Configuration Assistant for z/OS Communications Server.

Traffic Regulation (TR)

Traffic Regulation falls into two categories: TCP traffic regulation and UDP traffic regulation.

- UDP TR monitors the size of the UDP queues within the TCP/IP stack on a per-port basis and imposes size limits on those queues when high volumes of UDP traffic are encountered. UDP TR is not applicable to TN3270 since TN3270 is a TCP-based protocol.

- TCP TR controls how many TCP connections a given remote node is allowed to establish to a local TCP port based on the current number of unused connections. The goal here is to prevent a single host from monopolizing a given z/OS application. Since the TCP TR algorithm is based on the *current* number of unused connections, it automatically adjusts the number of connections that any given remote node can allocate as the overall number of connections to the given port grows.

TCP TR can be a very effective tool in preventing a denial of service attack on the z/OS TN3270 server (or any other TCP-based server, for that matter).

One other note regarding mechanisms for limiting the number of client connections to a given z/OS port: z/OS Communications Server also allows administrators to define Quality of Service (QoS) policies for their TCP/IP traffic through the Policy Agent. Among its many capabilities, QoS support allows an administrator to define specific connection limits for a given local TCP port. QoS connection limits are sometimes used in conjunction with TCP TR in cases where specific remote nodes must be able to establish connections to a given z/OS TCP application. The QOS limits for a specific remote node are honored by TCP TR as long as the port is not in a constrained state (a state in which the TCP TR limits for the port are being approached).

TN3270E server controls

The z/OS TN3270E server provides a variety of controls for client access, client authentication and data overruns. In addition, related login controls are provided between the TN3270E server and the Communications Server Digital Certificate Access Services (DCAS).

Controlling client access

Numerous parameters supported within the z/OS TN3270 profile data set can be used to restrict client access to the TN3270E server and to the specific

3270 applications that are made visible through the server. Given the richness of this function, a complete discussion of this topic is beyond the scope of this paper. However, we will highlight a few of the more interesting parameters and capabilities here. For specific syntax of each of the TN3270E server profile statements, refer to the *z/OS Communications Server IP Configuration Reference Version 2 Release 1 (SC27-3651)*, Chapter 16.

NACUSERID

This parameter allows administrators to assign different z/OS user IDs to different TN3270 TCP ports for use in network security zone (NETACCESS) checks. See the topics entitled “NETACCESS resources” and “IP filter rules” above for more information.

Mapping function

The z/OS TN3270E server supports a very sophisticated set of mapping parameters for mapping clients to 3270 applications and resources. These controls are located in the TELNETPARMS and BEGINVTAM sections of the profile. They can be very powerful in ensuring that 3270 applications are only accessible to the clients for which they are intended. Many customers use individual BEGINVTAM statements extensively to identify and control their network of TN3270 users.

For a complete discussion on TN3270E server mapping configuration, refer to the heading “Mapping Objects to Client Identifiers” in Chapter 12 of the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*.

To illustrate some of the TELNETPARMS capability available to administrators through the TN3270 profile data set, here are a couple of the key parameters:

ALLOWAPPL

This parameter controls whether access to a target VTAM® application is permitted. The scope of this parameter can include all users, specific LUNAMEs, or LUGROUPs.

RESTRICTAPPL

This parameter indicates that the specified 3270 application(s) are only to be accessed by clients that meet the specific restrictions listed within the RESTRICTAPPL statement. Many types of restrictions are possible, including, but not limited to:

- the specific z/OS user IDs allowed (causes the TN3270E server to prompt the client for a user ID and password or passphrase before allowing access to the 3270 application),
- the specific LU name that must be specified by the client when the connection is initiated,

- the specific IP addresses that are allowed access to the application.

TN3270E LU exits
The z/OS TN3270E server also provides a user exit that allow an enterprise to even further control client access to specific 3270 applications. For more information on these exits, refer to the heading “Telnet LU exit setup” in chapter 16 of the *z/OS Communications Server IP Configuration Reference Version 2 Release 1 (SC27-3651)*.

TN3270 client authentication

As described under the heading “Cryptographic network security protocols” on page 16, TN3270 connections to z/OS can be secured using either TLS/SSL or IPSec. The use of a cryptographic protocol adds multiple dimensions of security to your TN3270 connections, including peer authentication, data authentication and integrity protection, and privacy protection. These technologies can help reduce the potential TN3270 attack surface, allow you to control which users are able to access your TN3270 server and the 3270-based applications it exposes, and can also provide a better audit trail should a misbehaved emulator be detected.

The z/OS TN3270E server provides a few different mechanisms for authenticating TN3270 client identities:

- TLS client authentication, as described under the heading “TLS/SSL” on page 16, relies on the TLS protocol implementation to authenticate the identity of the client using the client’s X.509 digital certificate. Used on its own, TLS client authentication ensures that the connecting client is trusted according to the enterprise’s Public Key Infrastructure. However, the TN3270E server supports additional authentication functions that build upon the TLS client authentication protocol…

- For both SECUREPORT and TTLSPORT configurations, you can specify that once TLS client authentication completes successfully, an additional check should be made to ensure that the client’s X.509 certificate identity is associated with at valid z/OS user ID in the system’s SAF-based security manager (RACF or equivalent product). If such an association does not exist, then the connection will be denied, even though the digital certificate was authenticated successfully.

  For SECUREPORT configurations, this behavior is specified using the CLIENTAUTH SAFCERT parameter on the relevant TELNETPARMS statement in the TN3270 profile data set.

  For TTLSPORT configurations, this behavior is specified using the

ClientAuthType SAFCheck on the relevant TTLSEnvironmentAdvancedParms statement in the AT-TLS policy.

- For SECUREPORT, if the SAFCERT check succeeds and an EZB.TN3270.*sysname.tn3270name*.PORT*xxxx* resource is defined for the TCP port, then the TN3270E server will then verify with the SAF-based security manger that the user ID associated with the X.509 certificate identity is permitted to the SAF profile for the PORT*xxxx* resource. If that check fails, then the connection will be denied.

Express Logon Feature (ELF)

Express Logon Feature (ELF) is an enhanced logon solution that allows 3270 clients to log into 3270 applications using their X.509 digital certificate instead of entering a z/OS user ID and password.

ELF is supported in a two tier and three tier network design. In the two tier design, the z/OS TN3270E server supports ELF natively using the EXPRESSLOGON parameter in the TN3270 profile data set. In the three tier design, ELF is supported between the off-platform (non-z/OS) TN3270 server and the z/OS Digital Certificate Access Server (DCAS), which is a component of the z/OS Communications Server. Different IBM host access products like Host on Demand (HoD) and Personal Communications support ELF.

Specifically, when using ELF, after a successful TLS handshake with client authentication, the 3270 client's X.509 certificate is used to determine the client's z/OS user ID and to generate a one-time password called a *PassTicket* for the 3270 emulator to use to log into the selected 3270 application.

ELF not only reduces the need for user ID / password authentication, but it also provides a form of single sign-on across z/OS-based 3270 applications.

For more information on ELF, refer to the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*, Appendix C. For more information on DCAS, refer to Chapter 32 of the same book.

Data overrun controls

The z/OS TN3270E server provides a set of configuration parameters to protect against data overruns in various conditions (for example, a client stuck in a send-data loop, unresponsive clients, host applications that are not receiving data, and so forth). These protections help ensure that the memory consumed by the TN3270E server does not become constrained. The parameters are:

- MAXRECEIVE - limits the number of bytes received from a client without an End of Record (EOR) being received.

- MAXRUCHAIN - limits the number of chained RUs received from an application without an end of chain (EC) being received.
- MAXTCPSENDQ - limits the number of bytes that are queued in the TN3270E Server to be sent to a client.
- MAXVTAMSENDQ - limits the number of data segments (RPLs) queued to be sent to VTAM.

For a complete list and descriptions of these data overrun parameters, refer to the subheading “Data overrun security” in Chapter 12 of the *z/OS Communications Server IP Configuration Guide Version 2 Release 1 (SC27-3650)*.

Auditing

While not necessarily a realtime control, audit trails maintained by TCP/IP and the various z/OS components described in this section are a very powerful tool in identifying and tracking down suspicious TN3270 traffic.

Each component writes its own set of audit records written using the z/OS System Management Facilities (SMF). Some of the more important SMF records in relation to TN3270 traffic are the following:

- Type 119 Subtype 2 TCP connection termination: Records vital information and statistics including local and remote IP addresses and ports, socket information, elapsed time, number of bytes transferred and so on for each TCP connection that’s terminated through the local TCP/IP stack. initiation: Records a subset of the information that is eventually reported in the associated

- Type 119 Subtype 1 TCP connection initiation: Records a subset of the information that is eventually recorded in the associated Type 119 Subtype 2 TCP connection termination record. As such, it is quite customary to only collect the termination records. However, if you want an immediate record as soon as each connection is initiated, then these initiation records can be useful.

- Type 119 Subtype 21 TN3270E Telnet server SNA session termination: Records vital information and statistics including local and remote IP addresses and ports, SNA LU name, application name, number of bytes transferred, and so forth for each SNA session that’s terminated between the TN3270 server and a TN3270 client. The information in this record relates to a given LU-LU session, and not to the TCP/IP Telnet connection; for example, if multiple LU-LU sessions use the same Telnet connection, separate SNA session initiation records for each LU-LU session are reported.

- Type 119 Subtype 20 TN3270E Telnet server SNA session initiation: Records a subset of the information that is eventually reported in the associated Type 119 Subtype 21 TN3270E Telnet server SNA session termination record. As such, it is quite customary to only collect the termination records. However, if you want an immediate record as soon as each session is initiated, then these initiation records can be useful.

Searching and sorting through large volumes of SMF records can be a very labor intensive and time consuming task. IBM Security zSecure suite of products provides a rich set of function that can help analyze your SMF records for unusual activity and detect suspicious activity as it happens. For more information on IBM Security zSecure suite, visit http://www.ibm.com/software/security/products/zsecure/index.html

Chapter 5. z/VM controls

The z/VM hypervisor provides a TCP/IP suite of virtual machines as a standard component of its primary product offering. This feature is comprised of several predefined virtual machines which are defined by default by IBM when z/VM is ordered. That said, steps must be taken to enable and configure TCP/IP and TN3270 traffic to the hypervisor.

This chapter provides an overview of TCP/IP and TN3270 on z/VM and its associated security mechanisms.

Note: The TCP/IP services for z/VM apply primarily to the hypervisor layer of a z/VM installation. Guest operating systems running under z/VM (z/OS, z/VSE, Linux on z Systems) will have their own TCP/IP stacks and configurations. Review pertinent chapters of this document for further information.

TCP/IP on z/VM

TCP/IP for z/VM provides network services based on an implementation of a TCP/IP stack. TCP/IP for z/VM runs in a CMS virtual machine (by default, called 'TCPIP') and supports connectivity on the link, network, transport, and application layer as defined by ISO/OSI. The TCP/IP application implements the Telnet protocol; this allows the remote access of virtual machines through Telnet.

TCP/IP listens to the respective network ports and manages all IPv4 and IPv6 traffic between virtual machines and the Internet or other external networks. Routing of traffic is done by TCP/IP for z/VM by using the communication channels provided by the z/VM Control Program (CP).

The Telnet Server for z/VM

The Internal Client

TN3270 capability is surfaced to z/VM administrators through configuration of the TCP/IP stack. This functionality is referenced as either the 'Telnet Server' or as the 'Internal Client' in IBM documentation. The purpose of the Telnet Server is to allow TN3270 communication to connect to the hypervisor layer – for example, to point a 3270 emulator to a z/VM LOGO green-screen.

Network traffic pointed to a z/VM hypervisor in this fashion is isolated from other virtual networks on the hypervisor, preventing data collision or a cross-contamination of network zoning. Incoming traffic is coordinated through an OSA device attached to the local virtual network. Because network traffic is processed in a distinct virtual machine, data about connections are kept separate from guest workload running on the system as well as hypervisor-level administrators.

z/VM TCP/IP and the Telnet server provide several basic security options, from the timeout of inactive connections to the restriction of activity for well-known ports (0-1023, per IETF standards). These options are described at length in the *z/VM TCP/IP Planning and Customization Guide, Chapter 17.*

Requiring encryption for TN3270 traffic

Since the 3270 protocol does not have built-in security mechanisms, it is recommended that TN3270 traffic to z/VM be cryptographically protected. z/VM supports modern TN3270 emulators that also support TLS/SSL encryption. Encryption by z/VM is handled by the SSL-TLS Server (described in more detail below).

For application configuration, a parameter will be designated to indicate if encrypted connections shall be REQUIRED (i.e., mandatory), ALLOWED, or NEVER accepted. The Telnet Server for z/VM must be configured by adjusting the PROFILE TCPIP configuration file. Specifically, indicate one of the three values listed above on the SECURECONNECTION setting in the INTERNALCLIENTPARMS statement. This setting can be adjusted dynamically.

All handshaking will assume the presence of the server's certificate on both ends of the connection (server and client). The certificate label is specified on the TLSLABEL operand of the INTERNALCLIENTPARMS statement; it must be an upper-case string with a maximum length of eight (8) characters.

In addition to encryption of TN3270 traffic based upon z/VM's server certificate, it is also possible to configure the z/VM Telnet Server to require the TN3270 client of choice to present a digital certificate as well. This certificate will be validated against the certificate database maintained within the hypervisor and enforce that a client be trusted before the possibility of logon is allowed. Client certificate validation is handled through the CLIENTCERTCHECK operand in the INTERNALCLIENTPARMS statement in z/VM's PROFILE TCPIP configuration file.

For more information on the Telnet Server, refer to the *z/VM TCP/IP Planning and Customization Guide, Chapter 17.*

Encryption support for z/VM (TLS/SSL)

Description of the SSL-TLS virtual machines

The z/VM SSL-TLS Server supports both SSL and TLS for the encryption and decryption of connections. The basics of these protocols are described under the heading "TLS/SSL" on page 16. z/VM's cryptographic library is based on z/OS System SSL, also described under the same heading. The specific version of System SSL will vary based upon z/VM release. z/VM 6.3 supports a System SSL version equivalent to z/OS V1.13 with some additional functional enablement.

The SSL-TLS Server is a virtual machine (or pool of like-configured VMs) which work exclusively on behalf of a given z/VM TCP/IP stack to encrypt and decrypt traffic. Cryptography strength is set within the SSL-TLS Server; the determination of requirement is set on a per-application or per port basis (as described earlier in this document).

All releases of z/VM currently under service support TLS 1.0 by default; SSLv2 and SSLv3 are disabled by default. z/VM 6.3 also provides the capacity to enable TLS 1.1 and TLS 1.2 for stronger encryption of data in flight.

Understanding your security policy and cryptographic requirements should be done in advance of configuring the SSL-TLS Server, because its settings cannot be adjusted dynamically.

Protocol selection and compliance modes (z/VM 6.3 only)

Configuration for the SSL-TLS Server is handled in a file called the DTCPARMS file. DTCPARMS is the type of file; the filename will often be the name of the z/VM system or specific TCPIP virtual machine. This file handles settings for specific applications running as part of the TCP/IP suite, as well as some extra configuration options for the TCP/IP and Telnet Servers themselves.

For the SSL-TLS Server, a certificate database containing the Internal Client's server certificate should be specified on the :Parms. tag. Additionally, protocols can be enabled or disabled via the PROTOCOL keyword on that :Parms. tag. For example,

```
PROTOCOL +TLSV1_2
```

would enable TLS 1.2 for any secure TN3270 connections incoming to the TCP/IP stack. Bear in mind that, as SSL and TLS negotiate a specific protocol during the handshaking process, the specification of TLS 1.2 is not a guarantee that any connection will use it unless older protocols are also disabled.

The EXEMPT keyword follows the PROTOCOL keyword on the :Parms. Tag. This keyword can be used to remove specific cipher-suite combinations from processing. TN3270 clients may have a specific set of cipher suites which are supported for encrypted TN3270 connections; administrators should investigate client compatibility before disallowing specific protocols or ciphers when configuring z/VM secure connectivity.

Finally, a MODE keyword can be specified on z/VM 6.3 to enact more stringent requirements related to specific security documents. If compliance to FIPS 140-2 or NIST SP 800-131a is something pertinent to your z/VM installation, this option may be particularly pertinent.

For more information on the SSL-TLS Server, refer to the *z/VM TCP/IP Planning and Customization Guide, Chapter 16.*

User authentication on z/VM

Secure TN3270 connections, when encryption is set to REQUIRED, will complete the handshaking process before the z/VM LOGO screen is presented. This means that verification of the server certificate, the client certificate (if requested), and the negotiation of encryption standards will be handled before either a user ID or password can be entered.

Once the secure connection is established, the user credentials can be verified by either CP or an External Security Manager such as the RACF Security Server for z/VM. User credentials are maintained separately from the digital certificate database, so there is not a one to one correspondence between virtual machines and client certificates. However, maintaining a client certificate for each human administrator is a more reasonable task, especially as there is a small subset of commands which can be executed in advance of virtual machine logon.

Chapter 6. z/VSE controls

This chapter provides an overview of the TCP/IP and TN3270 implementations on z/VSE, along with relevant security features of those implementations.

Two different TCP/IP implementations are available for z/VSE, both from independent software vendors:

- TCP/IP for VSE/ESA from CSI International (CSI)
- IPv6/VSE from Barnard Software Incorporated (BSI)

Both of these implementations support IPv4, while the latter also supports IPv6. They also provide a TN3270 daemon that runs natively on z/VSE. We will explore these implementations and the security features they provide that are relevant to TN3270. Note that this chapter only addresses the subset of security features that are specifically relevant to TN3270 – it is not a comprehensive survey of all the TCP/IP-related security features in the subject products.

For more information on both of these TCP/IP implementations, please refer to their respective bookshelves on the IBM z/VSE documentation page at http://www.ibm.com/systems/z/os/zvse/documentation/index.html#tcpip

In addition to these TCP/IP implementations, z/VSE can use the IP stack of a Linux on z Systems through a special API. This alternative makes a native z/VSE IP stack obsolete, but does currently not provide an own TN3270 daemon. Instead, the TN3270 daemon from IPv6/VSE would have to be used. This implementation is called Linux Fast Path (LFP) and a function of the z/VSE product.

For more information on all of these TCP/IP implementations, please refer to their respective bookshelves on the IBM z/VSE documentation page at http://www.ibm.com/systems/z/os/zvse/documentation/index.html#tcpip

More details about TN3270 configurations are in IBM Redbooks

- Security on IBM z/VSE:
  http://www.redbooks.ibm.com/abstracts/sg247691.html?Open
- Enhanced Networking on IBM z/VSE:
  http://www.redbooks.ibm.com/abstracts/sg248091.html?Open

One final note: This chapter only addresses TCP/IP product versions licensed and distributed by IBM. CSI and BSI may offer newer versions of their respective products that may provide additional functionality.

TCP/IP for VSE/ESA

TCP/IP for VSE/ESA provides a TELNETD daemon that supports the TN3270 and TN3270E protocols.

TN3270E implements two types of telnet daemons. The listener daemon listens on a specified TCP/IP port (for example, PORT 23). When it receives an incoming request, it passes the request to an eligible effector daemon. The effector daemon is responsible for managing the session between the TN3270E client and the VTAM application. You must have one listener daemon for each TCP/IP port that you want to use for incoming telnet traffic and you must have one effector daemon for each concurrent session. TN3270E requires the coordination of resource definitions. The TN3270E client selects the LU name but the installation must still have a virtual terminal of that name defined to VTAM and a TN3270E effecter daemon within TCP/IP for VSE/ESA that specifies that LU name using the TERMNAME parameter. Many VSE sites use the terminal name for security and it is important to note that while TCP/IP for VSE/ESA provides client-specified LU names, the specification of the LU name by the client can still be rigorously controlled by the installation LOGMODEs.

When a TN3270E client attempts to connect to TELNETD, it must specify a port (normally port 23) that a TN3270 listener daemon is listening on. The IP address of the TN3270E client must be able to connect to the TN3270E listener, meaning that it cannot be excluded by the IPADDR parameter of the TN3270E listener daemon. To confirm that your listener daemon is listening on port 23, and to see whether it places restrictions on the IP addresses that can connect to it, you can issue the QUERY TELNETDS TCP/IP for VSE/ESA operator command. When the connection is established, the TN3270E listener daemon attempts to locate a TN3270E effecter daemon (DEFINE TELNETD,TN3270=E) that is eligible to process the request. The TN3270E effecter daemon is deemed eligible if its TERMNAME matches the terminal name specified by the incoming TN3270E session.

Associating VTAM terminal names with IP addresses

When a TN3270 client (for example, a terminal user) requests a telnet session and does not specify an LU name, the first available daemon is normally assigned. This may be undesirable for several reasons. You may want to enforce certain session properties based on the originating IP address, or you may want to restrict the number of sessions permitted with some applications. In addition, you may have a security policy that is based on CICS terminal identifiers or VTAM net-names. You can associate a VTAM terminal name with an IP address in one of the following ways:

- By creating daemon pools
  By convention, telnet requests are sent to port 23. You may also use port numbers to create separate pools of telnet daemons in order to establish pools with different characteristics. The drawback is that the end user must know which port to select.

- By specifying address patterns

- By allowing the client to specify the VTAM terminal name using TN3270E

Security layers

TCP/IP for VSE/ESA also provides features that help control access to the server and secure TN3270 sessions with clients. Multiple layers of security can be implemented to control access. These layers can all be used or implemented in any combination and are listed from top to bottom as the client passes through each layer and fall into the following categories:

- Network masking
- TLS/SSL support
- TN3270 user ID/password authentication
- Security exits

Network masking (IP address access control)

The first layer of security can be controlled by specifying the client IP addresses that are allowed to connect into the TN3270 server running on the VSE system (TELNETD).

The CONNECT_SEQUENCE ON command must be issued to activate the enforcement of controlled access for each TELNETD. This command can also be placed in the startup configuration.

The DEFINE TELNETD keyword IPADDR=*nnn.nnn.nnn.nnn* will then use pattern matching to control the TELNETD that the TN3270 client is allowed to connect into. CONNECT_SEQUENCE ON causes a telnet daemon to be selected on a best-fit basis according to the following algorithm:

1. An exact match of the IP address of the incoming request with the IP address of each telnet daemon (IPADDR= on DEFINE TELNETD).
2. If Step 1 fails, an attempt is made to match the network and subnetwork values of the incoming request with a generic network and subnetwork address based on the IPADDR parameter of each telnet daemon.
3. If Step 2 fails, an attempt is made to match the network portion of the incoming request with a generic network number based on the IPADDR parameter of each telnet daemon.
4. If Step 3 fails, TCP/IP for VSE/ESA matches the IP address of the incoming request with an IPADDR of 0.0.0.0 on the IPADDR of a

telnet daemon. If IPADDR was omitted on the DEFINE TELNETD command, an IPADDR of 0.0.0.0 is assumed.

You should specify CONNECT_SEQUENCE=ON in the following situations:

- To guarantee that an incoming telnet request is always associated with a given telnet daemon and its associated terminal name.

- To limit the number of telnet daemons available to TCP/IP hosts on a given network and subnetwork.

CONNECT_SEQUENCE=ON may result in slightly higher CPU utilization during telnet connection requests.

Note that even after a connection is established, the IP address, port number, user ID, and password of the person trying to log in is passed to the security exit. A rejection could still occur at that point.

TLS/SSL support

From z/VSE 5.2 onwards, Language Environment C (LE/C) applications can use openSSL via the LE/C Multiplexer. OpenSSL is a z/VSE base component and supports SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2.

The next layer of security after the TELNETD has allowed the connection is the ability to secure the connections using the TLS/SSL protocol. The TLS/SSL handshake negotiation occurs before any 3270 data is exchanged and provides authentication, privacy, and integrity of the data exchanged between TELNETD and the TN3270 client. Of course the TN3270 client must be able to support the TLS/SSL protocol and almost all clients provide this support, but it can be an extra cost feature. Authentication is provided by the TELENTD by providing a certificate to the client so that it can validate the identity of the server. Privacy is accomplished since all data sent and received will be encrypted across the network using industry standard strong encryption such as triple-DES and AES.

Integrity is also increased since the TLS/SSL protocol also adds a digitally signed hash (SHA-MAC) to each encrypted record that is then verified so you can know the bits sent have not been modified. This added integrity aspect of using TLS/SSL cryptographically to guarantee the message has not been modified is often overlooked, but is just as if not more important than the privacy that the encrypted data provides.

TN3270 user ID/password authentication

Each daemon can connect the end user directly to an application or can present the user with a menu. Menus provide additional flexibility, including the ability to require a user ID and password. The most common TN3270 target application under VSE is CICS. TCP/IP for VSE/ESA provides functionality similar to that available with VTAM's USS table and the USSMSG10 display. When you provide a TCP/IP for VSE/ESA telnet menu, inbound telnet users can choose available applications with a simple command or PF key. The menu facility in TCP/IP for VSE/ESA provides the following features:

- Easy application selection
- Network solicitation screen
- Message of the day Security.
  This feature permits you to request a user ID and password before you allow access to any applications. This security check supplements the user ID and password that is required to access a specific application.

The standard layer that most shops already implement is a sign-on menu screen where the user must enter a user ID and password. These are then passed to the security exit which can also invoke an external security manger product to validate the user ID/password.

By default, security is off, and any user ID or password is accepted. If you do not know whether security is active, issue the following command:

```
QUERY SECURITY
```

If the response indicates that security is OFF, issue the following command:

```
SECURITY ON MODE=WARN AUTO=ON
```

Most installations can use the automatic security feature of TCP/IP for VSE/ESA. This command activates security in Warn mode, and a message log is created that can help identify the user IDs being used and resources accessed. It still allows all logins and accesses because MODE=WARN is specified. Remember that issuing the SECURITY OFF command leaves your system completely exposed to hackers and unauthorized users. For securing TN3270 incoming clients you can also create a custom security exit that can internally call an external security manager to validate the user ID and password attempting to access the TELNETD.

Security exits

User ID/password can be validated through the BSSTISX security exit which is part of the z/VSE Basic Security Manager (BSM).

IPv6/VSE

IPv6/VSE provides a TN3270E daemon that supports the TN3270 and TN3270E protocols. It also provides features that help control access to the server and secure TN3270 sessions with clients. These features fall into the following categories:

- IP filtering
- TLS/SSL support
- Security exits

IP filtering

IPv6/VSE provides basic facilities for filtering based on IP address and subnet. This allows connections to be restricted to specific IP addresses and subnets. In addition, session LUNAMEs can be specifically allocated based on IP addresses and subnet ranges.

Once a connection is permitted by the local firewall, an LUNAME must be allocated to the session. The LUNAME can be allocated in a number of ways but one method is based on the TN3270E client's remote host IP address. The BSTTVNET TN3270E server can select an LUNAME for a session based on the IP address or subnet address of the TN3270E client. If the BSTTVNET TN3270E server is unable to allocate an LUNAME the session is rejected.

Another method of allocating an LUNAME is to have the TN3270E client specifically request the name. This is generally done in the TN3270E client's configuration dialog using a Resource or LUNAME field. If the LUNAME requested does not match a list of valid selections the session is terminated.

TLS/SSL support

IPv6/VSE supports SSL and TLS connections using z/VSE's OpenSSL. This includes TLSv1.2 and the latest security updates.

OpenSSL on z/VSE supports RSA key lengths of 512, 1024, 2018, and 4096 bits. Symmetric algorithms DES, 3DES, and AES are supported, as well as hash algorithms SHA-1 up to SHA-256. RC4 has been removed due to known security issues. SSL cipher suites based on Diffie-Hellman key exchange with and without Elliptic-Curves are available when the keystore contains DH parameters and a separate keystore containing an EC key is provided. Supported SSL/TLS protocol versions are SSLv3, TLSv1.0, and TLSv1.2

All algorithms except Elliptic-Curve (ECC) are hardware-accelerated when IBM Crypto Express features are available.

Security exits

IPv6/VSE also provides security exits for TN3270E connections providing validation of source IP address, LUNAME selection and application selection. The BSTTVNET TN3270E server calls the BSTTTNSX TN3270E security exit 3 times for each connection. The 1st call is done to validate the source IP address of the connection. Is this a valid source IP address? If not the BSTTVNET TN3270E server will terminate the connection.

The 2nd call to the BSTTTNSX security exit is done to validate the selected LUNAME. If the LUNAME selected is not acceptable the session is terminated.

The 3rd call to the BSTTTNSX security exit is done to validate the selected application. Is the application selected valid for the IP address and LUNAME? If it is not the application selection menu is redisplayed.

Chapter 7. What about Linux on z Systems and z/TPF?

Two more operating systems run natively on z Systems: Linux and z/TPF. 3270 security is not a concern for either of these environments as explained below.

As an operating system, Linux on z Systems provides a very limited amount of 3270 support, none of which includes network connectivity. Rather, IBM provided a 3270 to tty device driver to the open source community that is now part of the Linux kernel tree. Being a device driver, it requires channel connectivity to z Systems – it does not support network attachment which greatly reduces the risk of misuse. This driver supports both line mode as well as 3270 data streams. However, the only exploiter of the fullscreen 3270 mode is an ISV-written XEDIT/ISPF implementation called NED that is no longer supported by the vendor.

It should be noted that IBM Communications Server for Linux runs on z Systems and provides TN3270 services. For more on this, refer to Chapter 8. Distributed TN3270 on page 39.

z/TPF does not provide any 3270 data stream support for application programs. As such z/TPF applications programs do not use 3270 data streams at all. The only 3270 support in z/TPF is for the operator’s console itself.

Chapter 8. Distributed TN3270

3270 support on distributed platforms (Windows, Linux, AIX, HP, Oracle and so forth) is provided in two ways: emulators and servers. Emulators usually run on desktops or are served up by web application servers, and mostly use TN3270. There are some Windows based 3270 emulators that may not use Telnet-based protocols, but use direct SNA interfaces (LUA application for standard usage) to connect to mainframe application sessions. This chapter will address the security best practices for distributed TN3270.

Direct SNA 3270

Emulators that provide direct SNA connectivity should use the best practices for session management described below. Direct SNA is actually more likely to flow over IP connections using Enterprise Extender or a remote client/server TCP/IP connection, which can be encrypted in IPsec, secure tunneling, and VPN networks**.**

TN3270 Servers

In the market, there are TN3270 Server products for most every platform. These provide off-loading of network processing for z/OS and are practical in managing thousands of LU resources for network access. A TN3270 Server defines client access by settings for port, LU characteristics, LU name, encryption, filtering and device specifications. Each setting has best practices considerations in managing a secure network.

Encryption via TLS/SSL is supported by TN3270 Servers on distributed platforms using the GSKit toolkit. Supported protocol versions are SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2.

Port configuration

TN3270 Servers on distributed platforms should specifically list the interface that it is listening on. As a best practice, it is not a good idea to listen on all the server's interfaces for a given port. This allows the possibility for a connection over an unintended path.

Managing LUs on distributed platforms

TN3270 Server LUs use can have several different configurations. LUs can be used for teller devices, printers, or associated printers (specifically assigned to a terminal LU). For associated printers, when a terminal LU session is initialized for a client, the printer LU is also started.

LU assignment is important to providing secure and intended use of the session traffic for a TN3270 Server. LUs can be explicitly assigned to a port, or implicitly assign by being part of a pool of LUs assigned to a port. TN3270 Server allows ports to have default LU settings so clients that do not specify a name will get a default LU or pooled LU. Pools are groupings of LUs that allow one to manage access to a common application. By specifying a pool name as a default name for a port, one might limit access to a specific back end application. Pools can cross PU boundaries. On distributed platforms, LUs can be defined to no more than one pool at a time.

If a pool name is assigned as the default name on a port, a client will be assigned the next available LU from a pool. As a best practice in defining pooled LUs, either authentication or filtering should be implemented so that the assignment of a random LU from a pool is for an intended user.

Filtering clients

TN3270 Servers on distributed platforms allow administrators to assign specific IP addresses to a specific port, and specific LU or pool name on the port. This assignment will assure the connecting 3270 device is assigned the proper LU or pool, but does not authenticate the user. The user can be authenticated using X.509 certificates via TLS/SSL and also by User Authentication on z/VM. Here is an example of a filter definition on an AIX TN3270 Server:

```
[define_tn3270_access]
description = Assign LU to specific client
default_record = NO
client_address = somewhere.in.network.com
{tn3270_session_data}
port_number = 23
description = ""
lu_name = LUXYX
printer_lu_name = ""
tn3270_support = TN3270E
allow_specific_lu = NO
ssl_enabled = NO
security_level = SSL_AUTHENTICATE_MIN
cert_key_label = ""
```

Conclusion

IBM z Systems play a key role in large enterprise IT infrastructure around the globe and, given the continued evolution and innovation of the platform, will continue to do so for the foreseeable future. Since 3270 data streams play such an integral part in many of z Systems-based applications and middleware, they will also continue to serve an important role in enterprise computing for many years to come.

As we have seen, the evolution of 3270 connectivity, especially the advent of TN3270, has increased the visibility and access to 3270 data streams to new levels. As such, controlling access to 3270-based applications and middleware as well as controlling the installation of 3270 emulator software on enterprise clients can help minimize the exposure to potential 3270-based intrusion attempts.

Each of the different z Systems operating systems that support 3270 data streams provide a variety of security mechanisms for not only controlling access to the 3270 endpoints, but also protecting the TN3270 traffic as it traverses the IP network. In addition, other administrative and network-based controls can and should be used to lock down the use of TN3270 to only the users with a need for such access.

By using the facilities and strategies described in the preceding pages, you can maximize the integrity and security of your 3270-based applications and middleware.

Acknowledgments and Contributions

This paper was a collaborative effort. Thanks to the following individuals for their contributions to this paper.

- John Dayka
- Mark Gambino
- Michael Kasper
- Peter Spera

IBM Poughkeepsie, NY

- Kerry Harpe
- Gus Kassimis
- Linwood Overby

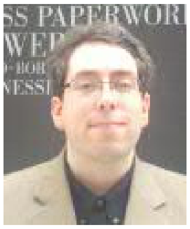
IBM Research Triangle Park, NC

- Don Stoever, CSI International
- Jeff Barnard, Barnard Software Incorporated

- Alan Altmark, IBM Endicott, NY
- Thomas Cosenza, IBM Tampa, FL
- Martin Schwidefsky, IBM Boeblingen, Germany

About the Authors:

Chris Meyer, CISSP is the security designer for IBM's z/OS Communications Server. He has over 30 years of experience developing IBM operating systems and security-related software products. Chris can be reached at meyerchr@us.ibm.com.



Brian Hugenbruch, CISSP is a Virtualization Security Architect for IBM z Systems. His primary job is the secure design, development, testing, compliance and certification of the z/VM hypervisor. Brian can be reached at bwhugen@us.ibm.com or (for the brevity minded) on Twitter at @Bwhugen.

Ingolf Salm is IBM's z/VSE lead architect. Since 1981 he has been a member of the VSE development team in Boeblingen, Germany. He is responsible for the z/VSE requirements, the system design and z/VSE release content.

Jeff L Smith is the Chief Programmer for Distributed Communications Servers in IBM z Systems. Jeff has been with IBM for 25 years working on multi-protocol networking software products, specializing in SNA system connectivity to the mainframe from distributed platforms.

Copyright IBM Corporation 2015
IBM Systems and Technology Group
Route 100
Somers, New York 10589
U.S.A.
Produced in the United States of America,
02/2015
All Rights Reserved

AIX, IBM, IBM logo, RACF, System z, VTAM, z Systems, z/OS, z/TPF, z/VM and z/VSE are trademarks or registered trademarks of the International Business Machines Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States, other countries, or both. Other names may be trademarks of their respective owners.

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

All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

ZSW03276-USEN-01