Got the world on your shoulders?

AT-TLS and CS IPSec can help lighten the load for security administrators

BY LIN OVERBY

As security concerns continue to increase, more enterprises are deploying network security protocols, such as IP Security (IPSec) and Transport Layer Security (TLS) on z/OS to protect their mission-critical data as it crosses the network. However, the programming changes needed to enable applications for security, and the complexity of security configuration can increase the cost and deployment time for network security.

In z/OS V1R7, we add the following new functions to z/OS Communications Server to address these issues by simplifying the requirements for implementing network security on z/OS:

- Application Transparent Transport Layer Security (AT-TLS). This function provides TLS for TCP applications without requiring application modification for TLS enablement.
- Communications Server IPSec (CS IPSec). This function provides an alternative to z/OS Firewall Technologies for host-based IPSec and IP filtering.

Both AT-TLS and CS IPSec feature a policy-based configuration that:

- Requires less definition
- Uses existing z/OS Communications Server infrastructure, such as the policy agent
- Is optimized for host-based security scenarios.

To help you implement these new functions, z/OS V1R7 includes a new configuration tool, the Network Security Configuration Assistant (NSCA). This tool combines the configuration activities for AT-TLS and IPSec into a single administrative task. (See Figure 1)

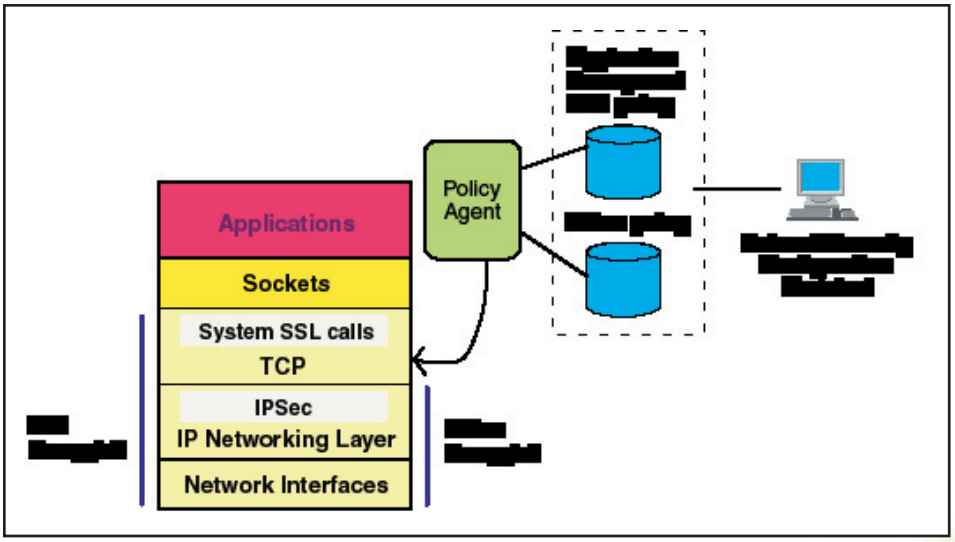


Figure 1 - Policy-driven network security that is transparent to the application

What is Application Transparent TLS?

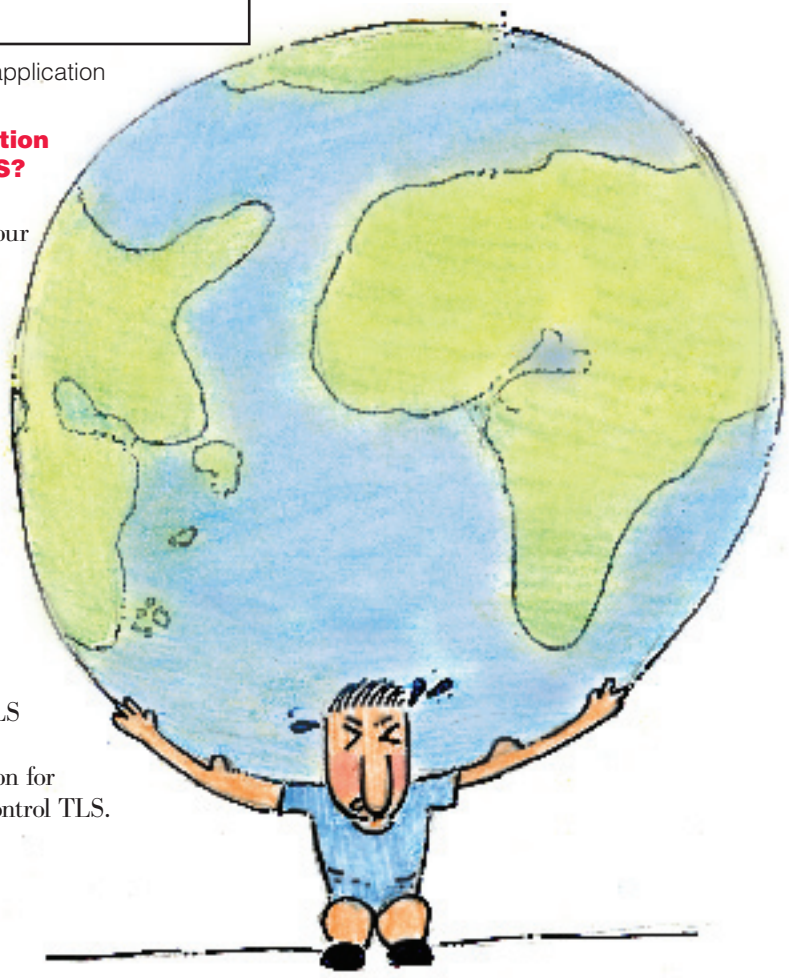
Traditionally, you needed to enable your applications to use TLS services and these changes incurred programming costs. For an application, you would usually need to add:

- TLS service calls
- Dual path application logic to support both TLS and non-TLS paths
- New configuration for parameters to control TLS.

As a result, the traditional TLS model created more administrative complexity where each application typically had a separate, application-specific TLS configuration.

In z/OS V1R7, AT-TLS lowers the cost of TLS on z/OS by transparently performing TLS in the TCP layer of the TCP/IP stack. A z/OS application using AT-TLS can interoperate with any partner TLS-enabled application (even one that is not using AT-TLS), because AT-TLS exchanges standard TLS protocols with the TLS partner. AT-TLS is available to z/OS applications using all supported socket APIs, except the PASCAL API.

Many existing applications need only basic TLS services and can take advantage of AT-TLS without requiring application code changes. Applications that use advanced TLS functions might require changes. For example, some applications need to execute application-defined



negotiations for TLS prior to TLS session initialization, or might require access to the TLS partner's client certificate.

To support these applications, a new ioctl service is provided to control and request information about the TLS session. Using ioctl, an application can direct AT-TLS to start TLS after a negotiation, or can request AT-TLS to provide the client certificate to the application after TLS session initialization.

The decision to TLS-protect a particular TCP connection is based on an AT-TLS policy. Mapping a TCP connection to policy is done in the TCP layer at predefined points. For outbound connections, the policy is checked by the TCP/IP stack when the outbound TCP connect is processed. For inbound connections initiated from a remote connection partner, the policy is checked after the connection is established, during the process of the first inbound or outbound data transfer. When the connection is mapped to a policy, the TLS session initialization is handled based on the TLS policy action. If the policy indicates that the TLS session should be controlled by the application, the TLS session initialization is deferred until the application issues a new ioctl to requesting TLS. Otherwise, the TLS session is started when the connection is mapped to a policy.

Although AT-TLS is implemented in the TCP/IP stack, the security endpoint affinity is with the application as though the application were enabled with traditional TLS. For example, the keyring that contains the digital certificate that represents an application during TLS authentication must be accessed under the correct user identity. Before accessing the keyring, AT-TLS replicates the application's security environment including the user identity of the application at the time that the policy is mapped. This action ensures that only authorized users can authenticate using the certificate. Additionally, application data secured with traditional TLS is not visible in data traces at the socket layer because the data is encrypted in the application. With AT-TLS the data is "in the clear," that is, not encrypted, at the sockets layer. AT-TLS policy specifies whether the application data is to be traced if tracing is active. This action preserves data confidentiality at the sockets layer unless otherwise specified in the policy.

In z/OS V1R7 a new IPSec solution for z/OS, CS IPSec, is included in z/OS Communications Server and provides an alternative to z/OS Firewall Technologies.

What is CS IPSec?

Because IPSec is implemented in the TCP/IP stack at the IP layer, application enablement cost is not an issue. However, IPSec can be a more complex protocol than TLS to administer because IPSec supports more configuration scenarios than TLS. While TLS provides exclusively end-to-end security, IPSec supports end-to-end security or can be used to secure portions of the data path.

The trend for IPSec deployment on z/OS is moving toward host-to-host security. Another prevalent scenario is host-to-branch office gateway protection. Both of these scenarios are depicted in Figure 2.

In z/OS V1R7 a new IPSec solution for z/OS, CS IPSec, is included in z/OS Communications Server and provides an alternative to z/OS Firewall Technologies for IP packet filtering, IPSec, and Internet Key Exchange (IKE) functions. CS IPSec provides a simplified supporting infrastructure, reduced definition, and improved diagnostic and event messages.

Packet filtering controls which packets are permitted to enter or leave the system. IPSec provides cryptographic network security services at the IP layer for packets that enter or leave the system. The information necessary to protect a packet with IPSec, such as encryption key, is maintained in an IPSec security association (SA). An SA can be configured manually, or created dynamically using the Internet Key Exchange (IKE) protocol.

The simplified infrastructure of CS IPSec uses existing z/OS Communications Server services such as the policy agent and the traffic regulation management daemon (TRMD), and eliminates the need for specialized Firewall Technologies daemons. A new default set of filters defined in the TCP profile provides granular control of a restricted set of permitted traffic before the policy agent loads the IPSec policy. If, after the policy is loaded, it is suspected that the system is under attack, the default filters can be quickly reloaded to more tightly control traffic entering or leaving the system. The CS IPSec "wildcarding" function removes a Firewall Technologies configuration requirement to define each remote IKE peer.

CS IPSec provides new capabilities to interoperate with Network Address Translation (NAT) devices. NAT reduces the number of public IP addresses that are needed and also "hides" internal addresses from the public. Performed at a network

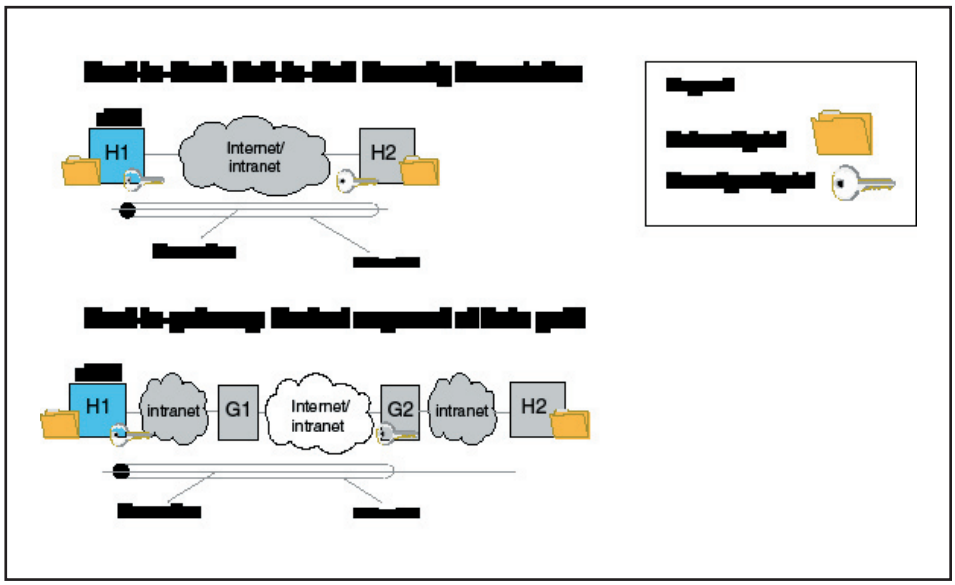


Figure 2 - z/OS host-based IPSec configuration scenarios

boundary, NAT accomplishes this function by translating IP addresses in packet headers.

Historically, NAT and IPSec have been incompatible. CS IPSec supports new Internet Engineering Task Force (IETF) standards that allow data that is protected by IPSec with an SA endpoint on z/OS to traverse a NAT device. NAT traversal support is provided for the z/OS host-to-host and z/OS host-to-gateway scenarios.

Network security policy

AT-TLS and CS IPSec are both configured with a network security policy, which defines the traffic to be protected and its security requirements. Separate policy files exist for CS IPSec and AT-TLS. The z/OS Communications Server policy agent application reads the policy definitions from the network security policy files and installs the policy in the TCP/IP stack.

Policies consist of a set of policy rules. A policy rule refers to a policy condition and policy action. The policy condition defines conditions that must be met to execute the policy action. The policy action defines actions to be performed when the policy condition is met.

Both AT-TLS and IPSec policy conditions control the selection of traffic to protect and include resource type attributes, such as source and destination IP addresses, ports, and protocol. AT-TLS also allows resource type conditions associated with the application running on z/OS, such as jobname and user identity. AT-TLS and IPSec policy actions specify whether network security is required, and the security levels to apply such as:

- Encryption algorithms
- Data authentication algorithms
- Security endpoint authentication requirements.

IPSec policy also allows specification of a permit or a deny IP packet filtering action.

Network Security Configuration Assistant

To configure the policy, you can either use the new NSCA tool or you can directly edit the policy files. The NSCA is a downloadable policy configuration tool that runs on a workstation. The tool allows policy administration to be performed at a higher level of abstraction than is possible in the individual policy file statements. With the tool, you are able to focus on what traffic to protect and how to protect it. There is less focus on low-level configuration details, although these controls are available on expert panels. The tool provides wizards and dialogs to guide you through a top-down approach to configuration. A navigational tree that supports a bottoms-up approach allows an experienced administrator to bypass wizard screens. The NSCA generates separate policy files for CS IPSec and AT-TLS which are then transferred to a z/OS system.

Summary

Both AT-TLS and CS IPSec help to minimize application enablement requirements for network security. The functions are policy driven for consistent, system-wide enforcement of security policies. The Network Security Configuration Assistant tool, which can configure AT-TLS and CS IPSec policy as a single administrative task, provides a simplified user interface to the administrator. This integrated security functionality provides a simple packet screening function with IP filtering and enables the creation of a network security infrastructure based on pure AT-TLS, IPSec, or a mix of AT-TLS and IPSec.

For more information, see *z/OS Communications Server IP Configuration Guide*, SC31-8775.

Got security?

Welcome to the future; where everything is secret! Your password, your communications, even your identity are concealed from bystanders. This is all made possible with the latest OpenSSH technology now available for your remote host data connections. Secure your inbound and outbound network traffic, meaning your passwords, session data, and file transfers…those eavesdroppers will have nothing on you!

It's true! The illustrious OpenSSH package has been ported and can now be implemented on z/OS V1R4 and up. Using the Rivest-Shamir-Adleman (RSA) algorithm, digital signature algorithm (DSA), Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and Blowfish cipher, all your network traffic can be secured. Port forwarding will even allow you to encrypt other protocols in addition to the obvious SSH protocol. Protect yourself from malicious network attacks, eavesdroppers and connection seizures.

You can enhance your security, why wait? Hurry before those eavesdroppers find you!