z/OS Communications Server Security

What is available

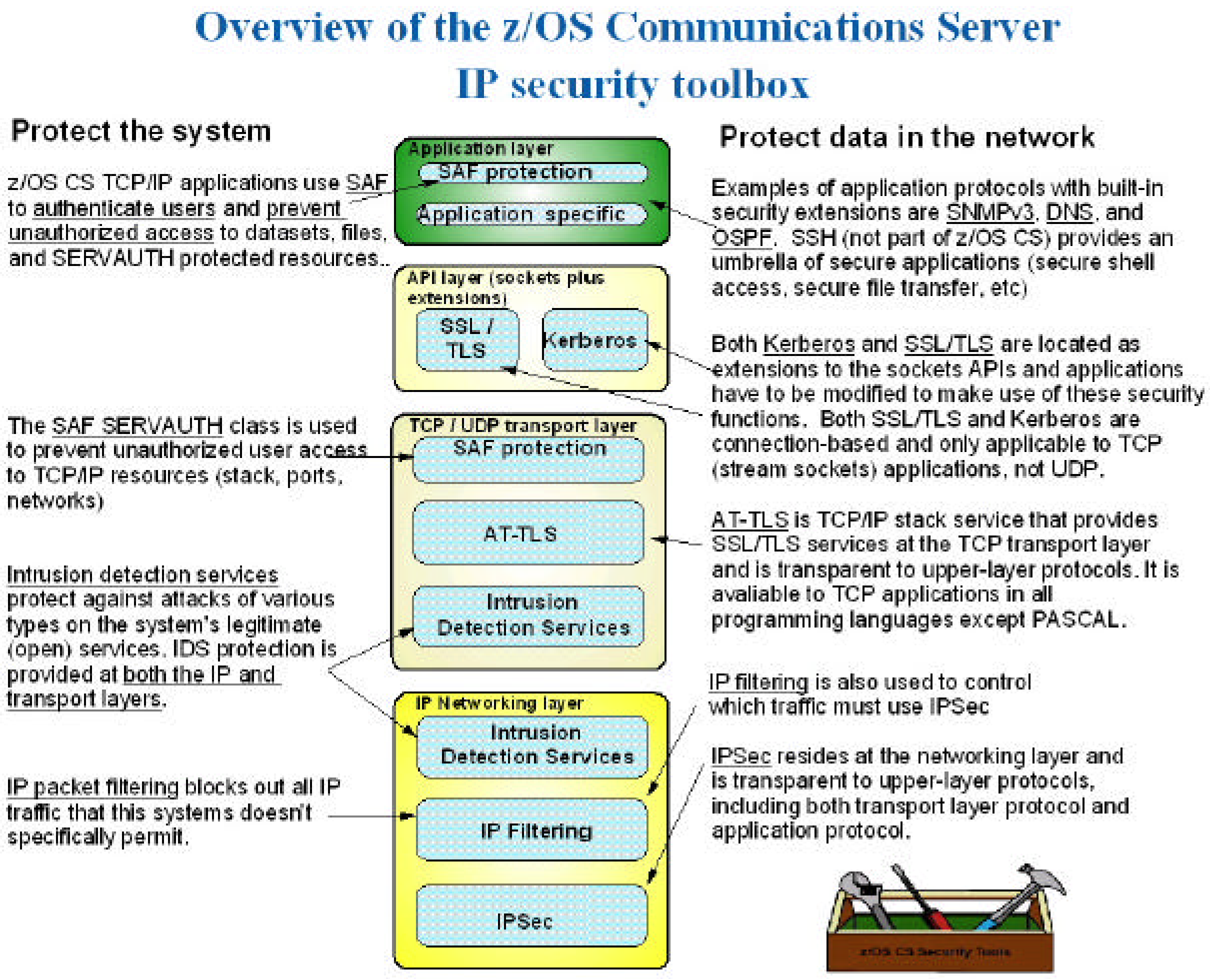
and how can it help your enterprise?

Chuck Gardiner
Enterprise Networking Solutions
cgardine@us.ibm.com

April 18, 2007

Overview

As you can see from the picture, z/OS Communications Server has a wide array of tools to help you secure your business systems, data, and transactions. In this paper we will explore some of the options to help give you an understanding of what features are available and how you can use them. We will provide some strategies to allow secure access to both TCP/IP and SNA applications and will also discuss recent trends that are increasing the focus on end-to-end security and self protection. And finally, we will show how the strengths of System z hardware and software can help your enterprise.



Overview of the z/OS Communications Server IP security toolbox

Protect the system

z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources..

The SAF SERVAUTH class is used to prevent unauthorized user access to TCP/IP resources (stack, ports, networks)

Intrusion detection services protect against attacks of various types on the system's legitimate (open) services. IDS protection is provided at both the IP and transport layers.

IP packet filtering blocks out all IP traffic that this systems doesn't specifically permit.

Protect data in the network

Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF. SSH (not part of z/OS CS) provides an umbrella of secure applications (secure shell access, secure file transfer, etc)

Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols. It is avaliable to TCP applications in all programming languages except PASCAL.

IP filtering is also used to control which traffic must use IPSec

IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

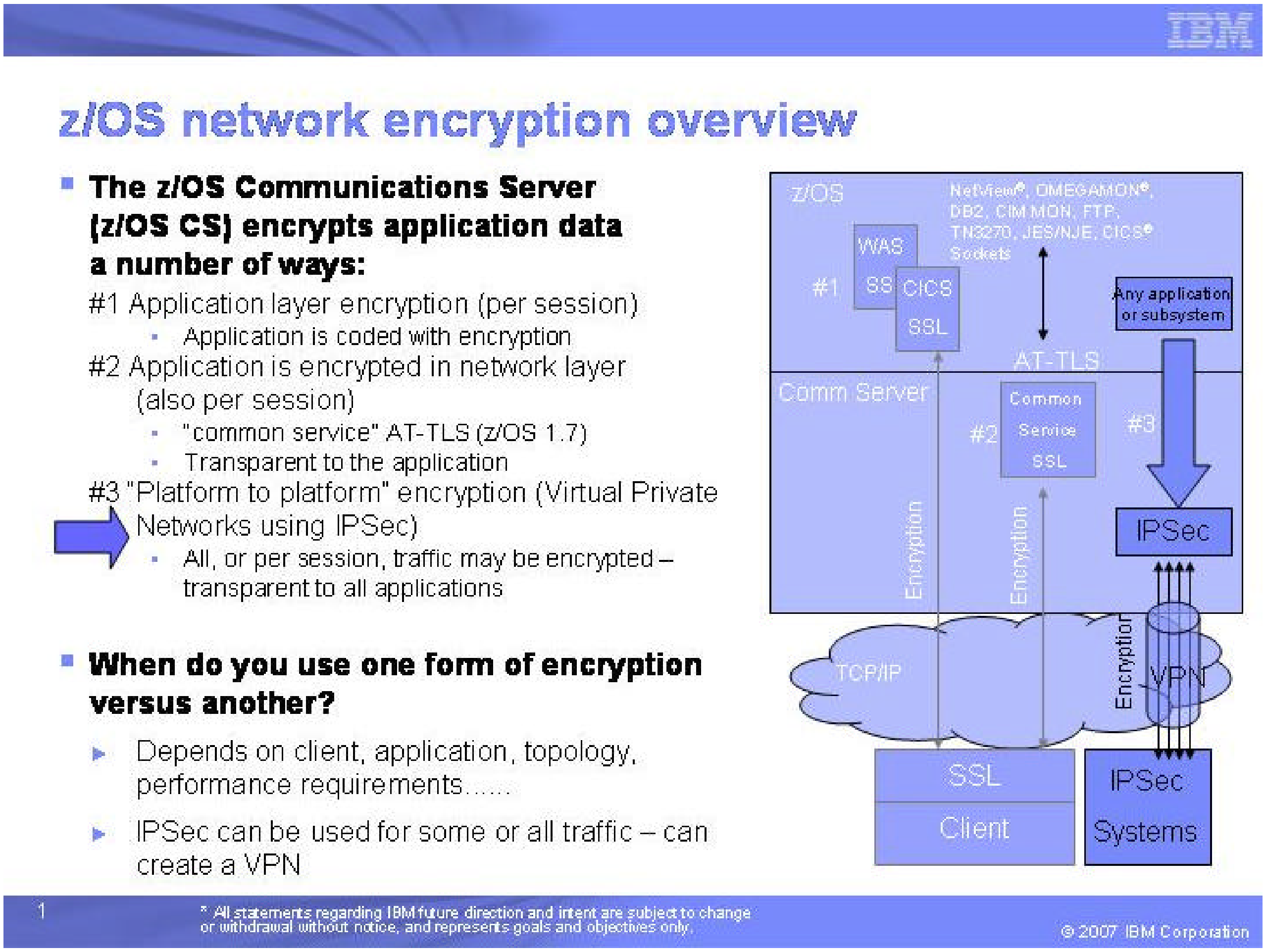
This analysis will focus on two main themes, “Protecting your systems and data”, and “Protecting your data in the network”. When we talk about protecting your systems and data, we mean all the things you do to protect system availability and prevent unauthorized access to data or system resources. Protecting data on the network will describe some choices you have for securing your data as it flows across untrusted, or even trusted, networks.

Protecting your data

z/OS enables encryption at 3 layers:

- Within the application
- On behalf of an application
- On behalf of all applications

In this section we will discuss some of the options provided for each of these layers.



z/OS network encryption overview

- **The z/OS Communications Server (z/OS CS) encrypts application data a number of ways:**

  #1 Application layer encryption (per session)
  - Application is coded with encryption

  #2 Application is encrypted in network layer (also per session)
  - "common service" AT-TLS (z/OS 1.7)
  - Transparent to the application

  #3 "Platform to platform" encryption (Virtual Private Networks using IPSec)
  - All, or per session, traffic may be encrypted – transparent to all applications

- **When do you use one form of encryption versus another?**
  - Depends on client, application, topology, performance requirements……
  - IPSec can be used for some or all traffic – can create a VPN

1

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

© 2007 IBM Corporation

Application layer

Application embedded security

Enabling encryption and authentication within an application can offer a high level of security. Doing so ensures that sensitive data is protected before it ever leaves the application. However, this approach can be less flexible than other choices. This is because if you want application layer security you need to enable it within each application. This could mean specific application coding, or if the application has some built in security, doing the required configuration. Since it is very likely that each application has its own method of providing security, the skills required to support this approach could be significant. Locating security policy within the application can also increase risk by placing administration of the security policy under the application administrator instead of the security policy administrator.

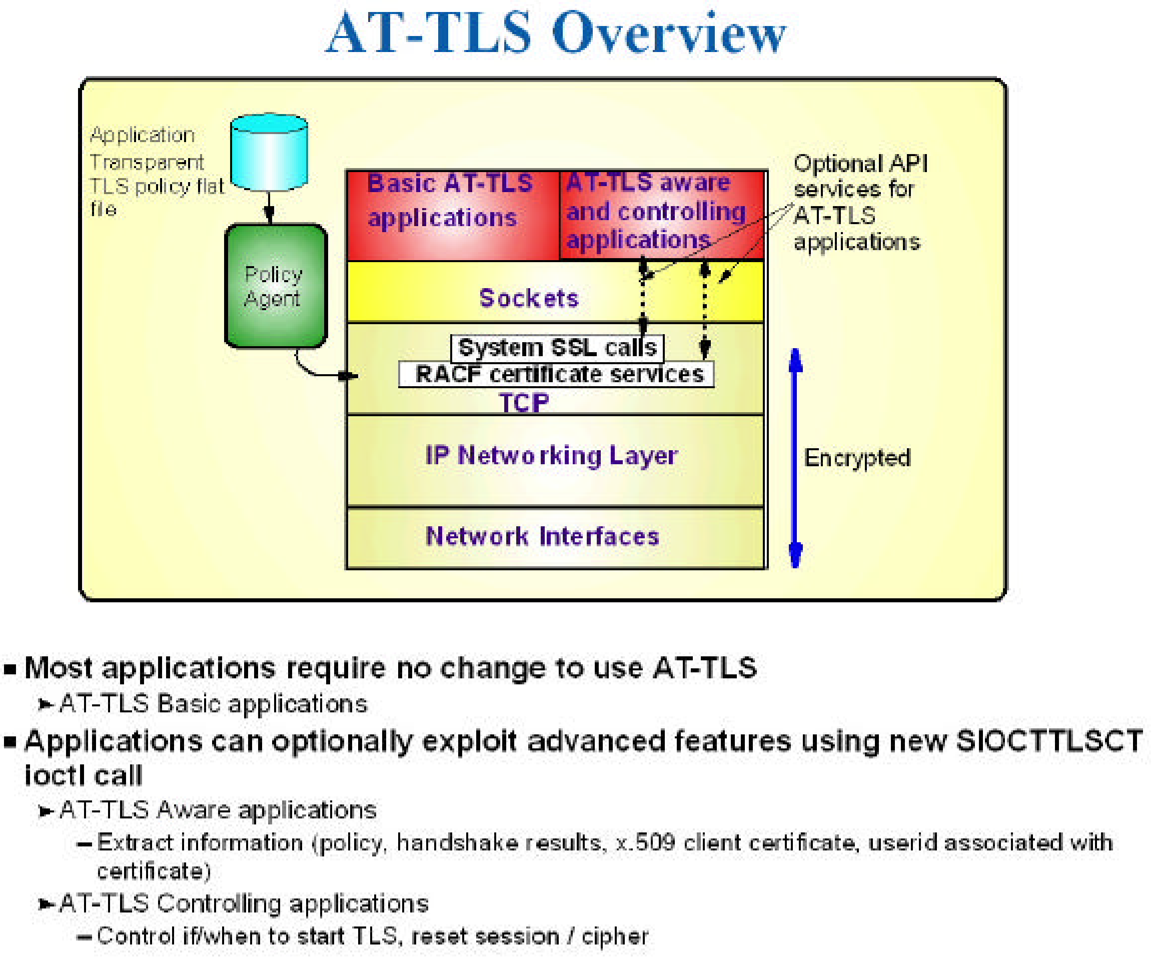
One method of building security into the application on z/OS is to use a system socket API-level security service such as **z/OS System Secure Sockets Layer** (SSL), or **z/OS Network Authentication Services** (Kerberos). Versions of network services such as SNMPv3, supported by the Communications Server, have security built directly into the application protocol at the message level using standards-based specifications for secure interoperability.

Application transparent security

Security implemented in the transport, or network, layer, can provide application independence. This can reduce the configuration and management complexity. Having the security session in the transport layer also provides end-to-end security.

Application Transparent Transport Layer Security (AT-TLS)

AT-TLS is implemented within z/OS Communications Server on behalf of the applications. It provides the benefits of application imbedded security, such as protecting the data very close to the source, but reduces or eliminates the need to implement security within the application.



AT-TLS Overview

Application Transparent TLS policy flat file
Policy Agent
Basic AT-TLS applications
AT-TLS aware and controlling applications
Optional API services for AT-TLS applications
Sockets
System SSL calls
RACF certificate services
TCP
IP Networking Layer
Network Interfaces
Encrypted

- Most applications require no change to use AT-TLS
  - AT-TLS Basic applications
- Applications can optionally exploit advanced features using new SIOCTTLSCT ioctl call
  - AT-TLS Aware applications
    - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
  - AT-TLS Controlling applications
    - Control if/when to start TLS, reset session / cipher

If you want to implement AT-TLS, you can usually do it without changing your applications. In addition, applications can optionally exploit advanced AT-TLS features using the new SIOCTTLSCT ioctl call. This allows AT-TLS aware applications to extract information such as:

- Policies
- Handshake results
- x.509 client certificates
- Userid associated with the certificate

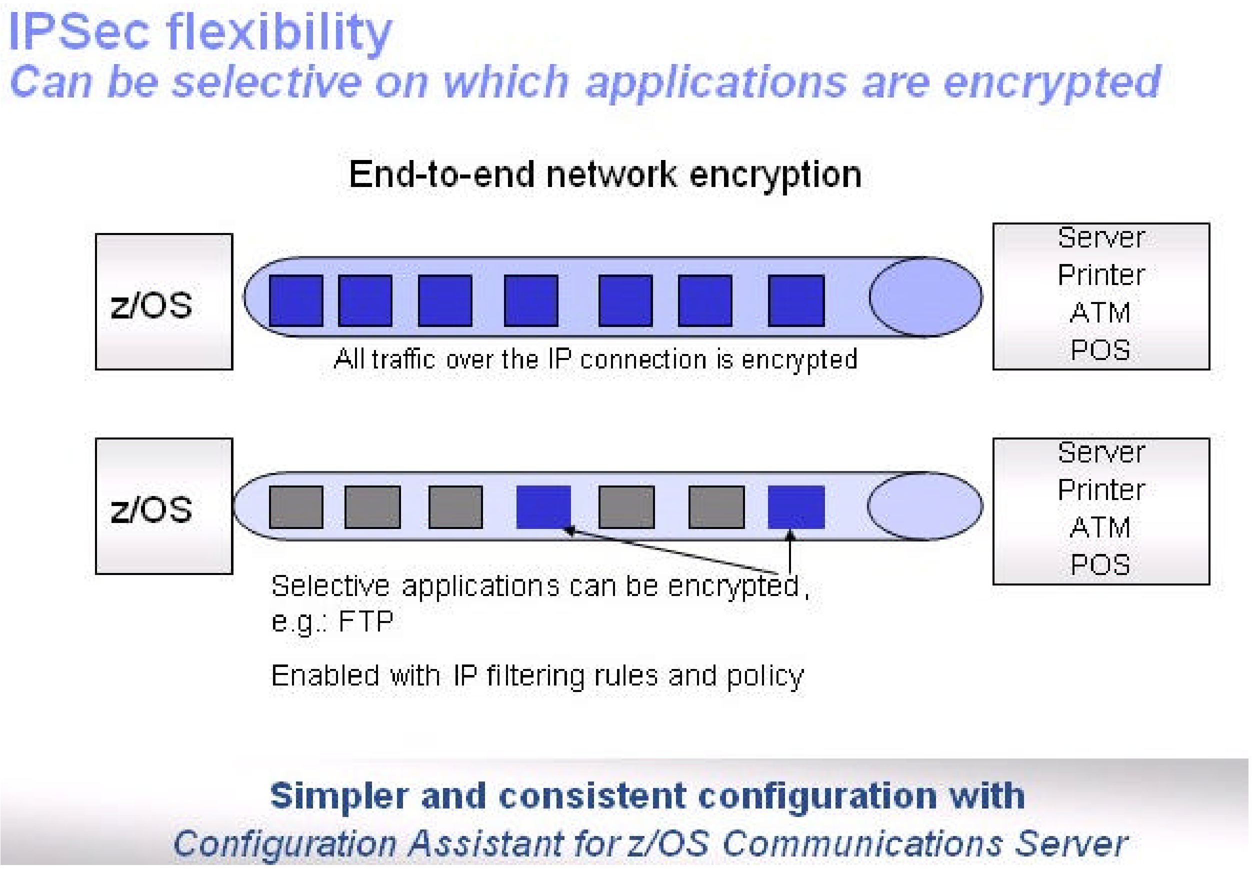
It is also possible for an application to control AT-TLS. These applications can:

- Control if or when to start TLS
- Reset sessions or cipher

IPSec

The last type of security we will describe, IPSec, is implemented in the network layer. IPSec is an open networking standard defined by the Internet Engineering Task Force (IETF) which can create highly secure connections between two points in an enterprise. These connections may be server-to-server, or server to network device, as long as they support the IPSec standard.

IPSec allows a company to create a secure connection, often called a Virtual Private Network (VPN) across trusted and untrusted networks, such as the internet. When data is sent across these VPN connections, each endpoint can encrypt and authenticate some or all of the data. This allows companies to build secure connections to virtually any other location without having the expense of buying dedicated lines.



IPSec flexibility

Can be selective on which applications are encrypted

End-to-end network encryption

All traffic over the IP connection is encrypted

Selective applications can be encrypted, e.g.: FTP

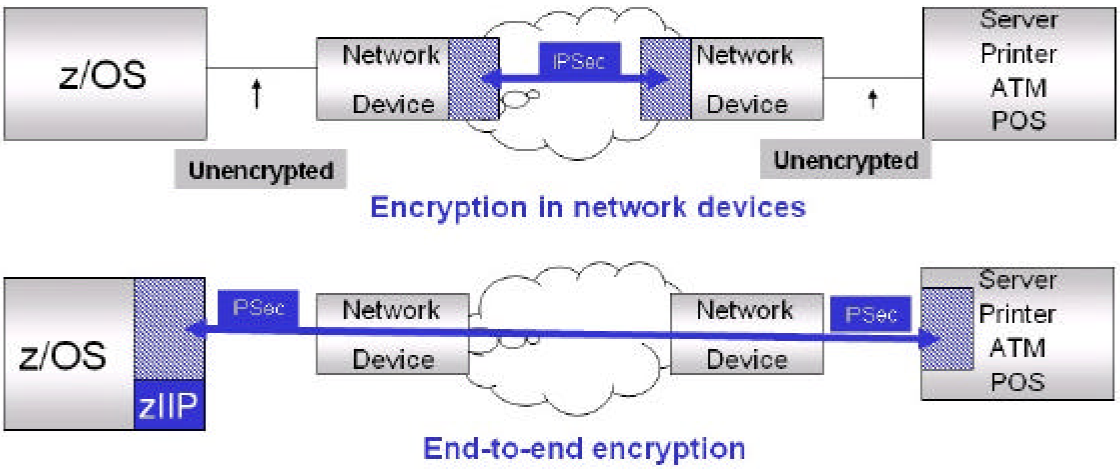
Enabled with IP filtering rules and policy

Simpler and consistent configuration with
Configuration Assistant for z/OS Communications Server

The IP Security support delivered in z/OS V1.7 Communications Server includes both IPSec capabilities and IP filtering. Using IPSec to provide end-to-end encryption helps provide a highly secure exchange of network traffic, and can help satisfy regulatory requirements. Unlike the transport layer solutions, IPSec can protect TCP and UDP applications.

End-to-end encryption with IPSec

Many traditional data center security practices have had data being encrypted by a network device and then flowing in the clear to the server. This worked ok as long as the network was protected from eavesdropping. Regulations and data security policies in several industries have changed and flowing unencrypted data across any connections is no longer acceptable.



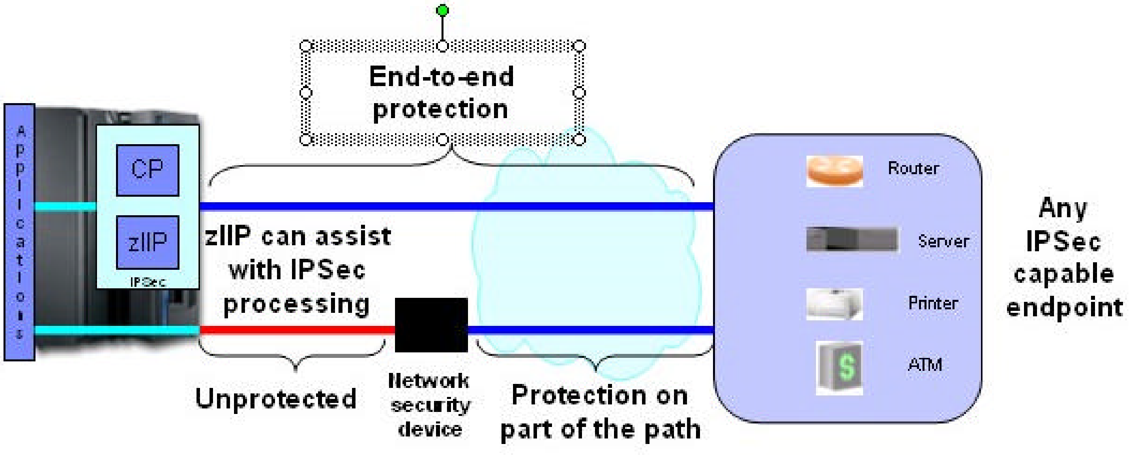
The above picture compares end-to-end encryption between z/OS and remote devices such as servers, printers, ATMs, or point of sale devices. Encrypting data within z/OS itself eliminates the exposure of sending unsecured data across any portion of the network.

zIIP Assisted IPSec

Recognizing that the extra work done for IPSec consumes some extra CPU cycles, IBM has announced the zIIP Assisted IPSec function which will move much of the IPSec workload to an IBM System z9 Integrated Information Processor (zIIP). The zIIP is a specialty engine which is available on the System z9 Enterprise Class (EC) and System z9 Business Class (BC) servers. The zIIP's execution environment accepts eligible work from z/OS, which manages and directs the work between the general purpose processors and the zIIPs. IBM will not impose software charges on zIIP capacity.[1]

[1] Additional IBM software charges will apply when additional general purpose CP capacity is used. The amount of general-purpose processor savings will vary based on the amount of workload executed by the zIIP, among other factors.

zIIP Assisted IPSec



zIIP is designed to help free-up general computing capacity and lower the overall cost of computing for select data and transaction processing. The zIIP, in effect, is a high-speed engine that better enables data to be centralized on the mainframe. The ease and economy of this solution help break down the walls between transactional datastores on the mainframe and BI, ERP and CRM applications that run on distributed computers. With the zIIP capability, the System z9 mainframe helps minimize the need to maintain duplicate copies of the data and provide better security between the applications and the data. Thus, zIIP can help your business by:

- Helping to improve resource optimization.
- May help lower cost of computing for eligible workloads.

The new zIIP Assisted IPSec function will, in effect, turn the zIIP into a high-speed IPSec protocol processing engine that is designed to provide better price performance for IPSec processing.

Protecting your systems

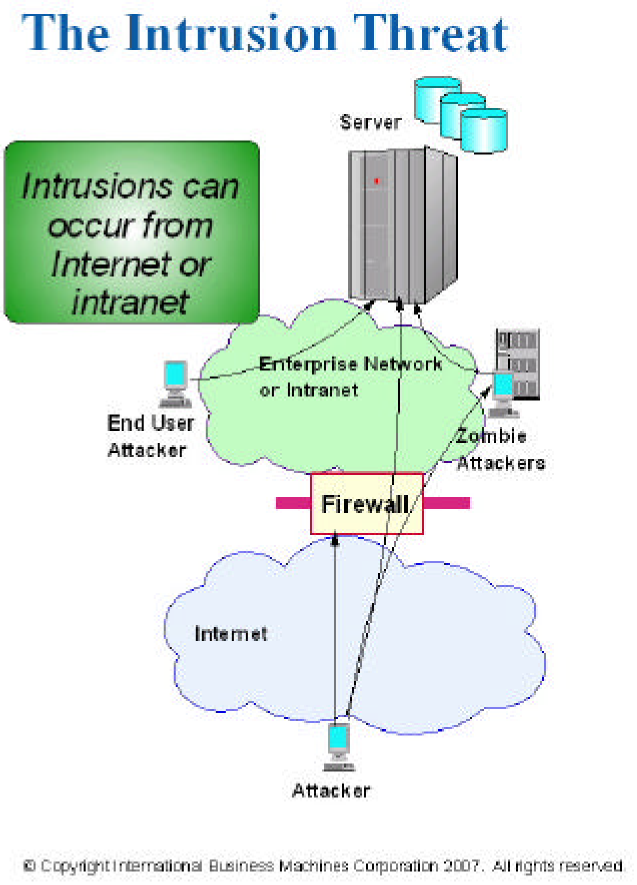
In addition to protecting data while it is flowing in the network, protecting systems from intrusion or attack is vitally important to a comprehensive security plan. z/OS Communications Server offers a robust set of Intrusion Detection Services (IDS) and packet filtering solutions to help protect your systems.

What kind of risks?

There are many types of intrusion or attacks against which you need to protect your systems and data.

Intrusion could take the form of information gathering, sometimes called scans, where someone is trying to learn about your network and system topology or the location or contents of data. This information could be used later to launch an attack against the system or perhaps to obtain access to data that is supposed to be secure. Another class of intrusions include eavesdropping, impersonation, or theft of ids. This could be attempted by someone on the system, or somewhere in the network. If successful, this information will be used for future attacks or intrusions.

Denial of service attacks are designed to impair the availability of an application or an entire system. These are usually done by exploiting a potential vulnerability in the system or an application, or by flooding the system with so much data that it is not able to accomplish any useful work.



The Intrusion Threat

Intrusions can occur from Internet or intranet

As you can see in the picture above, intrusions and attacks can come from outside your network, or within. A firewall on the boundary between your intranet and the internet can provide some protection, but for comprehensive protection, your systems also need to be able to protect themselves.

IDS

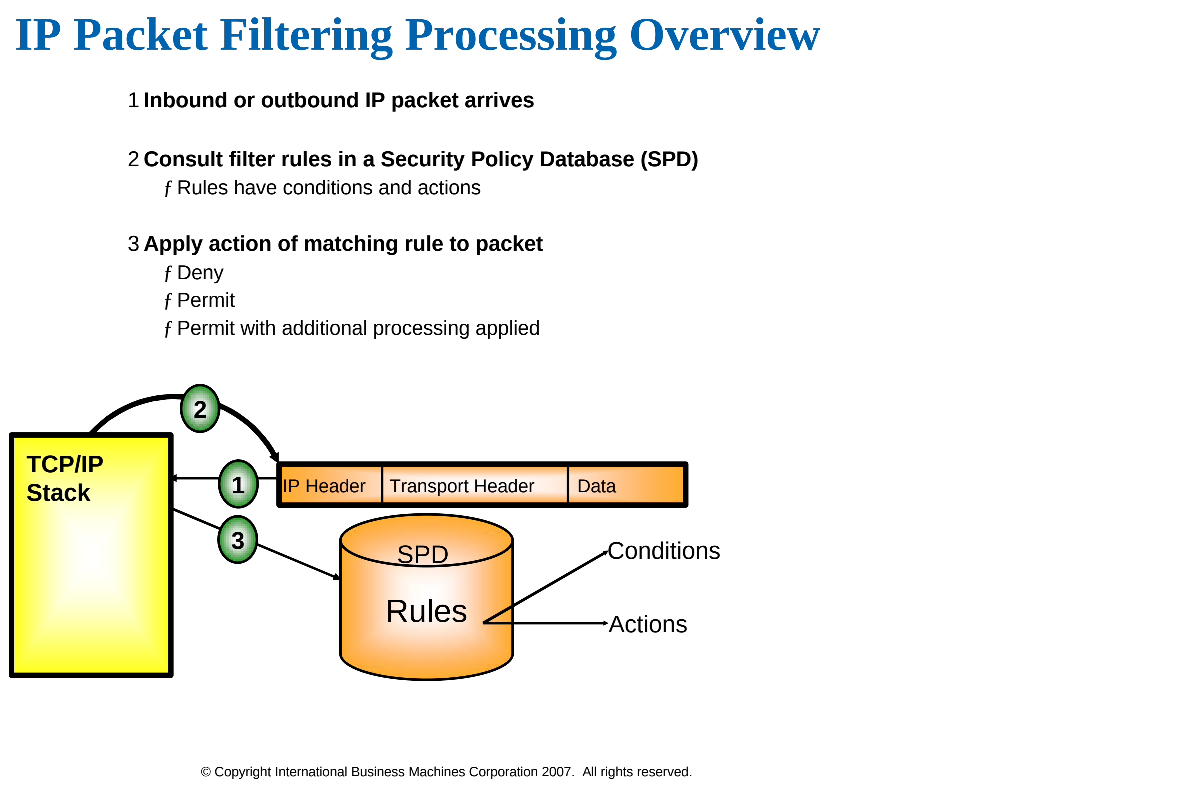
Now that you know some of the risks that you need to consider, we will talk about how IDS can help protect your systems.

IDS is designed to look for events that could represent attacks or intrusion. These events could be scans, attacks against the stack, or flooding the system with TCP or UDP packets. IDS can even evaluate inbound IPSec encrypted data after decryption.

Once IDS detects an event that represents an intrusion or attack, it can report that event and take action against it. Reporting can be done in a variety of ways including logging, messages to a console, an IDS packet trace, and notification to Tivoli NetView and Tivoli Security Operations Manager. In addition to reporting, IDS can take defensive actions. These actions can include discarding packets and limiting the connections to the system or application.

IDS is controlled by a set of policies. These policies define events and what actions IDS should take (reporting, connection limiting, packet discarding) when a potential intrusion event is detected. z/OS Communications Server includes a set of policies to help you get started.

Filtering



IP Packet Filtering Processing Overview

1 **Inbound or outbound IP packet arrives**

2 **Consult filter rules in a Security Policy Database (SPD)**

ƒ Rules have conditions and actions

3 **Apply action of matching rule to packet**

ƒ Deny

ƒ Permit

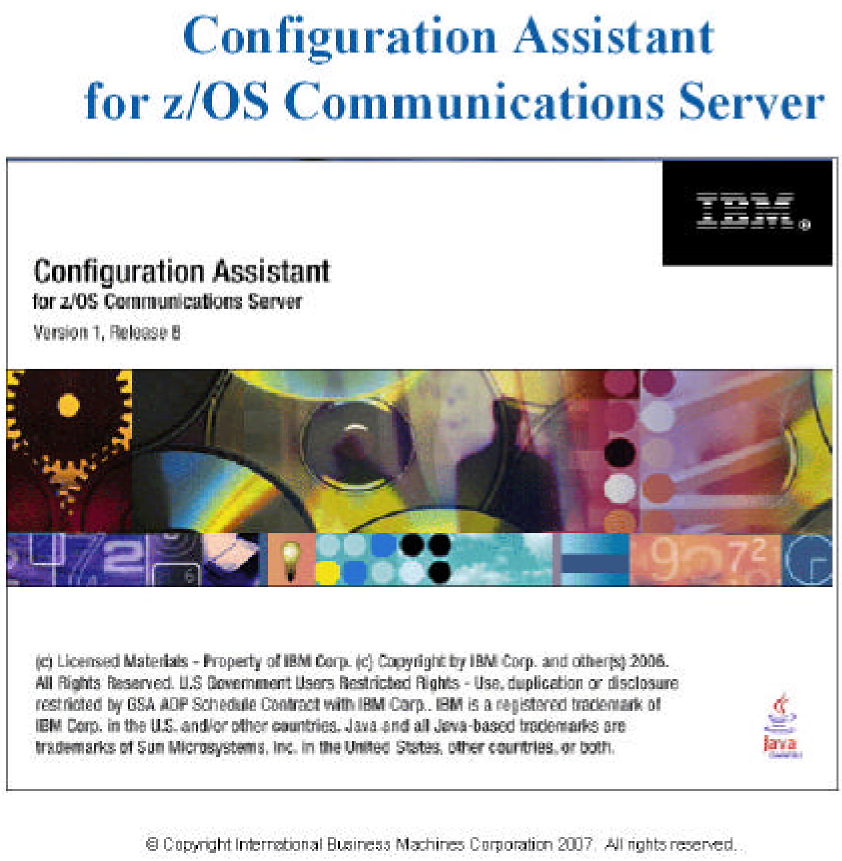
ƒ Permit with additional processing applied

You can also use Packet filtering to defend your systems. IP packet filters are rules defined to either discard or permit packets. These rules can be applied to traffic being routed through a host or traffic in the host that has the communication endpoint. Even when an external firewall provides filtering protection for a host, Communications Server IP packet filtering can act like your own personal firewall and can provide a secondary line of defense.

Making it simpler

We have described some of the main security features available on z/OS Communications Server. Now it is time to review options that simplify the task of implementing these security features.

You configure security such as IDS, IPSec, IP Packet Filtering, and AT-TLS on z/OS Communications Server through policies. Policies are a set of files that define the rules by which the security components should operate. New for z/OS Communications Server V1.8 is the IBM Configuration Assistant for z/OS Communications Server.



Configuration Assistant
for z/OS Communications Server

Configuration Assistant
for z/OS Communications Server
Version 1, Release 8

(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006. All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

© Copyright International Business Machines Corporation 2007. All rights reserved.

The Configuration Assistant is a downloadable[2] tool that provides a single, consistent administration interface for configuring AT-TLS, IP Security, and IDS policies. Instead of having to learn the detailed syntax of the security policies, the Configuration Assistant provides panels that allow you to focus on what traffic to protect and how to protect it.

[2] You can download the IBM Configuration Assistant for z/OS at http://www.ibm.com/support/docview.wss?rs=852&uid=swg24013160

More information

If you want more information on using the security capabilities of z/OS Communications Server or the IBM System z servers, we suggest the following as starting points:

z/OS Communications Server home page: http://www.ibm.com/software/network/commserver/zos

z/OS Communications Server security presentations, whitepapers, and Redbooks: http://www.ibm.com/support/docview.wss?rs=852&uid=swg27009582

Security on IBM System z mainframes: http://www.ibm.com/servers/eserver/zseries/security

IBM System z9 Integrated Information Processor: http://www.ibm.com/systems/z/ziip

Communications Server for z/OS V1R8 TCP/IP Implementation Volume 4: Policy-Based Network Security http://www.redbooks.ibm.com/abstracts/sg247342.html?Open

The IBM Software Services for WebSphere team provides fee-based services including designing solutions, skills transfer, and implementation assistance. For more information, contact Heather Johnson-Dunnings at hjd@us.ibm.com.