IBM Systems – Enterprise Networking Solutions

z/OS Communications Server Policy-Based Networking

May 28, 2015
Lin Overby – overbylh@us.ibm.com
z/OS Communications Server

Trademarks, notices, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC
- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- 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.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

Notes:

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Refer to www.ibm.com/legal/us for further legal information.

Agenda

- Policy-based networking overview

- Frequently used policy disciplines
  - IP Security
  - Application Transparent TLS
  - Intrusion Detection Services

- Policy Agent and Required Infrastructure

Policy-Based Networking

Policy-based networking disciplines

- z/OS Communications Server networking policies dynamically alter the way selected types of IP traffic is treated by TCP/IP on z/OS and in some cases how traffic is treated by equipment in the network

- Types of policy disciplines supported by z/OS Communications Server
  - IP Security
    - IP filters – Controls network traffic allowed in or out of z/OS
    - IPSec – Cryptographic protection using IPSec security associations
  - Application Transparent Transport Layer Security (AT-TLS)
    - Provides TLS support for applications as a TCP/IP stack service
  - Intrusion Detection/Defense Services (IDS)
    - Detects various intrusion attempts against TCP/IP such as scans, attacks, flooding
  - Networking Quality of Service (QoS)
    - Controls TOS, differentiated Services, VLAN priority, QDIO priority queues, etc.
  - Policy-based Routing (PBR) –
    - Controls selection of network interface, first-hop router, MTU size

What is policy?

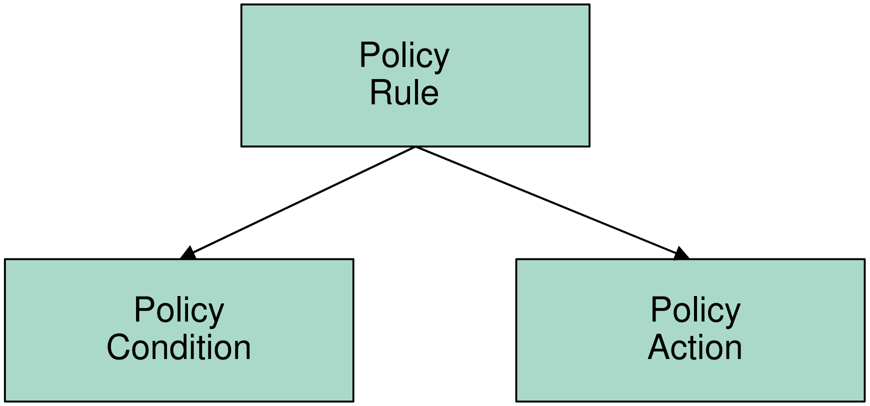
Policies consist of one or more policy rules:

- A policy rule is the main object and refers to:
  - Policy conditions:
    - Defines conditions which must be met to match on the policy rule

    Example: Outbound packet with specified destination IP address
  - Policy actions:
    - Defines action to be taken when policy condition is met

    Example: Perform IPSec processing on packet
- A policy, once enabled, is enforced by the TCP/IP stack

Basic Policy Objects

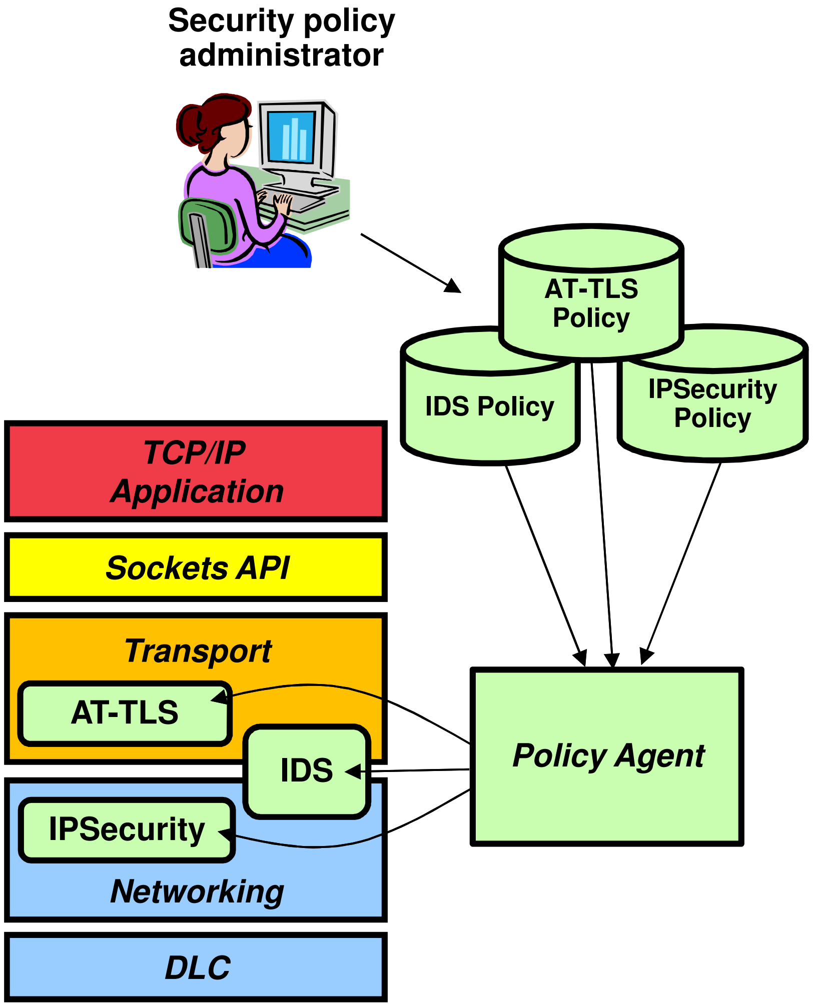


Policy Objects Relationship:

IF condition THEN Action

Policy-based networking on z/OS overview

- Policy is created through Configuration Assistant for z/OS Communications Server
  - z/OSMF-based tool
  - Configures each discipline (e.g. AT-TLS, IP Security, IDS) using consistent model
  - Generates and saves/uploads policy files to target z/OS system
- Policy Agent processes and installs policies into TCP/IP stack
  - Policies are defined per TCP/IP stack
  - Separate policies for each discipline
  - Policy agent also monitors and manages the other daemons and processes needed to enforce the policies (IKED, syslogd, trmd, etc.)
- Provides network policy services without requiring changes to your applications
  - Policies are enforced by TCP/IP stack
  - Different security disciplines are enforced independently of each other



IP Security

z/OS IP Security features

- IP (network) layer technology
  - Completely transparent to application
  - Supports all IP traffic, regardless of higher-layer protocols

- IP packet filtering control whether packets are permitted, discarded, or permitted with IPSec protection

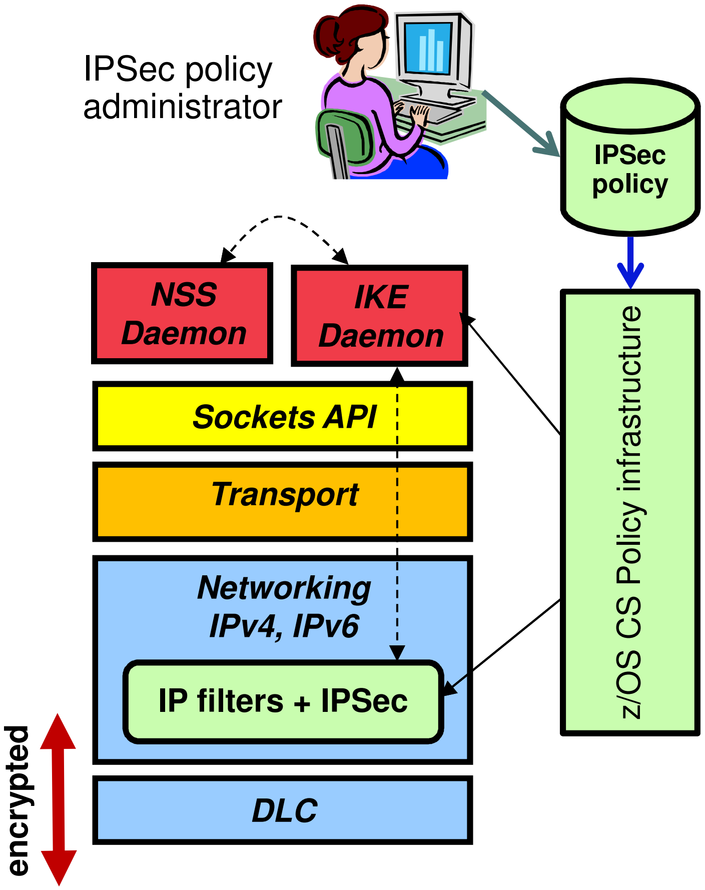
- A complete IPSec implementation
  - Authentication Header (AH) and Encapsulating Security Payload (ESP) Security Associations (SAs)
  - Transport and Tunnel Mode
  - Supports host and gateway roles
  - IKE version 1 and version 2 (RFC 5996)

- Wide range of modern cryptographic algorithms including AES (multiple modes), SHA2, SHA1, RSA, ECDSA, etc.

- Supports NAT Traversal and NAPT

- IPSec is sysplex-enabled
  - Sysplex-wide Security Associations allow SAs to be shared across the sysplex

- IPSec processing is zIIP-assisted
  - Moves IPSec processing from general CPs to zIIPs
  - All inbound IPSec traffic and a good portion of outbound IPSec traffic is processed on a zIIP processor



Full application payload encryption
.... plus some network protocol header fields

IPSec encryption:

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	>::"	*&hU$$$$	@%$#dd*&&^s^!:"J)*bGVM> (*hhgvvv<

IP header encryption varies based on transport/tunnel mode, and AH/ESP protocol

IPSec Scenarios and z/OS Roles

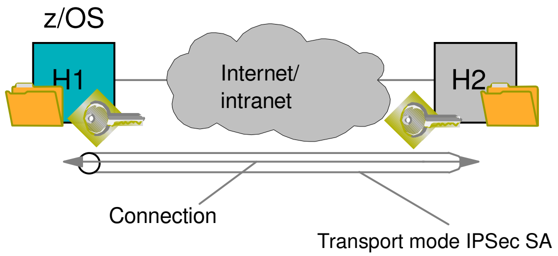
Legend

Data endpoint

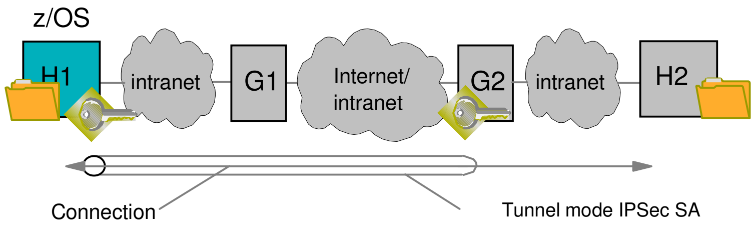
Security endpoint

z/OS as Host (Data Endpoint)

Host-to-Host: End-to-End Security Association

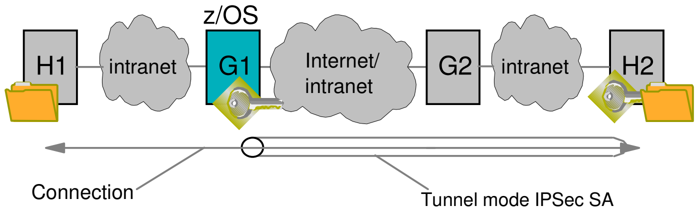


Host-to-gateway: Protect segment of data path

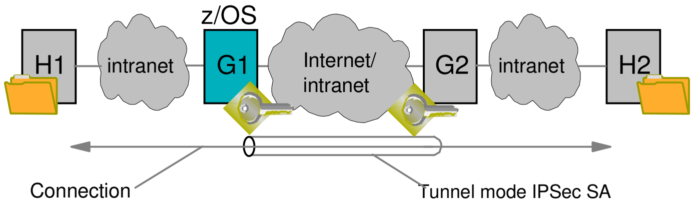


z/OS as Gateway (Routed Traffic)

Gateway-to-Host:
Protection over Untrusted Network Segment



Gateway-to-Gateway:
Protection over Untrusted Network Segment

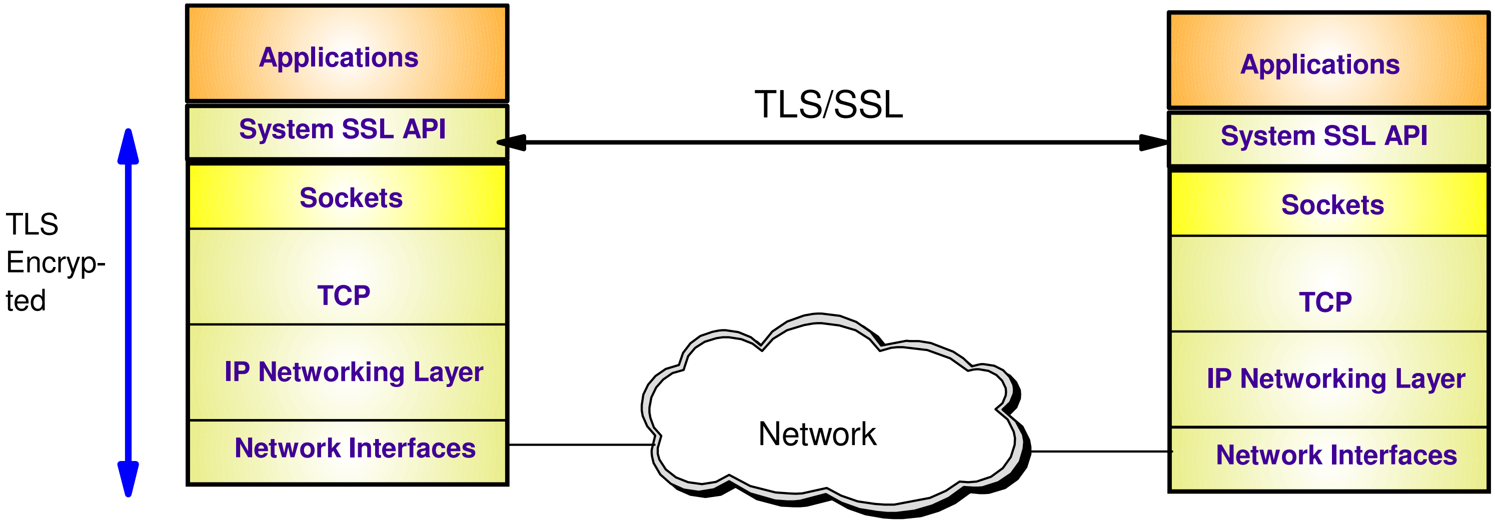


Some z/OS workloads that use IPSec

- Can provide “blanket” protection for all workloads between hosts
- Can provide selective protection for specific workloads:
  - Enterprise Extender (SNA applications over an IP network)
    - Since EE uses UDP/IP, TLS/SSL is not a viable option
    - IPsec is used heavily and very successfully in the industry for protecting EE traffic
    - IPSec protection can be set up for very specific EE traffic – even down to the specific EE ports if so desired
  - Internet Control Message Protocol (ICMP and ICMPv6)
    - These are their own IP protocols
    - Used for things like neighbor discovery, path validation, etc.
  - UDP-based protocols:
    - Domain Name System (DNS)
    - Network File System (NFS), Remote Procedure Call (RPC) and Portmapper (can be run over UDP)
    - Simple Network Management Protocol (SNMP)
  - TCP-based protocols whose implementations typically do not support TLS/SSL
    - sendmail / SMTP
    - Line Print Daemon (LPD)
  - We have seen IPSec deployments also for TCP workloads that are typically secured using TLS
    - TN3270
    - FTP

Application Transparent Transport Layer Security

Transport Layer Security enablement



- TLS traditionally provides security services as a socket layer service
  - TLS requires reliable transport layer,
    - Typically TCP (but architecturally doesn't have to be TCP)
  - UDP applications cannot be enabled with traditional TLS
    - There is now a TLS variant called Datagram Transport Layer Security (DTLS) which is defined by the IETF for unreliable transports
- On z/OS, System SSL (a component of z/OS Cryptographic Services) provides an API library for TLS-enabling your C and C++ applications
- Java Secure Sockets Extension (JSSE) provides libraries to enable TLS support for Java applications
  - However, there is an easier way…

… Application Transparent TLS!

z/OS Application Transparent TLS overview

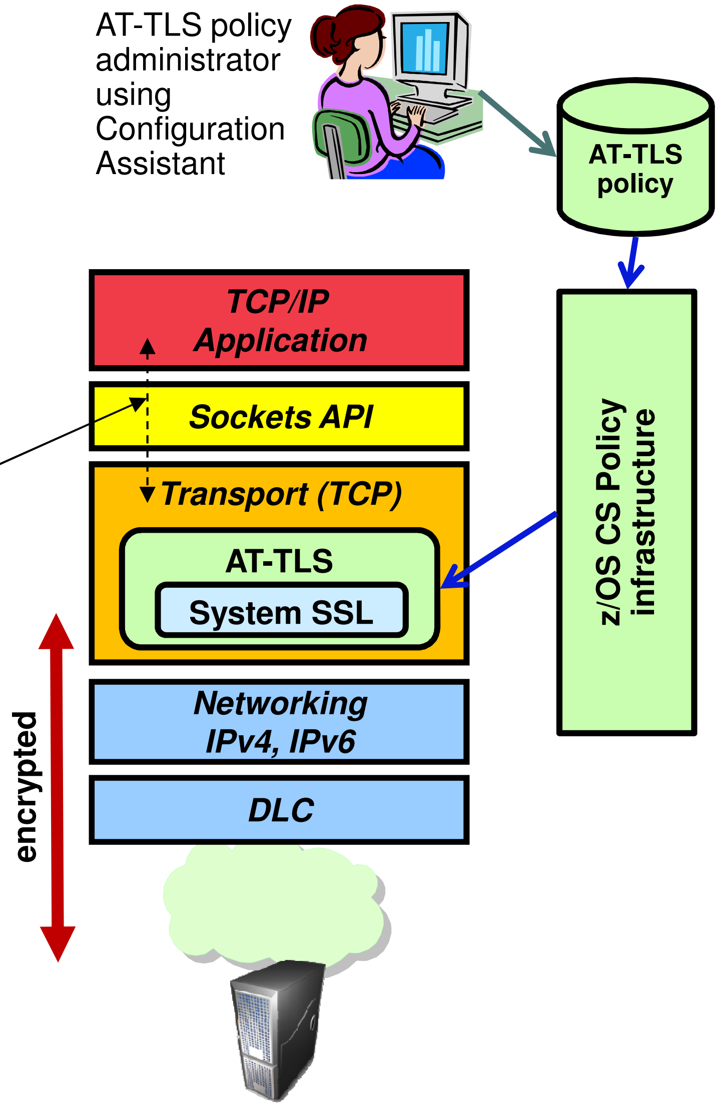
- **Stack-based TLS**
  - TLS process performed in TCP layer (via System SSL) without requiring any application change (transparent)
  - AT-TLS policy specifies which TCP traffic is to be TLS protected based on a variety of criteria
    - Local address, port
    - Remote address, port
    - Connection direction
    - z/OS userid, jobname
    - Time, day, week, month

- **Application transparency**
  - Can be fully transparent to application
  - An optional API allows applications to inspect or control certain aspects of AT-TLS processing – "application-aware" and "application-controlled" AT-TLS, respectively

- **Available to TCP applications**
  - Includes CICS Sockets
  - Supports all programming languages except PASCAL

- **Supports standard configurations**
  - z/OS as a client or as a server
  - Server authentication (server identifies self to client)
  - Client authentication (both ends identify selves to other)

- **Uses System SSL for TLS protocol processing**
  - Remote endpoint sees an RFC-compliant implementation
  - Interoperates with other compliant implementations



Some z/OS applications that use AT-TLS

- CommServer applications
  - TN3270 Server
  - FTP Client and Server
  - CSSMTP
  - Load Balancing Advisor
  - IKE NSS client
  - NSS server
  - Policy agent
  - DCAS server
- DB2 DRDA
- IMS-Connect
- JES2 NJE
- IBM Multi-Site Workload Lifeline
- Tivoli Netview applications
  - MultiSystem Manager
  - NetView Management Console
- RACF Remote Sharing Facility
- CICS Sockets applications
- InfoSphere Guardium S-TAP
- 3rd Party applications
- Customer applications

Advantages of using AT-TLS

- **Reduce costs**
  - Application development
    - Cost of System SSL integration
    - Cost of application's TLS-related configuration support
  - Consistent TLS administration across z/OS applications
  - Gain access to new features with little or no incremental development cost

- **Complete and up-to-date exploitation of System SSL features**
  - AT-TLS makes the vast majority of System SSL features available to applications
  - AT-TLS keeps up with System SSL enhancements – as new features are added, your applications can use them by changing AT-TLS policy, not code

- **Ongoing performance improvements**

  Focus on efficiency in use of System SSL

- **Great choice if you haven't already invested in System SSL integration**

  Even if you have, consider the long-term cost of keeping up vs. short term cost of conversion

Recent AT-TLS enhancements

…Added in z/OS V2R1

- TLS Protocol Version 1.2 (RFC 5246):
  - Twenty-one new cipher suites
    - 11 new HMAC-SHA256 cipher suites
    - 10 new AES-GCM cipher suites
- Support Elliptic Curve Cryptography (ECC)
  - Twenty new ECC cipher suites
    - ECC cipher suites for TLS (RFC 4492)
- Support for Suite B cipher suites (RFC 5430)
  - TLS 1.2 is required
  - ECC is required
  - Suite B has two levels of cryptographic strength that can be selected
    - 128 or 192 bit
- Transport Layer Security (TLS) Renegotiation Extension (RFC 5746):
  - Provides a mechanism to protect peers that permit re-handshakes
  - When supported, it enables both peers to validate that the re-handshake is truly a continuation of the previous handshake

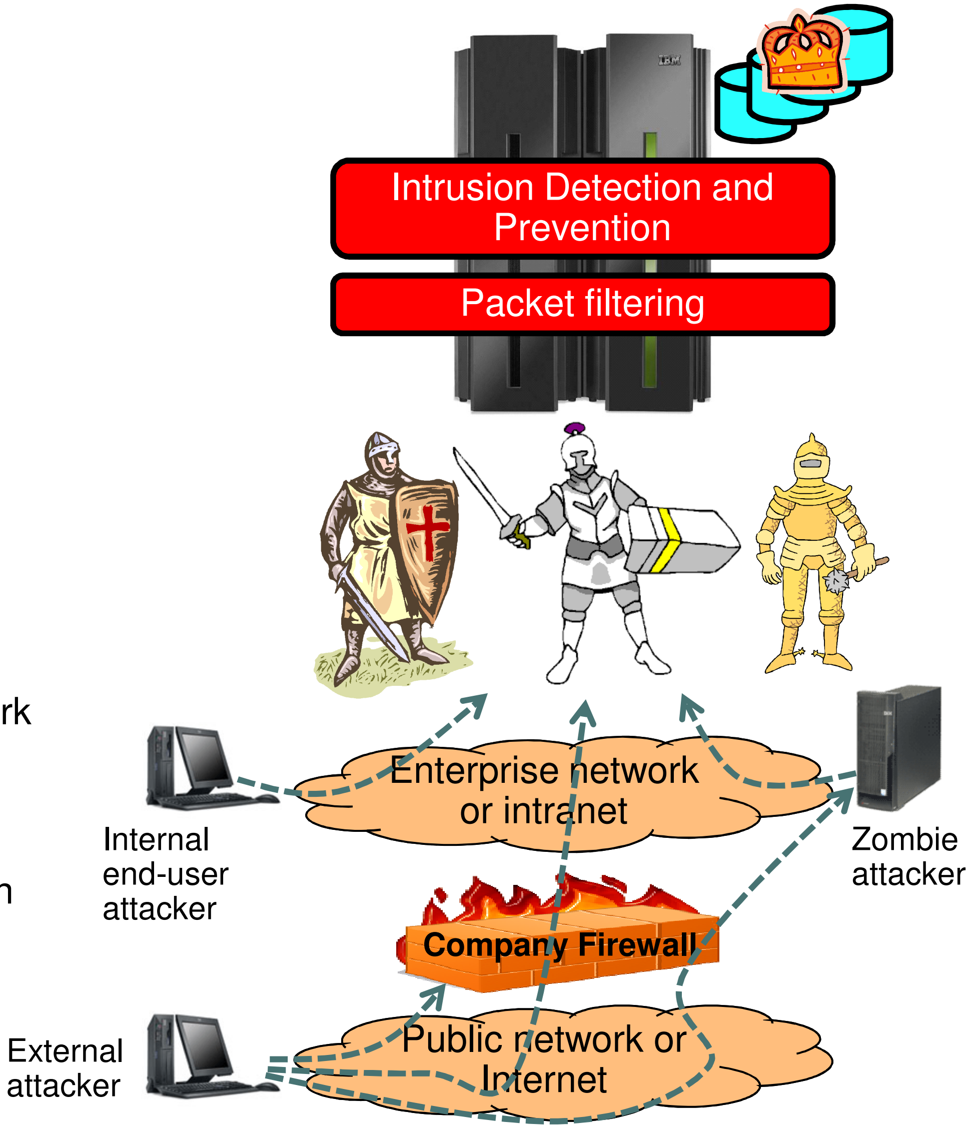
… Planned for z/OS V2R2

- Support retrieval of revocation information through the Online Certificate Status Protocol (OCSP)
- Support HTTP retrieval of CRLs
- Support for RFC 5280 certificate validation mode

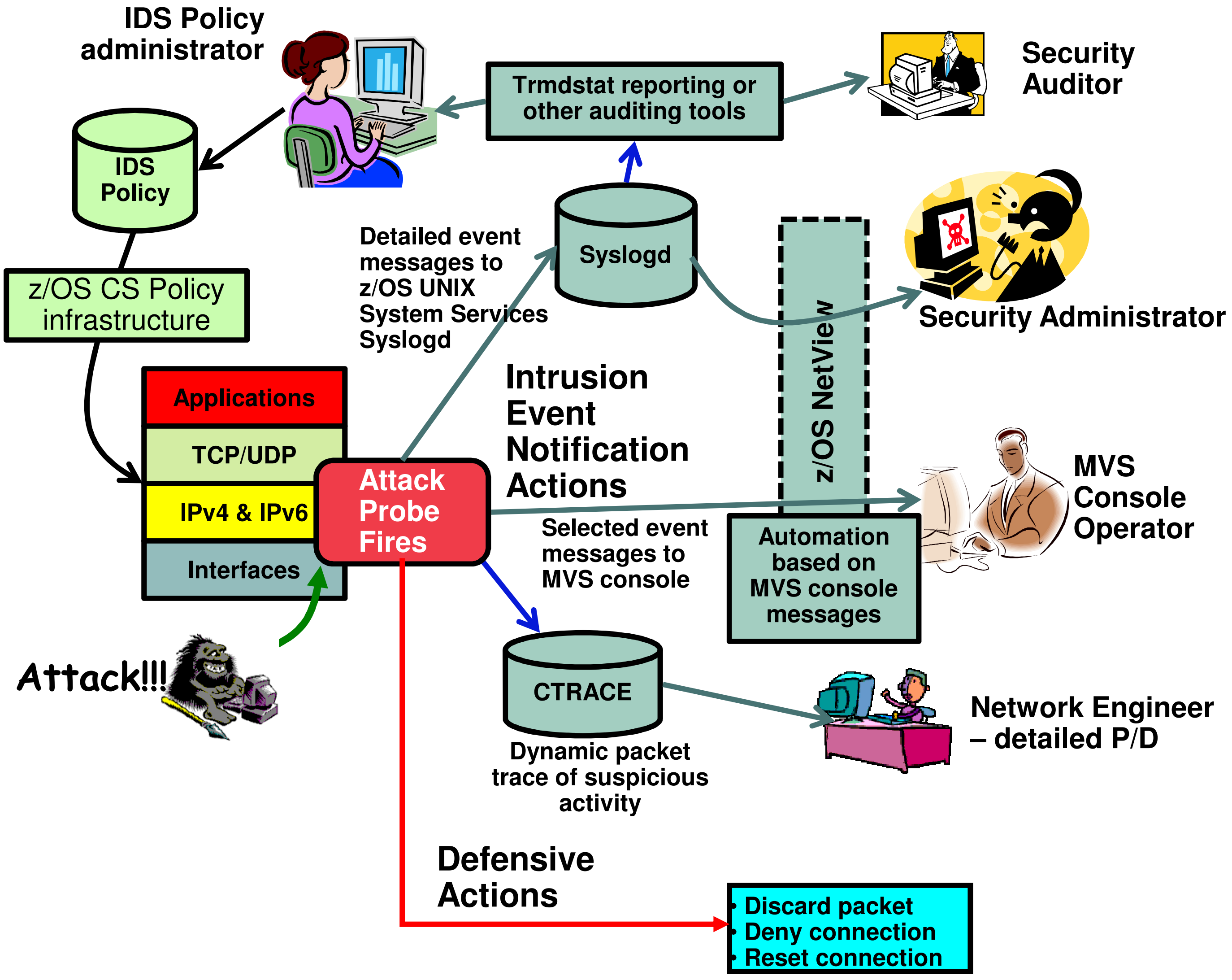
Intrusion Detection Services

The intrusion threat

- **What is an intrusion?**
  - Information Gathering
    - Network and system topology
    - Data location and contents
  - Eavesdropping/Impersonation/Theft
    - On the network/on the host
    - Base for further attacks on others through Amplifiers, Robots, or Zombies
  - Denial of Service - Attack on availability
    - Single packet attacks - exploits system or application vulnerability
    - Multi-packet attacks - floods systems to exclude useful work
- **Attacks cans be deliberate or unintentional**
  - Deliberate: malicious intent from outside or internal users or bots
  - Unintentional: various forms of errors on network nodes
- **Attacks can occur from Internet or intranet**
  - Company firewalls and intrusion prevention appliances can provide some level of protection from Internet
  - Perimeter security strategy alone may not be sufficient.
    - Some access is permitted from Internet – typically into a Demilitarized Zone (DMZ)
    - Trust of intranet


Intrusion Detection and Prevention
Packet filtering
Enterprise network or intranet
Internal end-user attacker
Zombie attacker
Company Firewall
External attacker
Public network or Internet

z/OS Communications Server IDS overview



IDS Policy administrator

IDS Policy

z/OS CS Policy infrastructure

Applications

TCP/UDP

IPv4 & IPv6

Interfaces

Attack!!!

Attack Probe Fires

Trmdstat reporting or other auditing tools

Security Auditor

Detailed event messages to z/OS UNIX System Services Syslogd

Syslogd

z/OS NetView

Security Administrator

Intrusion Event Notification Actions

Selected event messages to MVS console

Automation based on MVS console messages

MVS Console Operator

CTRACE

Dynamic packet trace of suspicious activity

Network Engineer – detailed P/D

Defensive Actions

- Discard packet
- Deny connection
- Reset connection

z/OS Communications Server IDS features

IDS Events

- **Scans** – attempts by remote nodes to discover information about the z/OS system
- **Attacks –** numerous types
  - Malformed packets
  - IP option and IP protocol restrictions
  - Specific usage ICMP
  - Interface and TCP SYN floods
  - and so forth…

- **Traffic Regulation**
  - **TCP -** limits the number of connections any given client can establish
  - **UDP –** limits the length of data on UDP queues by port

Defensive actions

- Packet discard
- Limit connections
- Drop connections

Reporting

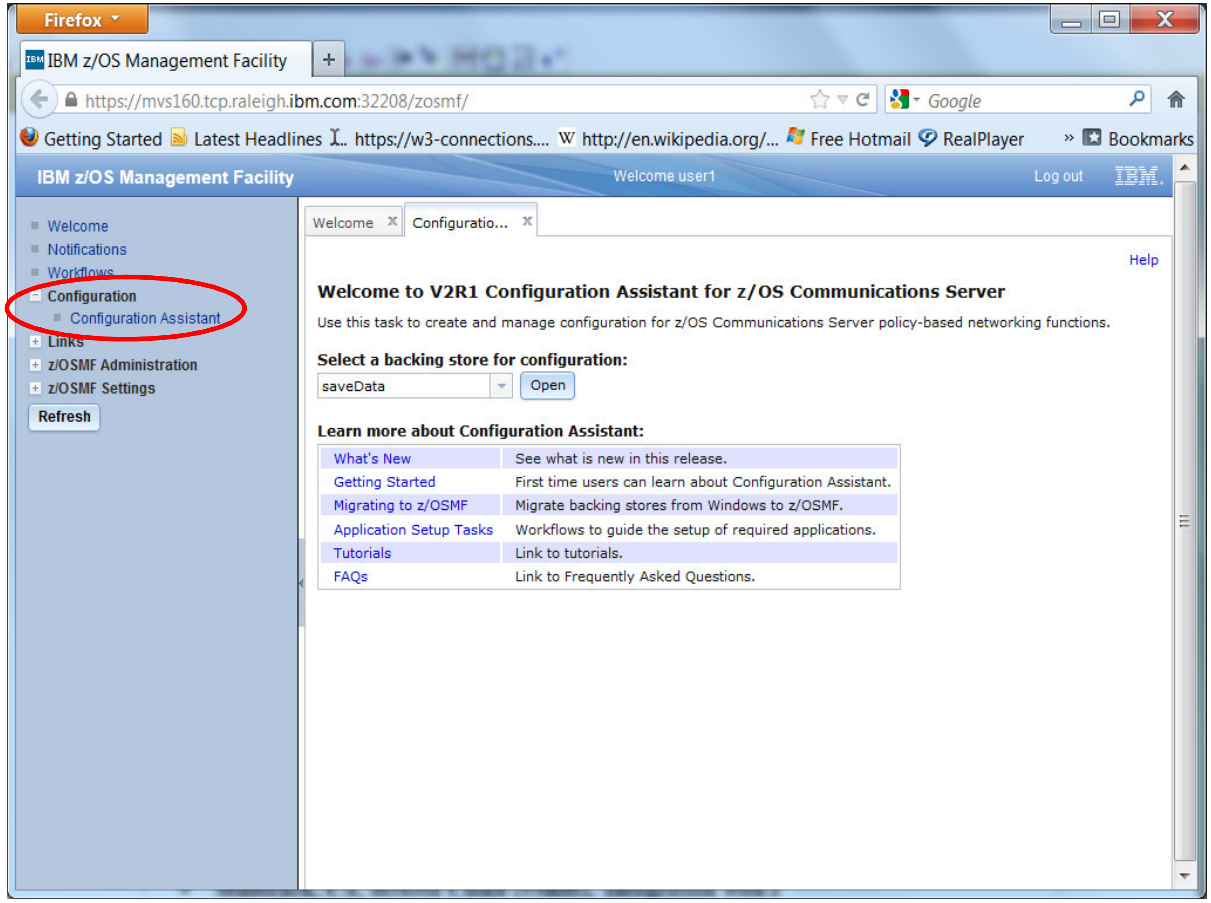
- Logging
- Console messages
- IDS packet trace
- Notifications to external event managers (like Tivoli NetView)

z/OS in-context IDS broadens overall intrusion detection coverage:

- Ability to evaluate inbound encrypted data - IDS applied after IPSec decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack probe fires
- Detects statistical anomalies realtime - target system has stateful data / internal thresholds that generally are unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

Policy Configuration

Configuration Assistant for z/OS Communications Server



Welcome to V2R1 Configuration Assistant for z/OS Communications Server

Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

Select a backing store for configuration:

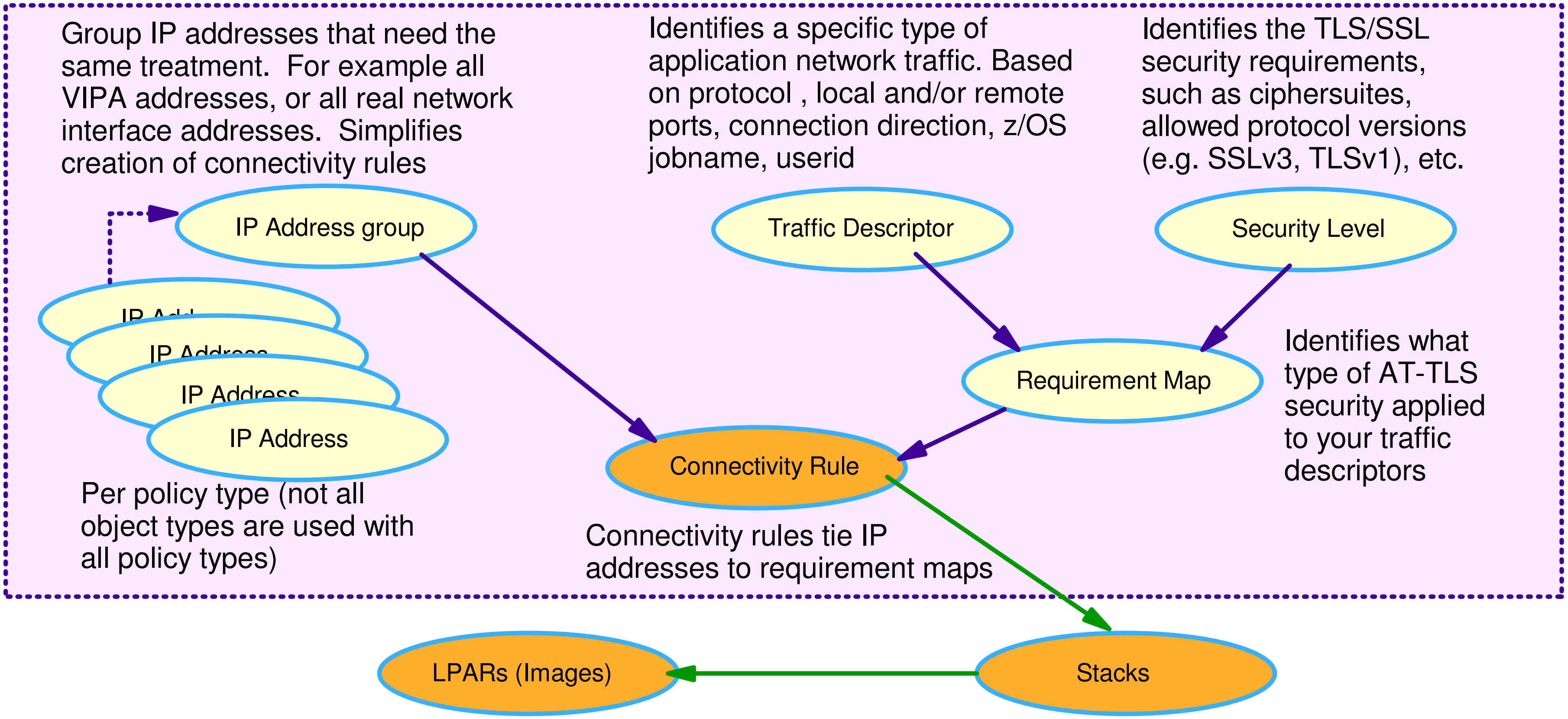
saveData [Open]

Learn more about Configuration Assistant:

What's New	See what is new in this release.
Getting Started	First time users can learn about Configuration Assistant.
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Application Setup Tasks	Workflows to guide the setup of required applications.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.

- **Configures:**
  - AT-TLS
  - IPSec and IP filtering
  - IDS
  - Quality of Service
  - Policy-based routing
- **Separate perspectives but consistent model for each discipline**
- **Focus on concepts, not details**
  - What traffic to protect
  - How to protect it
  - De-emphasize low-level details (though they are accessible through advanced panels)
- **z/OSMF-based web interface**
  - Standalone Windows application
    - Not supported after z/OS V1R13
- **Builds and maintains**
  - Policy files
  - Related configuration files
  - JCL procs and RACF directives

Configuration Assistant reusable object model – AT-TLS example



Group IP addresses that need the same treatment. For example all VIPA addresses, or all real network interface addresses. Simplifies creation of connectivity rules

Identifies a specific type of application network traffic. Based on protocol , local and/or remote ports, connection direction, z/OS jobname, userid

Identifies the TLS/SSL security requirements, such as ciphersuites, allowed protocol versions (e.g. SSLv3, TLSv1), etc.

IP Address group

Traffic Descriptor

Security Level

IP Add

IP Address

IP Address

IP Address

Requirement Map

Identifies what type of AT-TLS security applied to your traffic descriptors

Connectivity Rule

Per policy type (not all object types are used with all policy types)

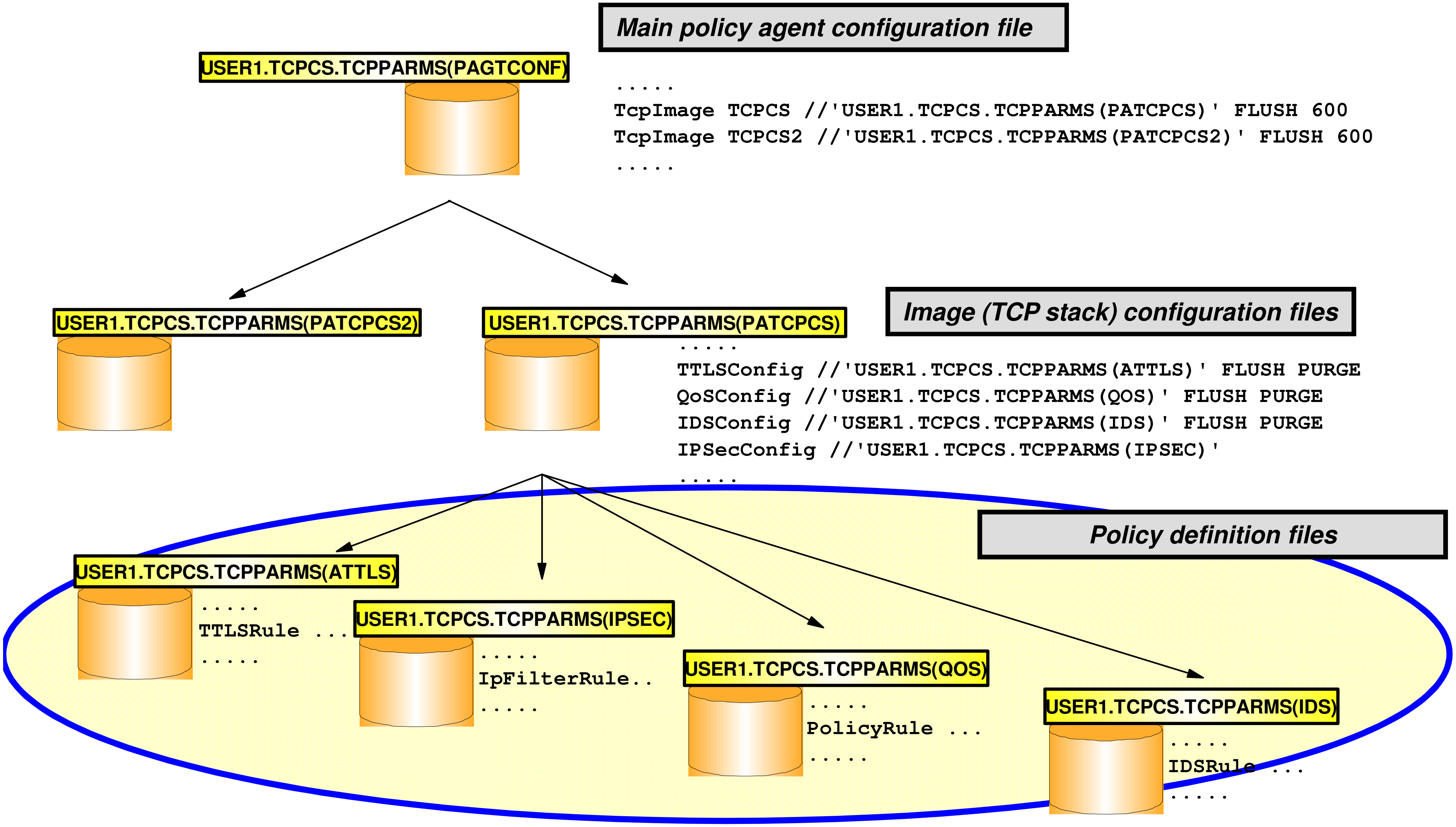
Connectivity rules tie IP addresses to requirement maps

LPARs (Images)

Stacks

1. Create system image and TCP/IP stack image
2. Create one or more Requirement Maps to define desired security for common scenarios (e.g. intranet, branch office, business partner)
   - Create or reuse Security Levels to define security actions
   - Create or reuse Traffic descriptors to define application ports to secure
3. Create one or more Connectivity Rules between Data Endpoints (IP addresses) and associate with a configured Requirement Map

A sample policy agent configuration file and policy definition file structure



Main policy agent configuration file

USER1.TCPCS.TCPPARMS(PAGTCONF)

```
.....
TcpImage TCPCS //'USER1.TCPCS.TCPPARMS(PATCPCS)' FLUSH 600
TcpImage TCPCS2 //'USER1.TCPCS.TCPPARMS(PATCPCS2)' FLUSH 600
.....
```

Image (TCP stack) configuration files

USER1.TCPCS.TCPPARMS(PATCPCS2)

USER1.TCPCS.TCPPARMS(PATCPCS)

```
.....
TTLSConfig //'USER1.TCPCS.TCPPARMS(ATTLS)' FLUSH PURGE
QoSConfig //'USER1.TCPCS.TCPPARMS(QOS)' FLUSH PURGE
IDSConfig //'USER1.TCPCS.TCPPARMS(IDS)' FLUSH PURGE
IPSecConfig //'USER1.TCPCS.TCPPARMS(IPSEC)'
.....
```

Policy definition files

USER1.TCPCS.TCPPARMS(ATTLS)

```
.....
TTLSRule ...
.....
```

USER1.TCPCS.TCPPARMS(IPSEC)

```
.....
IpFilterRule..
.....
```

USER1.TCPCS.TCPPARMS(QOS)

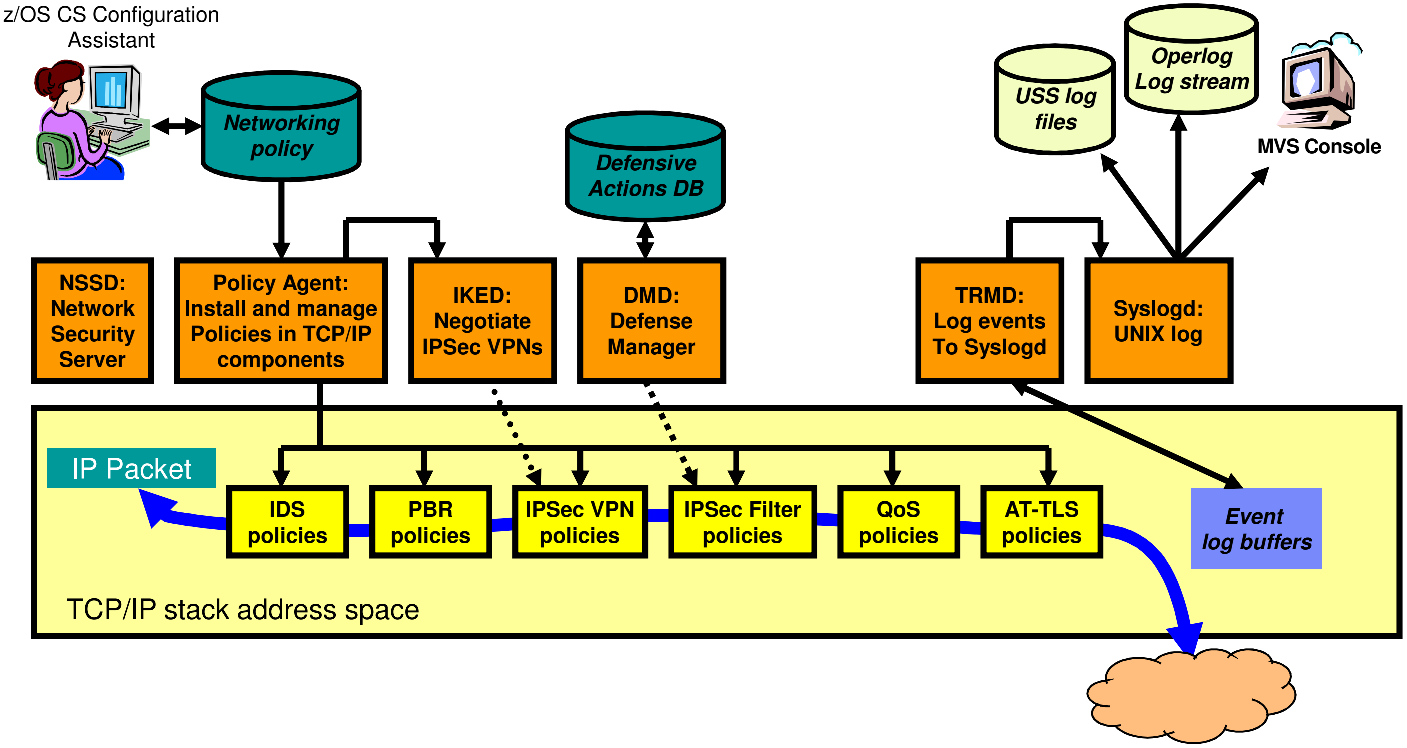
```
.....
PolicyRule ...
.....
```

USER1.TCPCS.TCPPARMS(IDS)

```
.....
IDSRule ...
.....
```

Policy Agent and Required Infrastructure

z/OS CS networking policy infrastructure overview



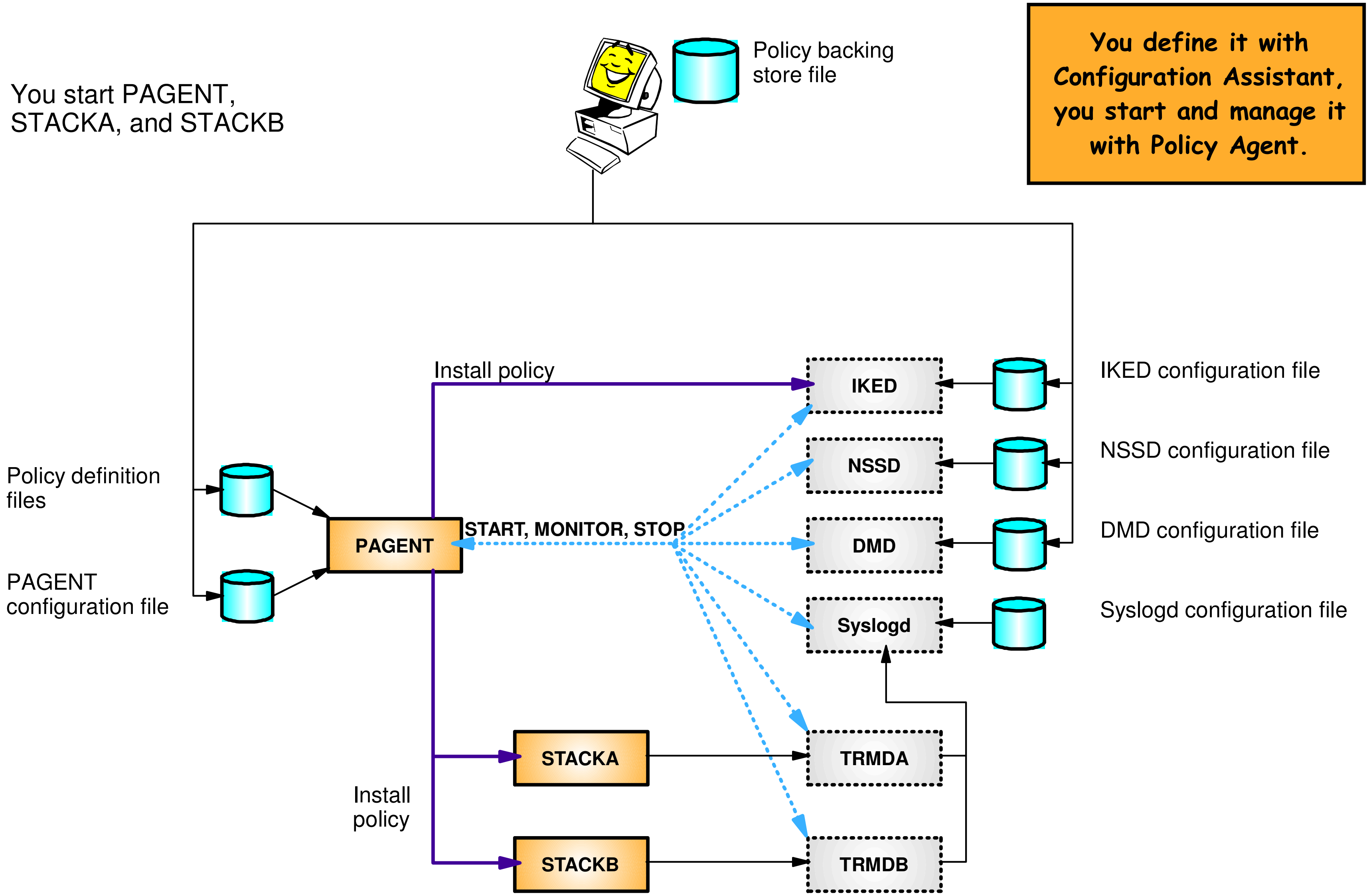
- **Configuration Assistant** – provides administrative user interface to configure policies, and other policy agent infrastructure configuration
- **Policy Agent** - installs and maintains policies in TCP/IP stacks (required for all policy types)
- **TRMD** - formats and sends messages from the TCP/IP stack to SyslogD (required for all policy types)
- **SyslogD** - UNIX System Services logging focal point (required for all policy types)
- **IKED** - Internet Key Exchange Daemon, used for dynamic VPNs (required for IPSec dynamic SA negotiation)
- **NSSD** - Network Security Server, centralized network security server (optional for IPSec)
- **DMD** - Defense Manager Daemon (dynamic defensive IP filters)

Policy infrastructure management overview

- Policy agent can be set up to manage the policy agent infrastructure applications

You define it with Configuration Assistant, you start and manage it with Policy Agent.

You start PAGENT, STACKA, and STACKB



Sample Policy Agent configuration for monitoring dependent functions

```
AutoMonitorParms
{
  MonitorInterval         10
  RetryLimitCount         5
  RetryLimitPeriod        600
}

AutoMonitorApps
{
  AppName         IKED
  {
    ProcName      IKED
    JobName       IKED
    EnvVar        IKED_FILE=//'USER1.POLICY.PROD.MVS098(IKEDCONF)'
  }
  AppName         SYSLOGD
  {
    ProcName      SYSLOGD
    JobName       SYSLOGD
    EnvVar        SYSLOGD_CONFIG_FILE=//'USER1.TCPCS.TCPPARMS(SYSLOGT)'
    StartParms    -c -u -i
  }
  AppName         TRMD
  {
    TcpImageName  TCPCS
    {
      ProcName    TRMD
      JobName     TRMD1
      StartParms  -p TCPCS
    }
  }
}
```

The Configuration Assistant will generate the initial set of definitions. You may want to update file locations, etc.

Policy Agent console commands for monitored applications

- You must use Policy Agent operator commands to start, stop, or restart monitored applications, so status can be maintained
  - For example if you monitor IKED, and issue a P IKED command, Policy Agent automatically restarts IKED

- Format of Policy Agent operator command for applications:

  F pagproc,MON,operation,application[,P=image]
  - operation is START, STOP, RESTART
  - application is DMD, IKED, NSSD, SYSLOGD, TRMD, ALL
  - image is TCP/IP stack name for TRMD

  - Example: F PAGENT,MON,STOP,IKED

- Tip: Stop all monitored applications before stopping Policy Agent if you want to shut down the whole policy infrastructure

```
F PAGENT,MON,DISPLAY
EZD1588I PAGENT MONITOR INFORMATION 142
APPLICATION  MONITORED  JOBNAME  STATUS      TCP/IP STACK
DMD          NO         N/A      N/A         N/A
IKED         YES        IKED     ACTIVE      N/A
NSSD         NO         N/A      N/A         N/A
SYSLOGD      YES        SYSLOGD  ACTIVE      N/A
TRMD         YES        TRMD1    ACTIVE      TCPCS
```

Controlling policy agent

- Policy Agent supports MVS console modify commands

- An F PAGENT,REFRESH command can be used to ask PAGENT to reread all its configuration and policy flat files and re-install those
  - Useful after you have made an update to your policy flat files
  - A REFRESH command will refresh all policies

```
12.33.57  f pagent,refresh
12.33.57  EZZ8443I PAGENT MODIFY COMMAND ACCEPTED
12.33.58  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : IDS
12.33.58  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : QOS
12.33.58  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : TTLS
```

- Policy Agent also supports an F PAGENT,UPDATE command that can be used to have PAGENT only update those policies that have been changed as opposed to doing a total refresh

```
12.35.37  f pagent,update
12.35.37  EZZ8443I PAGENT MODIFY COMMAND ACCEPTED
12.35.37  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : NONE
```

- Policy Agent can be stopped using a P command

```
p pagent
```

z/OS Communications Server policy-based networking

- z/OS Communications Server policy-based networking adds valuable application transparent, dynamic packet handling capabilities with fine-grained controls to basic z/OS TCP/IP function:

✓ Block unwanted traffic from entering or leaving z/OS (IPSec filtering)

✓ Connection-level security for TCP applications without application changes (AT-TLS)

✓ Make sure high-priority traffic gets high-priority processing by the network (QoS)

✓ Application-specific selection of outbound interface and route (PBR)

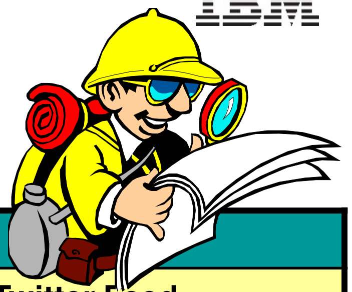
✓ Secure end-to-end IPSec protection (IPSec)

✓ Protecting against “bad guys” trying to attack your z/OS system (IDS)

- The Configuration Assistant for z/OS Communications Server greatly simplifies the initial setup and ongoing modifications

- Policy agent management of infrastructure simplifies the ongoing operations of the policy-based networking environment

For more information…



URL	Content
http://www.twitter.com/IBM_Commserver	IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver	IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/	IBM Communications Server library
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server