



IBM Software Group

# Monitoring IP filters and IPSec tunnels on your z/OS systems

Ovies Brabson  
IBM Corporation

[oviesb@us.ibm.com](mailto:oviesb@us.ibm.com)



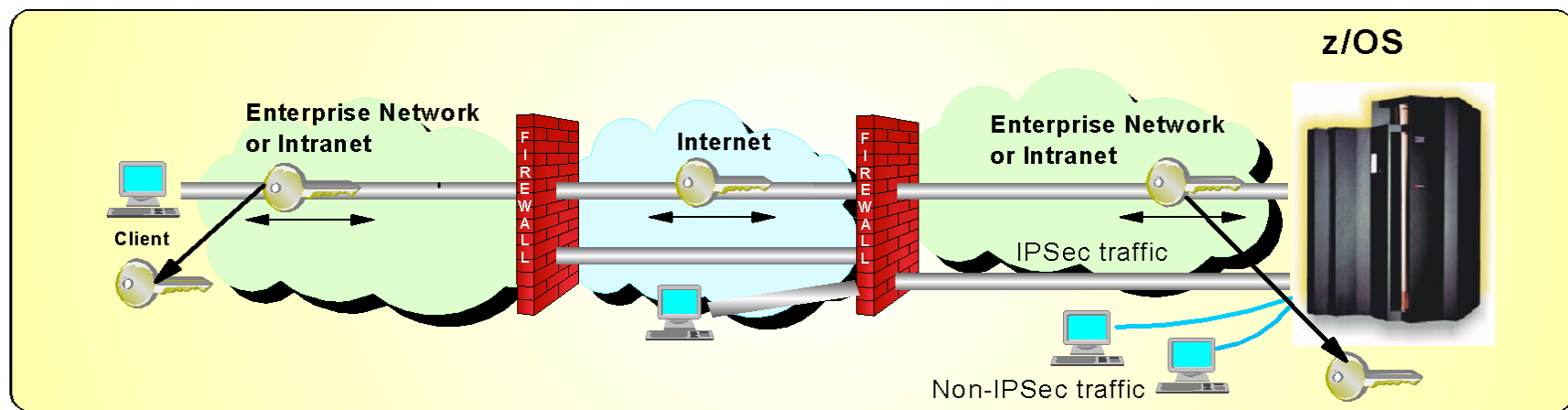
@business on demand software

# Agenda

- Introduction
- IP Security Concepts and Terminology
- OMEGAMON XE for Mainframe Networks IP Security Monitoring Application
  - ▶ Tivoli Management Services Common Features
  - ▶ OMEGAMON XE for Mainframe Networks
  - ▶ Common IP Security Problems
  - ▶ IP Security Status – The Dashboard
  - ▶ IP Security Situations and Thresholds
  - ▶ IP Security Historical Views
- **Sample Scenarios**
- **Description of IP Security Workspaces**
- Reference



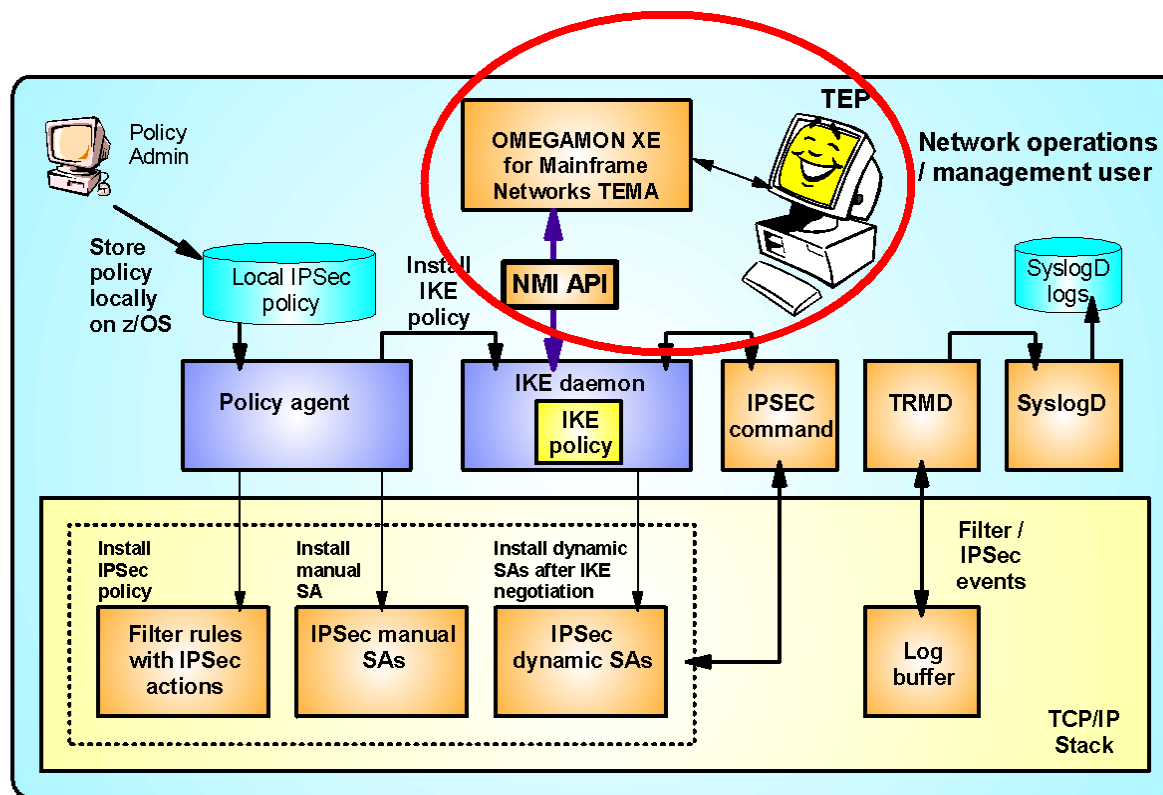
# z/OS IP Security Support



- Prior to z/OS V1R7, IP security packaged with Firewall Technologies
  - ▶ TCP/IP IPsec and IP filtering support
  - ▶ IKE daemon and configuration
- In z/OS V1R7, IP security solution is part of z/OS Communications Server
  - ▶ Alternative to Firewall Technologies
  - ▶ New IKE daemon and configuration
  - ▶ Services
    - IP filtering
    - Manual IPsec
    - Dynamic IPsec (IKE)
    - Filter directed logging to syslogd

# IP Security Network Management Interface (NMI)

- z/OS Communications Server V1R9 adds IPsec NMI allowing applications to monitor IP filters and IPsec tunnels. APARs PK43352, PK43353, PK50322 provide function in z/OS V1R8.



*(IKE tunnels)*

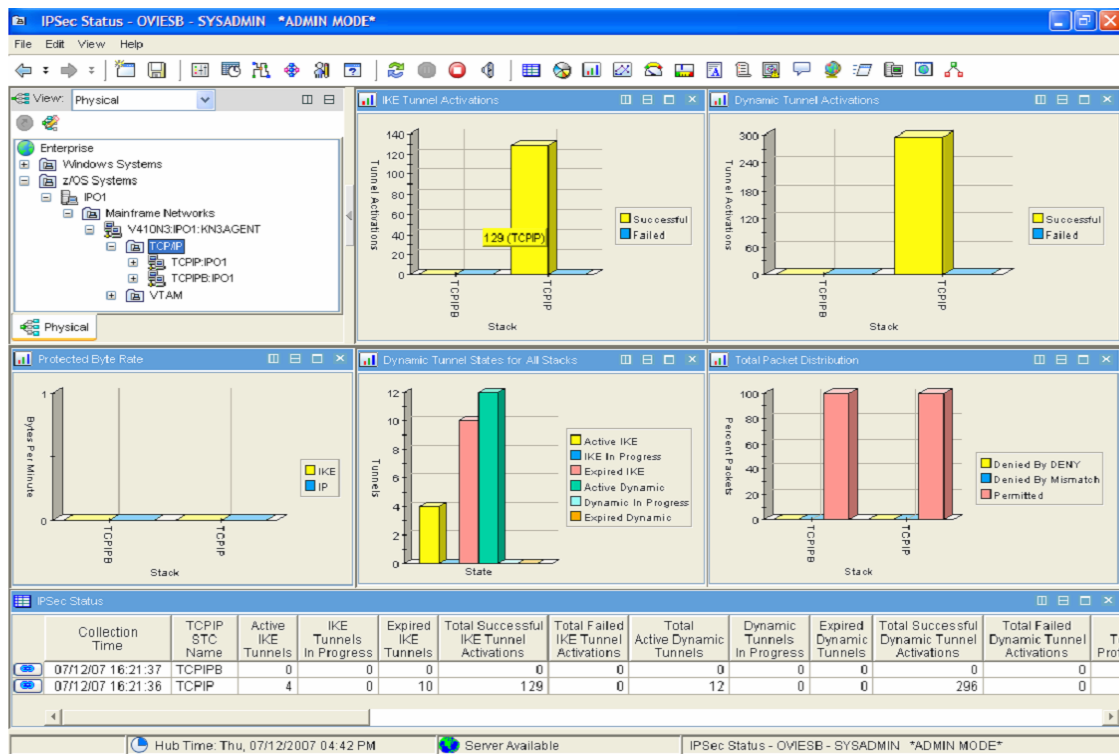
*(dynamic tunnels)*

*(manual tunnels)*



# IP Security Monitoring Application

- OMEGAMON XE for Mainframe Networks V4R1 APAR OA22263 and FP1 (4.1.0-TIV-ITM\_KN3-FP0001) add performance monitoring of z/OS IP security.



Provides graphical analysis of IP security activity for each TCP/IP stack  
 Monitors the use of IP filters and the performance of IPsec tunnels  
 Provides state and configuration information about filters and IPsec tunnels

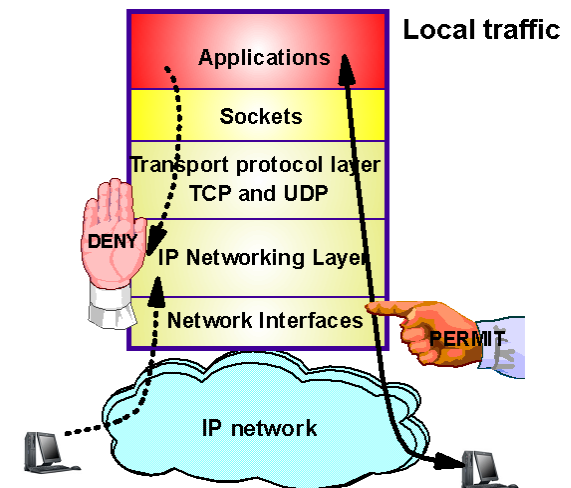
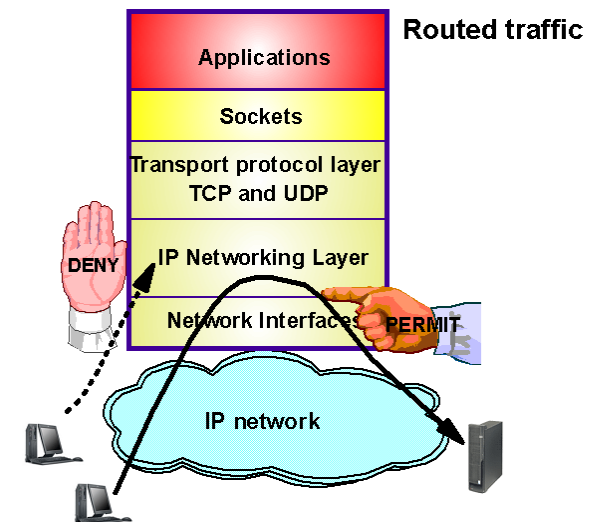
# Agenda

- Introduction
- IP Security Concepts and Terminology
- OMEGAMON XE for Mainframe Networks IP Security Monitor Application
  - ▶ Tivoli Management Services Common Features
  - ▶ OMEGAMON XE for Mainframe Networks
  - ▶ Common IP Security Problems
  - ▶ IP Security Status – The Dashboard
  - ▶ IP Security Situations and Thresholds
  - ▶ IP Security Historical Views
- **Sample Scenarios**
- **Description of IP Security Workspaces**
- Reference



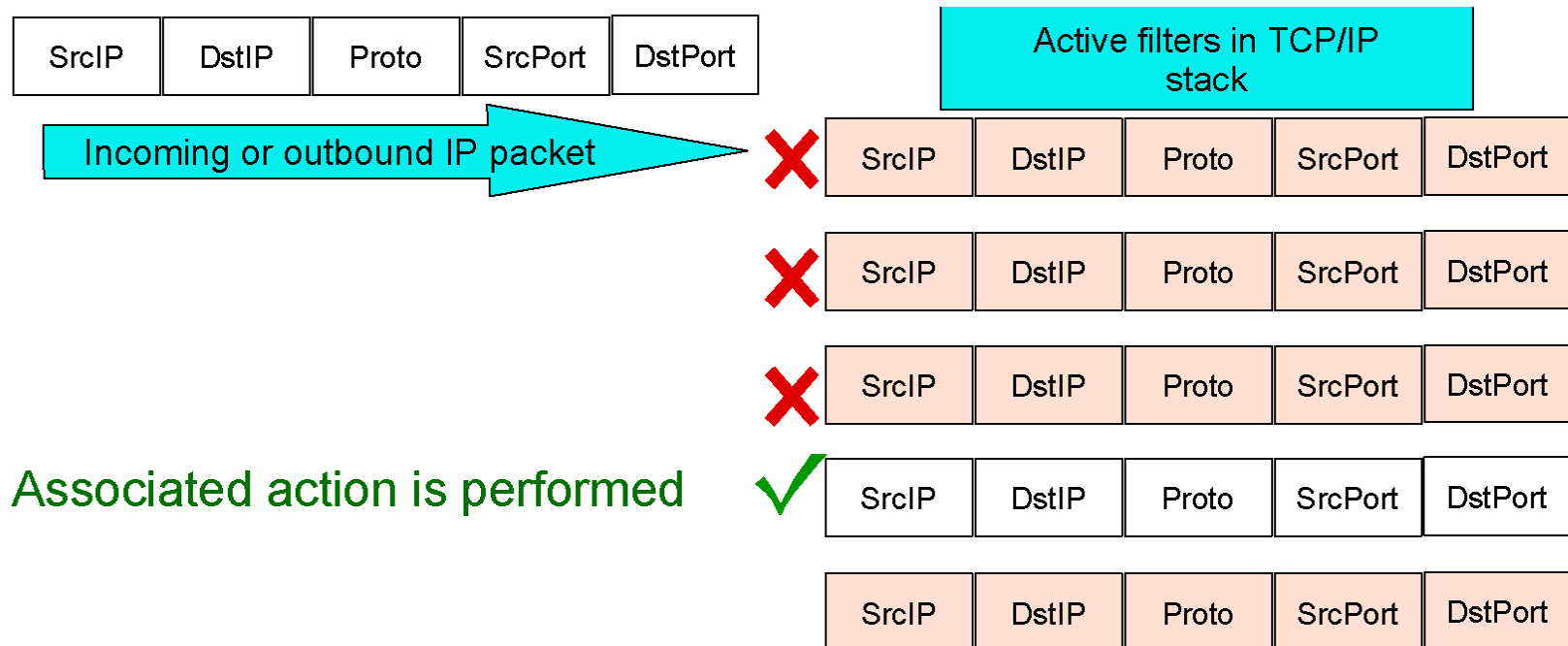
# Basics of IP Filtering

- Packet filtering at IP Layer
- Filter rules defined to match on inbound and outbound packets based on:
  - ▶ packet information
  - ▶ network attributes
  - ▶ time
- Used to control
  - ▶ traffic being routed
  - ▶ access at destination host
- Possible actions
  - ▶ Permit
  - ▶ Deny
  - ▶ Permit with manual IPsec
  - ▶ Permit with dynamic IPsec
  - ▶ Log (in combination with others)



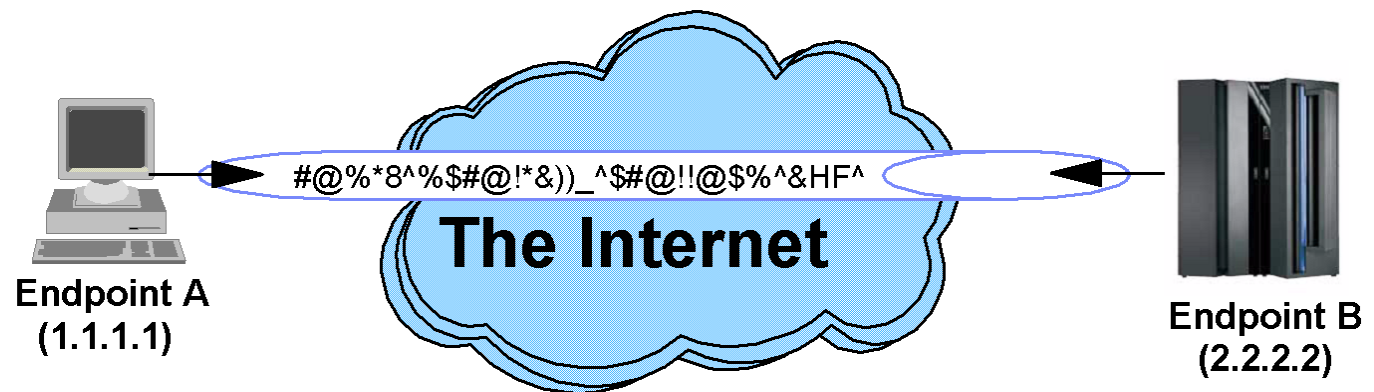
# Filter Matching

- Filters are searched in the order they were configured
- Each rule is inspected, from top to bottom, for a match
- If a match is found, the search ends and the action is performed

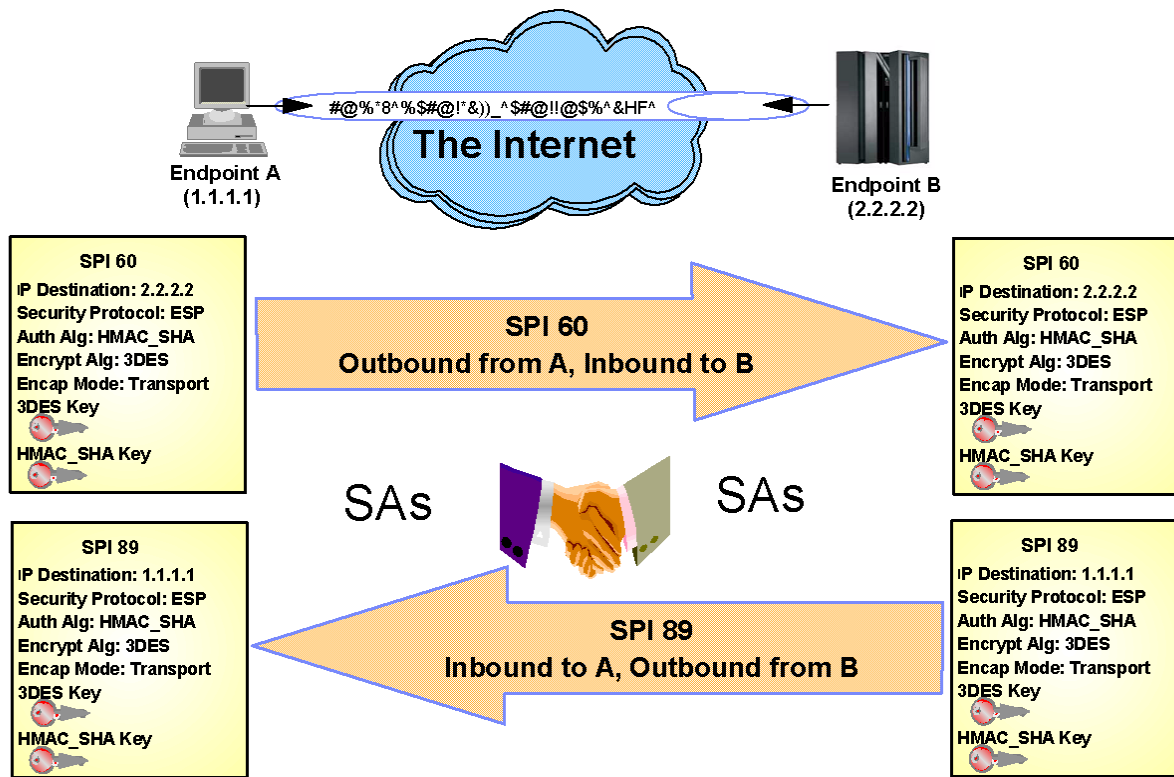


# Tunnels

- A tunnel is a secure logical connection used to protect traffic between two endpoints
- A tunnel is defined by a collection of security associations (SA)
- Tunnels are “installed” as a result of activating security associations



# Security Associations



- Security Association (SA) is agreement between endpoints as to how data is to be protected
  - ▶ IPsec protocol: AH or ESP
  - ▶ Algorithms to be used by security protocols
    - Encryption algorithm: DES, triple DES, or AES
    - Authentication algorithm: HMAC\_MD5 or HMAC\_SHA
  - ▶ Cryptographic keys
  - ▶ Encapsulation mode: tunnel or transport
  - ▶ Lifetime/Lifesize for dynamic SAs



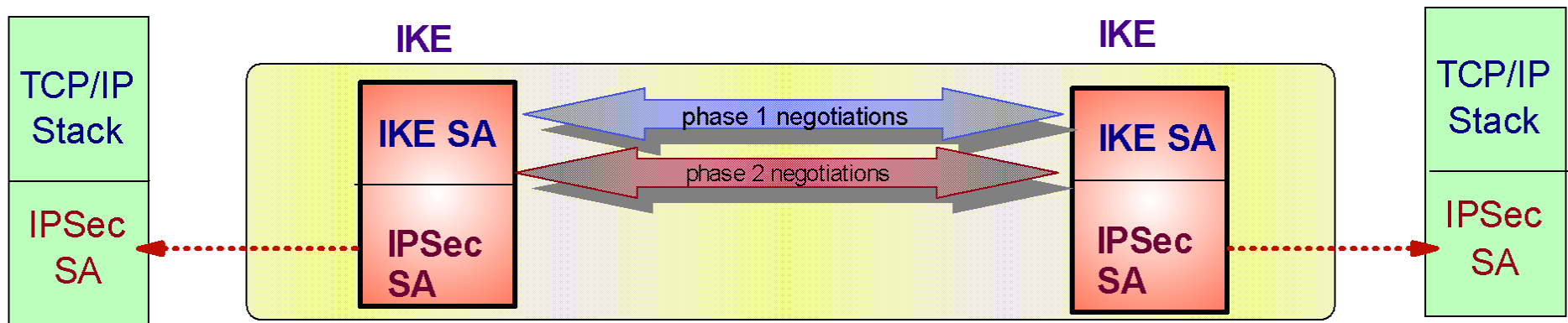
## Security Associations – Details

- SAs are associated with a direction of traffic (inbound or outbound)
- SAs are named and defined by VPN Action statements to the Policy Agent
  - ▶ IpManVpnAction
  - ▶ IpDynVpnAction
  - ▶ KeyExchangeAction
- SAs may be activated by a variety of methods
  - ▶ command line
  - ▶ Automatically
  - ▶ on-demand
  - ▶ remotely
- SAs are identified in security headers by the IP address of the remote endpoint and an SPI
- SPIs (Security Parameter Index) are used to find SAs in order to determine packet processing actions



# IKE Daemon

- Dynamic SAs are negotiated by IKE daemon using port 500 or 4500
- Two phased negotiation used
  - ▶ Phase 1 negotiates a secure channel (IKE SA (IKE Tunnel)) with a remote security endpoint
    - Generates cryptographic keys used during phase 2 and authenticates endpoints
    - Two modes: Main Mode and Aggressive Mode
  - ▶ Phase 2 uses IKE SA to negotiate an IPsec SA (Dynamic IP Tunnel)
    - Generates cryptographic keys used to protect data
    - Single mode: Quick Mode





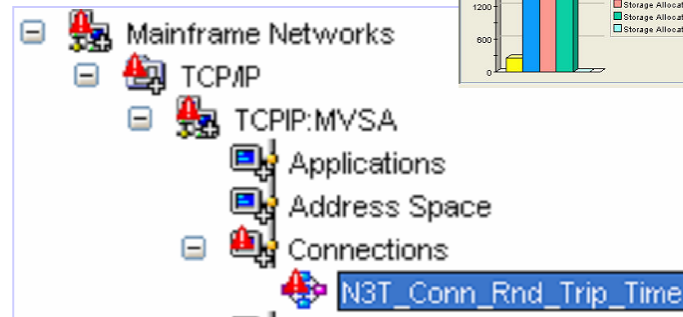
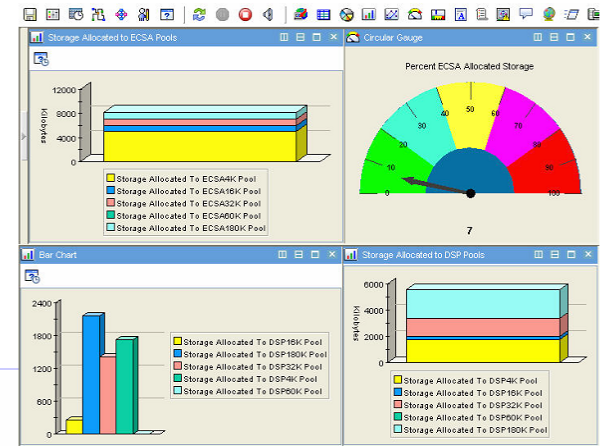
# Agenda

- Introduction
- IP Security Concepts and Terminology
- OMEGAMON XE for Mainframe Networks IP Security Monitoring Application
  - ▶ Tivoli Management Services Common Features
  - ▶ OMEGAMON XE for Mainframe Networks
  - ▶ Common IP Security Problems
  - ▶ IP Security Status – The Dashboard
  - ▶ IP Security Situations and Thresholds
  - ▶ IP Security Historical Views
- **Sample Scenarios**
- **Description of IP Security Workspaces**
- Reference



# Tivoli Enterprise Portal (TEP) Highlights

- Common, easy to use, interface
  - Integrates application monitoring
    - Navigation Tree
    - Dynamic Workspace Linking
  - Filter, sort
  - Display data in graphs, charts, tables
  - Display data in real time or from historical database
- Easy to Configure
  - Customize workspaces and reports
  - Define thresholds and generate events
- Out of the box best practices
  - Workspaces
  - Situations
  - Expert Advice



Out of the box situations to proactively notify you.

With so much data, how do you know what to look at?  
 • Highlight attributes of potential problems

Response Time	Origin Node	System ID
15.19	TCPIP:MVSA	MVSA
5.67	TCPIP:MVSA	MVSA
Response Time GE 5.00		

# Application Integration

z/OS Health check

***z/OS Management Console***

z/OS & USS

***OMEGAMON XE on z/OS***

NetView for z/OS

***IBM Tivoli NetView for z/OS V5.3***

Network

***OMEGAMON XE for Mainframe Networks***

DB2

***OMEGAMON XE for DB2 PE/PM***

CICS

***OMEGAMON XE for CICS***

IMS

***OMEGAMON XE for IMS***

Storage

***OMEGAMON XE for Storage***

WebSphere MQ

***OMEGAMON XE for Messaging***

WebSphere Appl Server

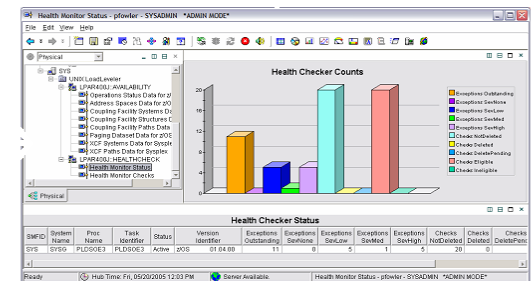
***ITCAM for WAS***

z/VM & Linux on z

***OMEGAMON XE on z/VM and Linux***

Distributed Monitoring

***IBM Tivoli Monitoring (ITM) & ITCAM***



**TEP**



# Situations

- What are they?
  - ▶ A situation describes a condition or set of conditions you want to examine to determine if a potential problem exists in the systems and resources you are monitoring.
  - ▶ When all of the conditions of a situation are met (the situation is triggered), an event is registered. The operator is alerted to events by indicator icons that appear in the Navigator. Operators can also be alerted by sound.
- Why use them?
  - ▶ Situations proactively monitor the performance of your system, allowing you to find and resolve problems before end users report them.
  - ▶ Situations can resolve problems automatically using Take Action (reflex automation).
  - ▶ Situations provide customized expert advice.



# Situation Triggered – Event Generated

The screenshot displays the Tivoli Enterprise Portal interface. On the left is a tree view of system components, including z/OS Management Console, MVSA, CICS, DB2, IMS, Mainframe Networks, and VTAM. The main window is titled 'Situation Event Console' and shows a table of 22 events. A modal dialog box is open, displaying a critical event: 'N3T\_Conn\_Rnd\_Trip\_Time' from source 'TCPIP:MVSA' on '05/09/06 21:07:22'. Below the dialog, a message reads 'KFVMTM1011 Select workspace link button to view situation event results.'

Status	Situation Name	Display Item	Source	Impact
Problem	Linux_Packets_Error		sles9094:LZ	Network
Problem	Linux_RPC_Bad_Calls		sles9094:LZ	Network
Problem	Linux_Process_High_Cpu		sles9094:LZ	Process
Problem	Linux_Packets_Error		sles9096:LZ	Linux for zSeries Net
Problem	Linux_RPC_Bad_Calls		sles9096:LZ	Linux for zSeries Net
Problem	Linux_Process_High_Cpu		sles9096:LZ	Process
Open	NT_Log_Space_Low	Security	Primary:HQDNT2:NT	System
Open	NT_Log_Space_Low	Application	Primary:HQDNT2:NT	System
Open	IMS_MQ_Connection_Status		IMSA:MVSA:IMS	IMS MQSeries Status
Open	IMS_MQ_Connection_Status		IMST:MVSA:IMS	IMS MQSeries Status
Open	N3T_CPU_Pct_Warning		TCPIP:MVSA	Address Space
Open	KHL_AddressSpace_Waiting		DEMOPLX:MVSA:AVAILABILITY	Address Space Data
Problem	Linux_High_Packet_Collisions		sles9094:LZ	Network
Problem	Linux_Process_stopped		sles9094:LZ	Process
Problem	Linux_System_Thrashing		sles9094:LZ	System Information
Problem	Linux_High_Packet_Collisions		sles9096:LZ	Linux for zSeries Net
Problem	Linux_Process_stopped		sles9096:LZ	Process
Problem	Linux_System_Thrashing		sles9096:LZ	System Information
Open	N3T_Conn_Rnd_Trip_Time		TCPIP:MVSA	Connections
Open	MQSeries_MQ_Channel_Stopped		WMQA:MVSA:MGESA	MQSeries Events
Open	DNET556_Disk_High_RespTime		CXEGA01:MVSA:STORAGE	Storage Subsystem
Open	KHL_High_Severity_Check		DEMOPLX:MVSA:HEALTHCHECK	Health Monitor Check

# Situation Workspace, Take Action and Expert Advice

- Shows attribute values at the time the situation triggered
- If situation is still true, shows current attribute values
- Highlights threshold triggering situation
- Provides customizable expert advice
- Provides ability to issue command enabling automation

The screenshot displays the IBM Security Manager interface for a situation named 'N3T\_IPSec\_Pkts\_Denied\_DENY'. The interface is divided into several panels:

- Physical View:** A tree view on the left showing the network configuration hierarchy, with 'N3T\_IPSec\_Pkts\_De' selected under 'IP Filters'.
- Initial Situation Values:** A table showing the state of the situation when it first occurred.
 

Percent Packets Denied By DENY	Origin Node	Sysplex Name	System ID	TCPIP STC Name	Collection Time	Active IKE Tunnels	IKE Tunnels In Progress	Expired IKE Tunnels	Total 8 Local I Acti
6	TCPIP:IP03	PLEX1	IP03	TCPIP	02/22/08 12:33:22	4	0	8	
- Current Situation Values:** A table showing the current state of the situation.
 

Percent Packets Denied By DENY	Origin Node	Sysplex Name	System ID	TCPIP STC Name	Collection Time	Active IKE Tunnels	IKE Tunnels In Progress	Expired IKE Tunnels	Total 8 Local I Acti
6	TCPIP:IP03	PLEX1	IP03	TCPIP	02/22/08 12:33:22	4	0	8	
- Take Action:** A panel for issuing commands. It includes a dropdown menu for 'Action Name' (currently set to '<Select Action>'), a text field for 'Command', and a 'Run' button.
- Expert Advice:** A panel providing guidance for the situation.
 

**N3T\_IPSec\_Pkts\_Denied\_DENY**

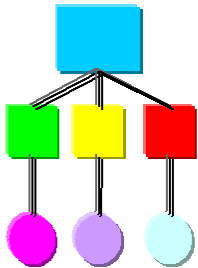
**Situation Description**  
The number of packets being denied by the DENY action associated with one or more filters may be high.

**Suggested Actions**  
This situation could indicate attempted suspicious activity. Enable logging for the filters with DENY actions and monitor the traffic using the UNIX sysloa.

The status bar at the bottom indicates the Hub Time as 'Wed, 02/27/2008 09:46 AM' and the Server as 'Available'.

# Mainframe Networks Components

One or more protocols including SNA, IP or both

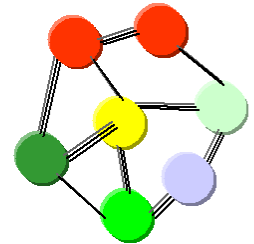


## SNA

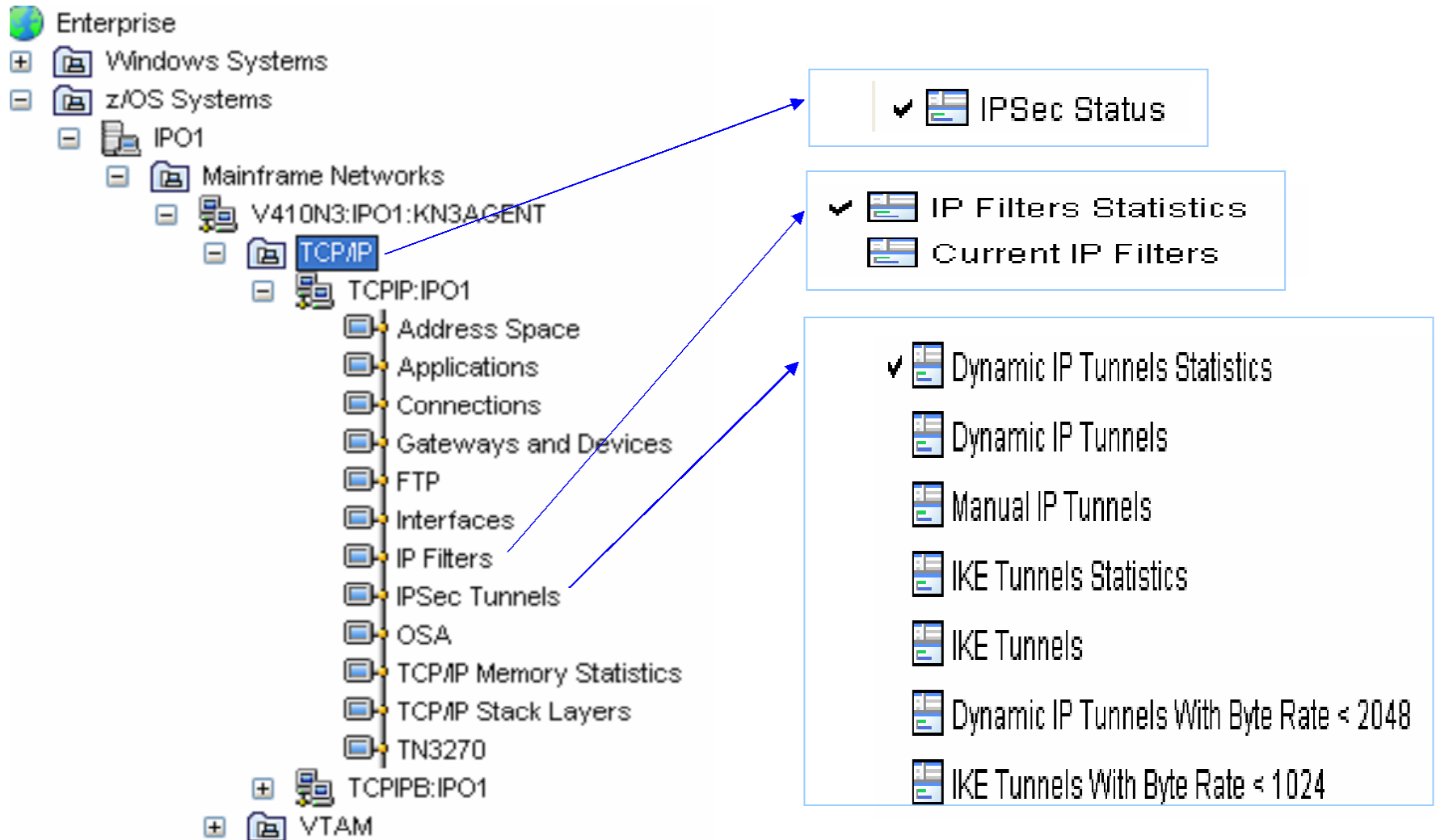
- Hierarchal (Subarea)
- Generic Alerts
- VR Flow Control
- HPR
- SNI
- Intelligent agents
- LUs and PUs
- Sessions Controlled
- 3745 ( CCL)

## TCP/IP

- Peer to Peer
- Traps
- Discards, retransmits
- Enterprise Extender
- Internet
- IP Security
- MIB Polling
- TN3270
- FTP
- OSA-Express, Cisco CIP
- Denial of Service Attack



# IP Security Workspaces in Mainframe Networks





## Some Common IP Security Problems and Symptoms

- Filter added in wrong order
  - ▶ Loss of connectivity to applications
- Security policies at endpoints are incompatible
  - ▶ Loss of connectivity to applications
  - ▶ Tunnel activation failures
- Loss of network connectivity between security endpoints
  - ▶ Loss of connectivity to applications
  - ▶ Tunnel activation failures
- Cryptographic services unavailable, misconfigured, or insufficient
  - ▶ Application performance is slow
  - ▶ Loss of connectivity to applications
  - ▶ Tunnel activation failures

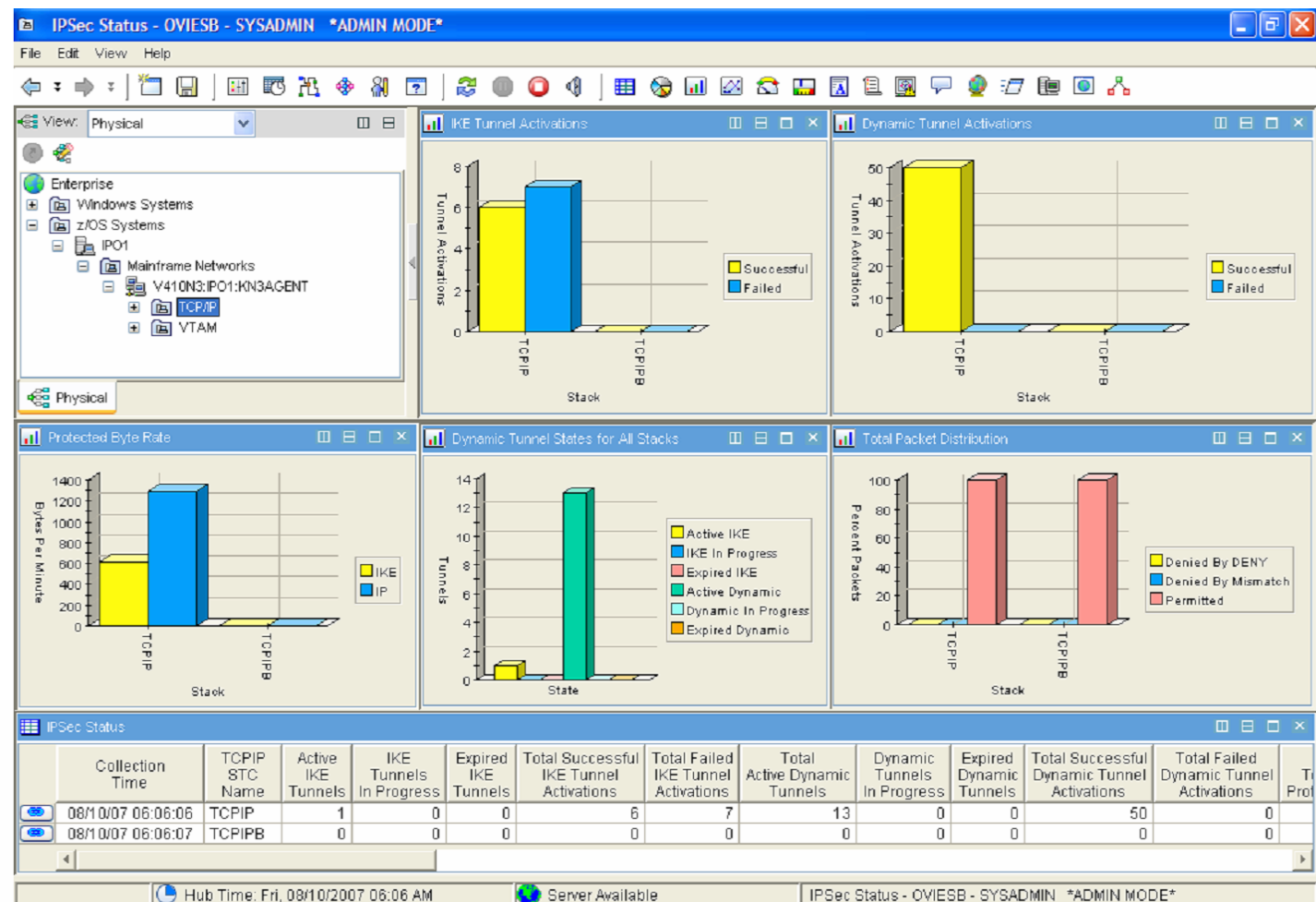


# IPSec Status Workspace – The Dashboard

- Tunnel activation statistics
- Tunnel throughput statistics
- Tunnel state analysis
- Packet permit, deny and mismatch statistics



## Links

- [Dynamic IP Tunnels Statistics](#)
- [IKE Tunnels Statistics](#)
- [IP Filters Statistics](#)



# IP Security Situations and Thresholds

## Filters Situations

-  N3T\_IPSec\_Pkts\_Denied\_DENY
-  N3T\_IPSec\_Pkts\_Denied\_Mismatch

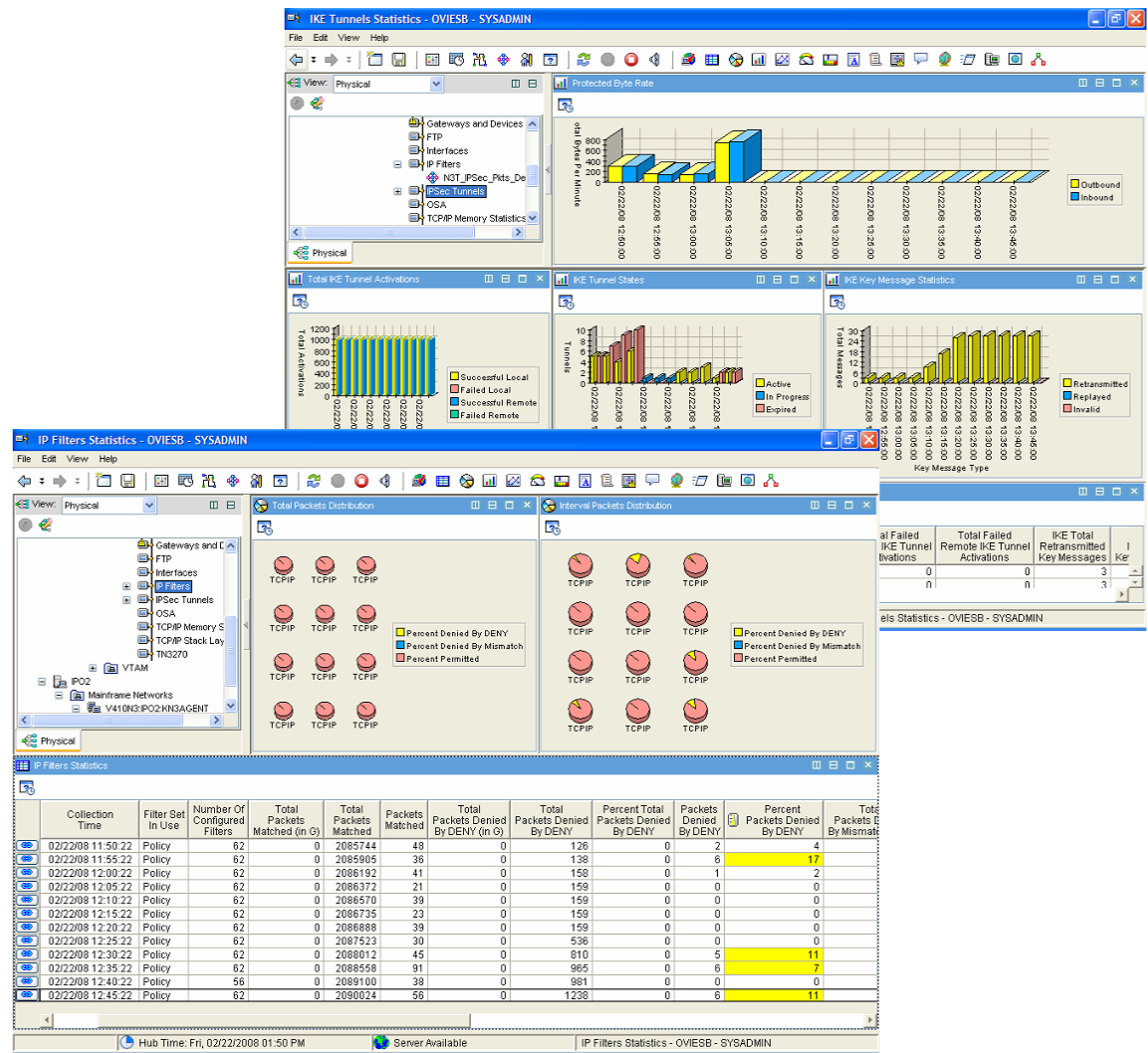
## IPSec Tunnels Situations

-  N3T\_IPSec\_Dyn\_Act\_Fail
-  N3T\_IPSec\_Dyn\_Act\_Fail\_IKE\_Tnl
-  N3T\_IPSec\_Dyn\_Act\_Fail\_IKE\_TnR
-  N3T\_IPSec\_IKE\_Act\_Fail
-  N3T\_IPSec\_Key\_Msgs\_Auth\_Fail
-  N3T\_IPSec\_Key\_Msgs\_Invalid
-  N3T\_IPSec\_Key\_Msgs\_Replayed
-  N3T\_IPSec\_Key\_Msgs\_Rtrnsmttd
-  N3T\_IPSec\_QUICKMODE\_Invalid
-  N3T\_IPSec\_QUICKMODE\_Replayed
-  N3T\_IPSec\_QUICKMODE\_Rtrnsmttd



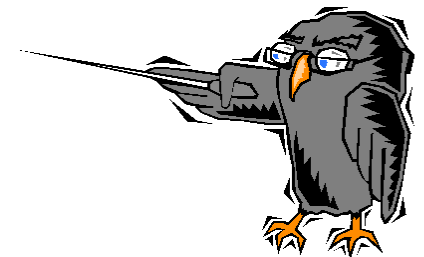
# IP Security Historical Views

- Trend analysis
  - Do I need more zIIP processors?
  - Do I need more cryptography processors?
- Workspaces enabled for historical data display
  - IPsec Status
  - IP Filters Statistics
  - Dynamic IP Tunnels Statistics
  - IKE Tunnels Statistics



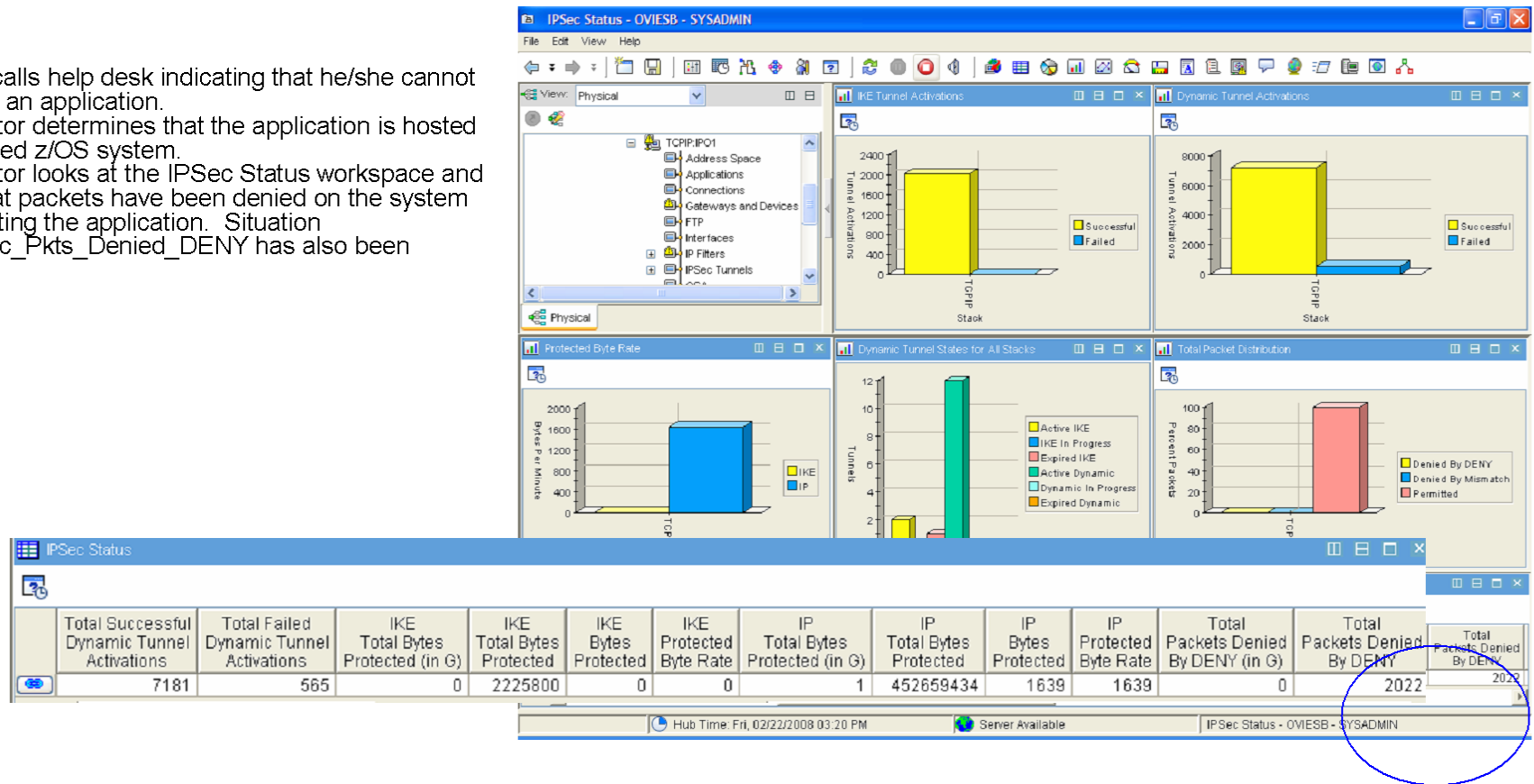
# Agenda

- Introduction
- IP Security Concepts and Terminology
- OMEGAMON XE for Mainframe Networks IP Security Monitoring Application
  - ▶ Tivoli Management Services Common Features
  - ▶ OMEGAMON XE for Mainframe Networks
  - ▶ Common IP Security Problems
  - ▶ IP Security Status – The Dashboard
  - ▶ IP Security Situations and Thresholds
  - ▶ IP Security Historical Views
- **Sample Scenarios**
- **Description of IP Security Workspaces**
- Reference



# Scenario 1: Application unavailable due to filter rule out of order

- End user calls help desk indicating that he/she cannot connect to an application.
- The operator determines that the application is hosted on a secured z/OS system.
- The operator looks at the IPsec Status workspace and notices that packets have been denied on the system that is hosting the application. Situation N3T\_IPSec\_Pkts\_Denied\_DENY has also been triggered.

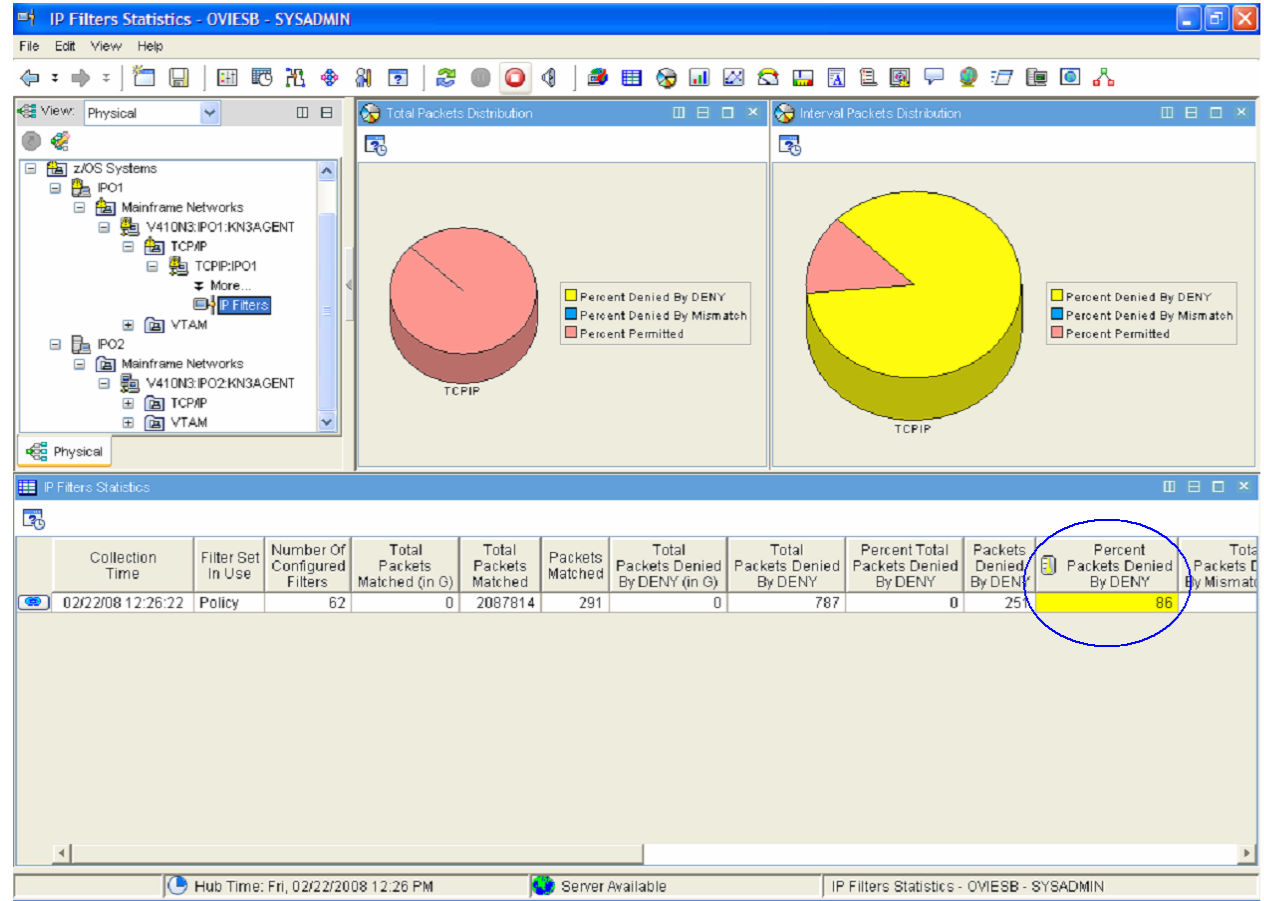


**WARNING**

N3T\_IPSec\_Pkts\_Denied\_DENY TCPIP:IPO1 02/22/08 15:20:49

# Scenario 1: Application unavailable due to filter rule out of order (cont)

- The operator navigates to the IP Filters Statistics workspace for the stack that has denied packets. He/She notices that 86% of the packets processed by the stack in the last collection interval were denied.



## Scenario 1: Application unavailable due to filter rule out of order (cont)

- The operator navigates to the situation event view and sees that a high percentage of the packets processed during each collection interval is being denied. He/She reads the situation description and suggested actions.

The screenshot shows the IBM Tivoli NetView interface. The top window displays a tree view of network components, including z/OS Systems, Mainframe Networks, and IP Filters. The 'N3T\_IPSec\_Pkts\_Denied\_DENY' situation is selected. Below the tree view, two tables show situation values:

Initial Situation Values										
Percent Packets Denied By DENY	Origin Node	Sysplex Name	System ID	TCPIP STC Name	Collection Time	Active IKE Tunnels	IKE Tunnels In Progress	Expired IKE Tunnels	Total S Local I	Acti
91	TCPIP:IP01	PLEX1	IP01	TCPIP	02/22/08 12:44:22	5	0	4		

Current Situation Values										
Percent Packets Denied By DENY	Origin Node	Sysplex Name	System ID	TCPIP STC Name	Collection Time	Active IKE Tunnels	IKE Tunnels In Progress	Expired IKE Tunnels	Total S Local I	Acti
16	TCPIP:IP01	PLEX1	IP01	TCPIP	02/22/08 12:46:22	4	0	5		

The bottom window shows the 'Expert Advice' for the situation 'N3T\_IPSec\_Pkts\_Denied\_DENY'. It includes a 'Situation Description' and 'Suggested Actions'.

**Expert Advice**

**N3T\_IPSec\_Pkts\_Denied\_DENY**

[Situation Description](#)  
[Suggested Actions](#)

**Situation Description**

The number of packets being denied by the DENY action associated with one or more filters may be high.

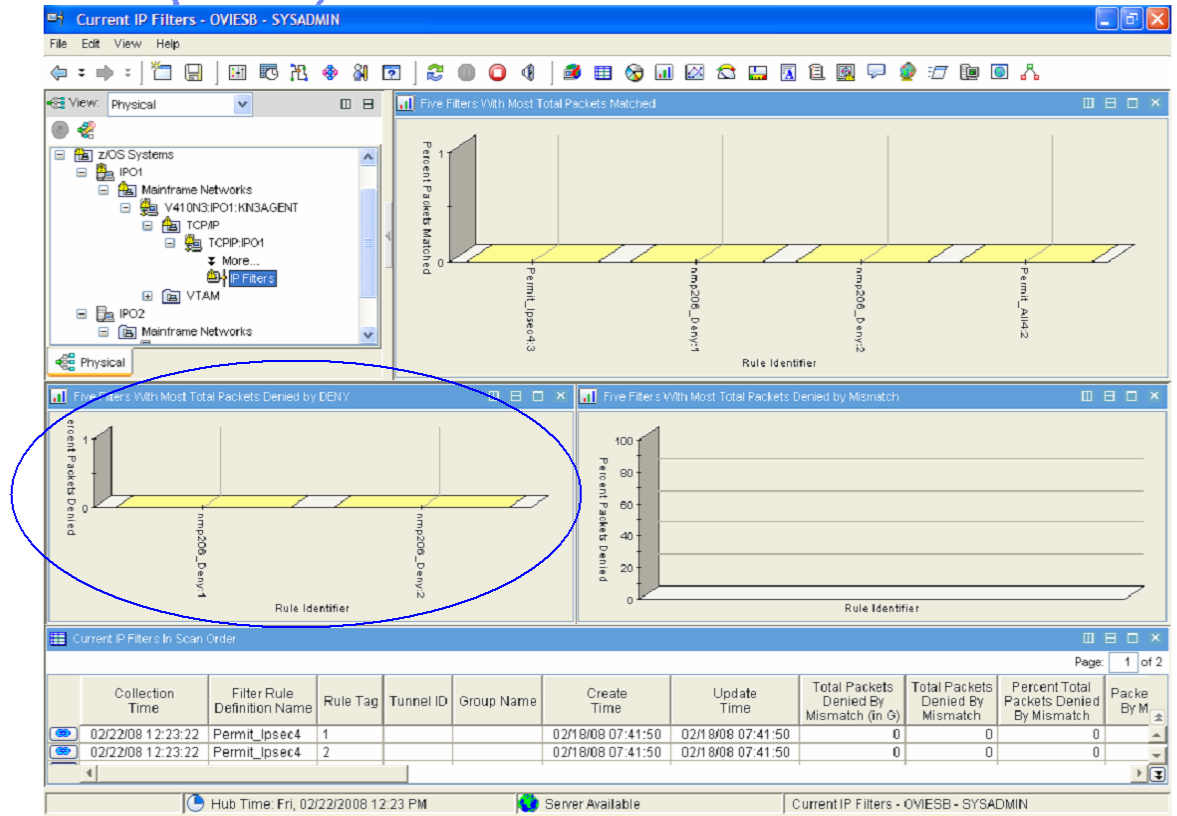
**Suggested Actions**

This situation could indicate attempted suspicious activity. Enable logging for the filters with DENY actions and monitor the traffic using the UNIX svslod.



# Scenario 1: Application unavailable due to filter rule out of order (cont)

- The operator navigates to the Current IP Filters workspace and sees that 2 filter rules are identified as having denied packets.



# Scenario 1: Application unavailable due to filter rule out of order (cont)

- He/She contacts the systems programmer.
- The systems programmer locates the filter rules denying packets in the table view.
- The create time for the filters denying packets is fairly recent.
- The destination address for traffic matching these filters matches the IP address of the system hosting the failing application.

	02/22/08 12:27:22	nmp114206_Tunnel_v6	1	YO		02/18/08 07:41:50	02/18/08 07:41:50
	02/22/08 12:27:22	nmp114206_Tunnel_v6	2	YO		02/18/08 07:41:50	02/18/08 07:41:50
	02/22/08 12:27:22	nmp206_Deny	1			02/22/08 11:47:54	02/22/08 11:47:54
	02/22/08 12:27:22	nmp206_Deny	2			02/22/08 11:47:54	02/22/08 11:47:54
	02/22/08 12:27:22	nmp206_Deny	3			02/22/08 11:47:54	02/22/08 11:47:54
	02/22/08 12:27:22	nmp206_Deny	4			02/22/08 11:47:54	02/22/08 11:47:54
	02/22/08 12:27:22	nmp206_Deny	5			02/22/08 11:47:54	02/22/08 11:47:54
	02/22/08 12:27:22	nmp206_Deny	6			02/22/08 11:47:54	02/22/08 11:47:54
	02/22/08 12:27:22	nmp206_Tunnel	1	YO		02/18/08 07:41:50	02/22/08 07:57:53

Src	Src	Src	Src	Src	Src	Src	Src
9:0:1:1::	9:0:1:1::fff	0	0	9::	9::	0	0
9.42.0.0	9.42.255.255	0	0	9.42.45.0	9.42.45.255	0	0
9.42.45.0	9.42.45.255	0	0	9.42.0.0	9.42.255.255	0	0
9.42.0.0	9.42.255.255	0	0	9.42.32.0	9.42.32.255	0	0
9.42.32.0	9.42.32.255	0	0	9.42.0.0	9.42.255.255	0	0
9.42.0.0	9.42.255.255	0	0	9.42.62.0	9.42.62.255	0	0
9.42.62.0	9.42.62.255	0	0	9.42.0.0	9.42.255.255	0	0
9.42.45.0	9.42.45.255	0	0	9.42.45.0	9.42.45.255	0	0
9.42.45.206		21	21	9.42.45.114		1605	1605
9.42.45.206		3446	3446	9.42.45.114		21	21

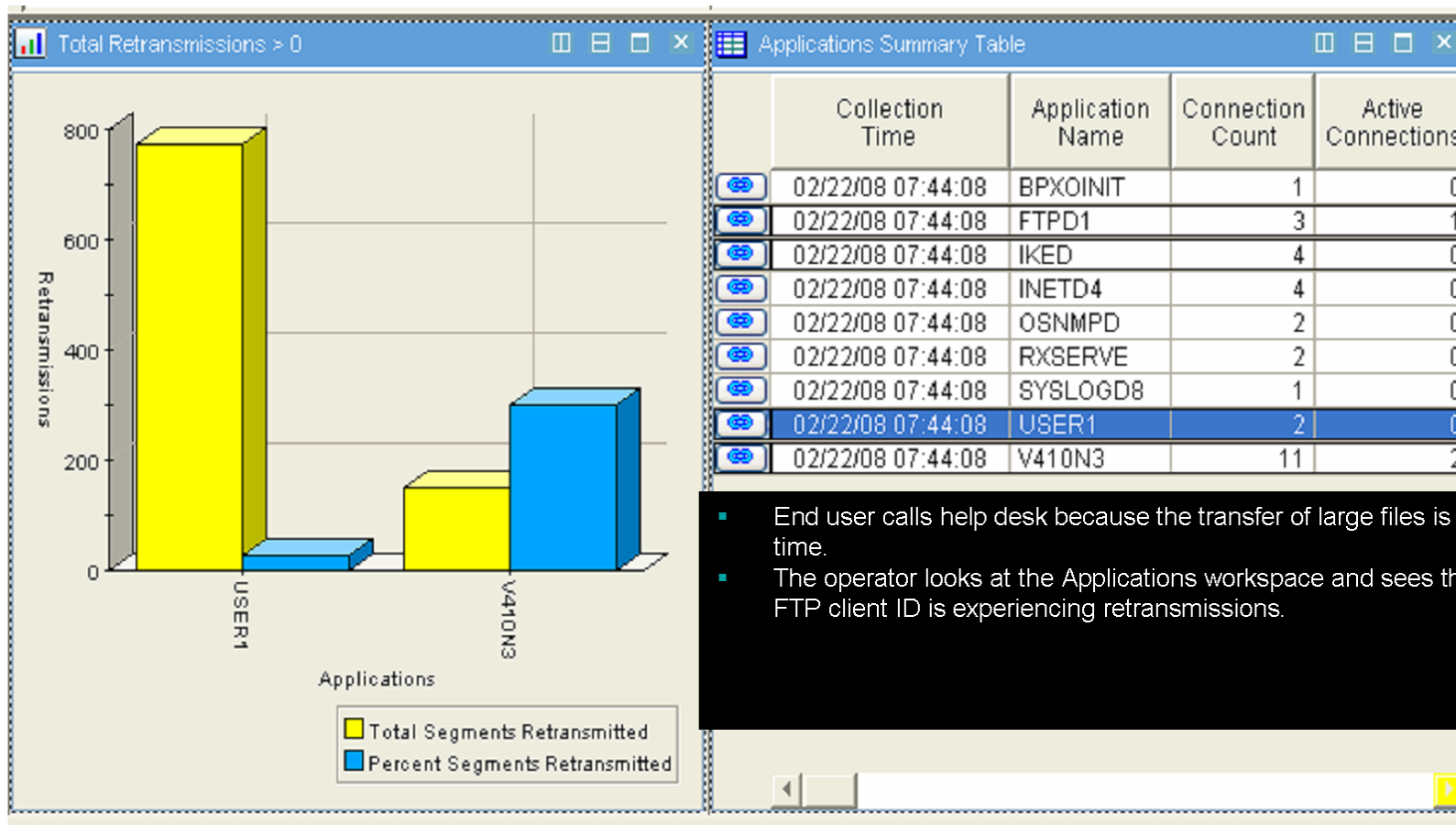


## Scenario 1: Application unavailable due to filter rule out of order *(cont)*

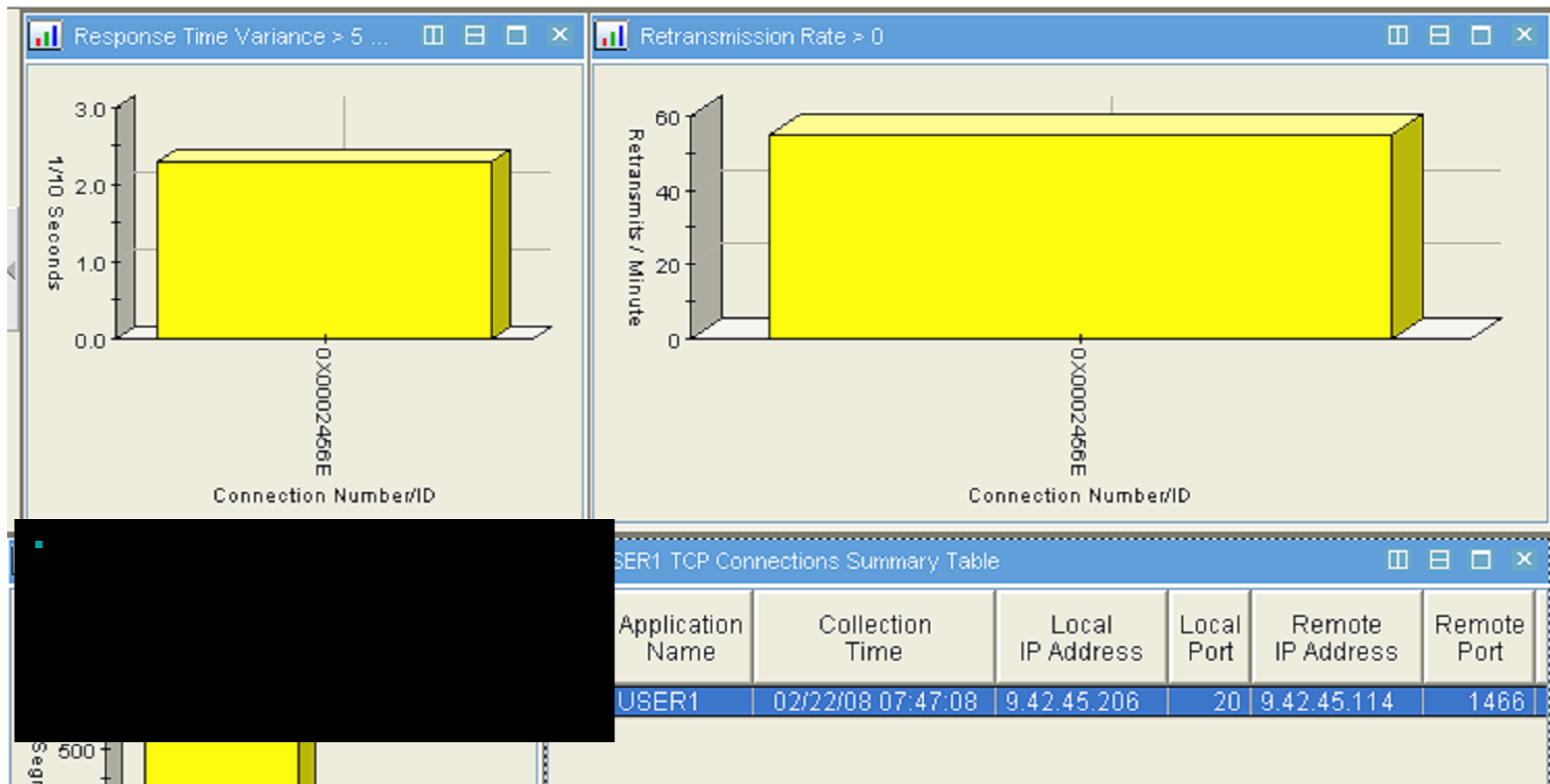
- The systems programmer examines the filter traffic descriptor information and the position of the filter relative to the other filters. He/She determines that the filter was added at the incorrect position in the filter policy.
- The systems programmer corrects the filter policy and the end user is now able to connect to the secured application.



## Scenario 2: Application performance problem due to short refresh time

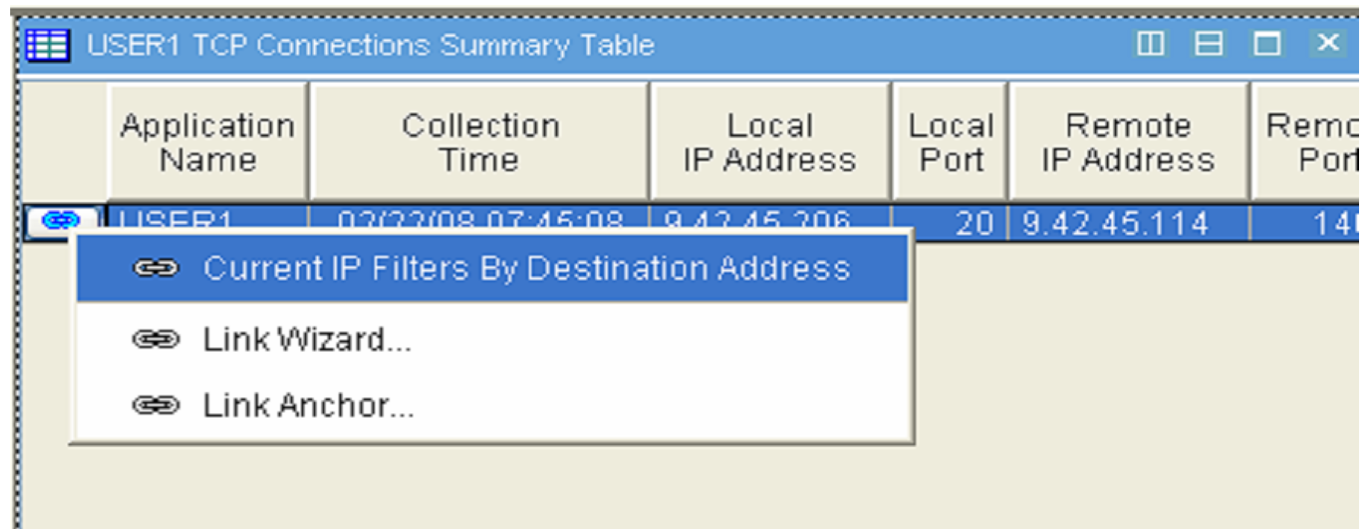


## Scenario 2: Application performance problem due to short refresh time (*cont*)



## Scenario 2: Application performance problem due to short refresh time *(cont)*

- The operator contacts the systems programmer.
- The systems programmer notices that the client and server involved in the transfer are on secured z/OS systems.
- The systems programmer navigates to the Current IP Filters By Destination Address workspace using the link available from the Application TCP Connections workspace.



Application Name	Collection Time	Local IP Address	Local Port	Remote IP Address	Remote Port
USER1	02/22/08 07:45:08	9.42.45.206	20	9.42.45.114	14

Context menu options:

- Current IP Filters By Destination Address
- Link Wizard...
- Link Anchor...

## Scenario 2: Application performance problem due to short refresh time (cont)

- The systems programmer locates a dynamic IP filter that matches the source and destination IP addresses associated with the file transfer and navigates to the dynamic IP tunnels workspace to display the associated dynamic IP tunnels.

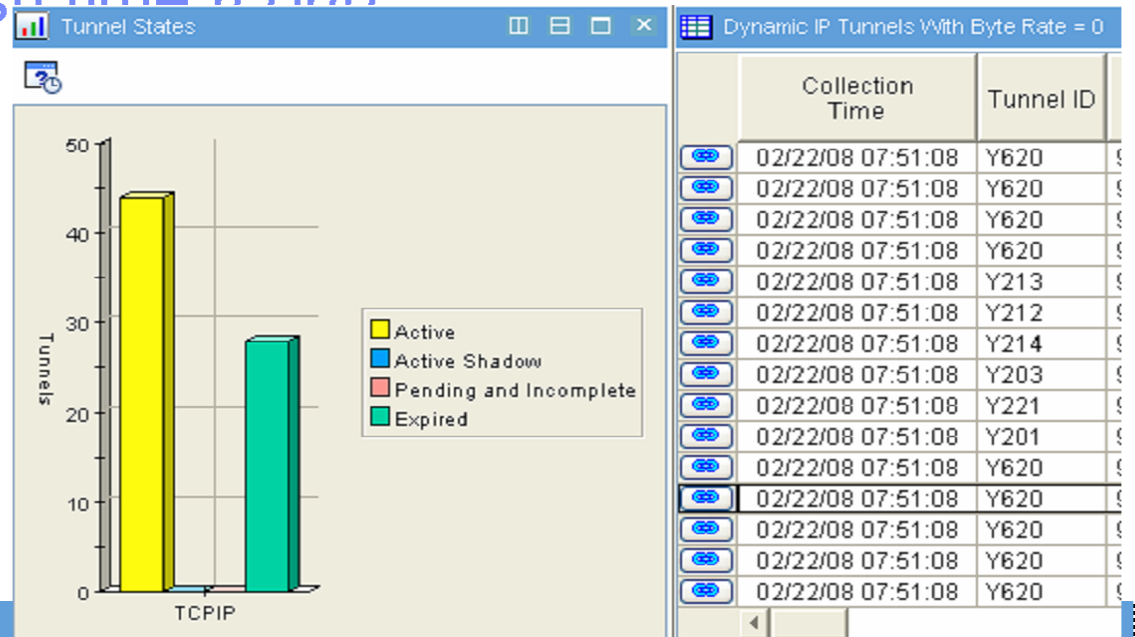
Current IP Filters By Destination Address				
	Collection Time	Filter Rule Definition Name	Rule Tag	Tunnel ID
	02/22/08 07:49:08	nmp206_Tunnel	1	Y0
	02/22/08 07:49:08	nmp206_Tunnel	1	Y620
	02/22/08 07:49:08	nmp206_Tunnel	1	Y619
	02/22/08 07:49:08	nmp206_Tunnel	1	Y618

'SA dow :ator	Source Address	Upper Source Address	Lower Source Port	Upper Source Port	Destination Address	Upper Destination Address	Lower Destination Port	Upper Destination Port
	9.42.45.0	9.42.45.255	0	0	9.42.45.0	9.42.45.2...	0	0
	ADOW	9.42.45.206		20	20	9.42.45.1...	1466	1466
	Current IP Filters By Destination Address				9.42.45.1...		1465	1465
	Dynamic IP Tunnels By Tunnel ID				9.42.45.1...		1463	1463



# Scenario 2: Application performance problem due to short refresh time (cont)

- The systems programmer notices that there is a high number of expired tunnels.
- The tunnel associated with the user's transfer has data rates of 0 and there are many tunnels with the same tunnel ID indicating it has been refreshed many times.



Tunnel ID	Local Security Endpoint	Remote Security Endpoint	Total Inbound Packets (in G)	Total Inbound Packets	Total Outbound Packets (in G)	Total Outbound Packets	Total Packets (in G)	Total Packets	Inbound Packets	Outbound Packets	Packets	Packet Rate
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0
Y620	9.42.45.206	9.42.45.114	0	0	0	0	0	0	0	0	0	0

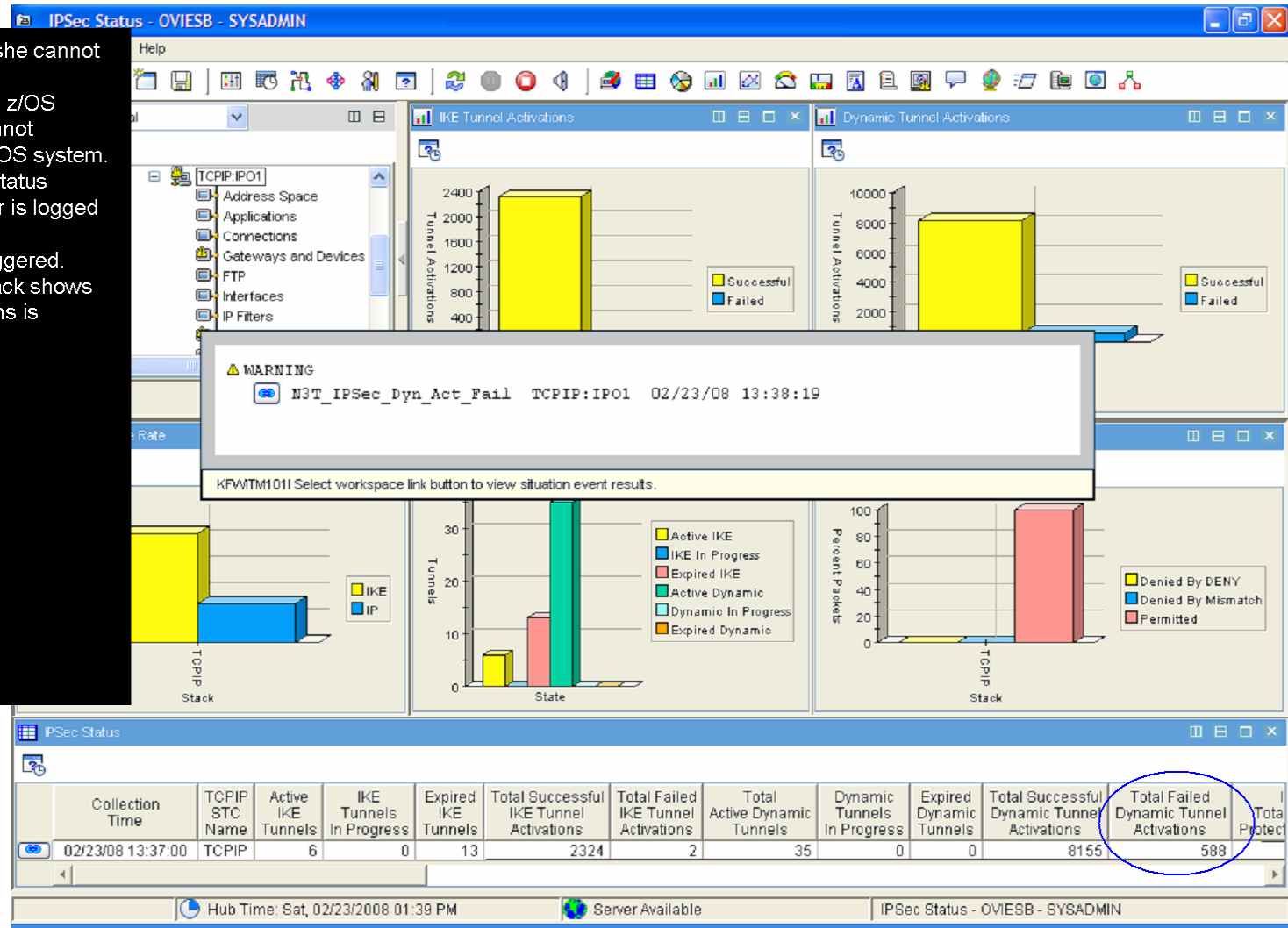


## Scenario 2: Application performance problem due to short refresh time (cont)

- The systems programmer examines the tunnel refresh and expiration information.
- Looking down the Life Expiration Time column and the Life Refresh Time column, he/she sees that the tunnel is being refreshed every 2 to 10 seconds.
- The systems programmer corrects the refresh time for the tunnel and fixes the performance problem.

Dynamic IP Tunnels By Tunnel ID							
ID	Current Life Size	Life Size	Refresh Life Size	Life Expiration Time	Life Refresh Time	VPN Life Expiration Time	Activation Method
	0	32768	26892	02/22/08 07:52:08	02/22/08 07:51:58	02/23/08 07:44:13	ONDEMAND
	0	32768	24982	02/22/08 07:52:06	02/22/08 07:51:52	02/23/08 07:44:13	ONDEMAND
	0	32768	26249	02/22/08 07:52:05	02/22/08 07:51:54	02/23/08 07:44:13	ONDEMAND
	0	32768	26810	02/22/08 07:52:04	02/22/08 07:51:54	02/23/08 07:44:13	ONDEMAND
	0	32768	26125	02/22/08 07:52:02	02/22/08 07:51:50	02/23/08 07:44:13	ONDEMAND
	0	32768	27834	02/22/08 07:52:01	02/22/08 07:51:52	02/23/08 07:44:13	ONDEMAND
	0	32768	23507	02/22/08 07:51:59	02/22/08 07:51:43	02/23/08 07:44:13	ONDEMAND
	0	32768	24314	02/22/08 07:51:58	02/22/08 07:51:43	02/23/08 07:44:13	ONDEMAND
	0	32768	27770	02/22/08 07:51:56	02/22/08 07:51:47	02/23/08 07:44:13	ONDEMAND
	0	32768	25679	02/22/08 07:51:54	02/22/08 07:51:42	02/23/08 07:44:13	ONDEMAND
	0	32768	26865	02/22/08 07:51:52	02/22/08 07:51:42	02/23/08 07:44:13	ONDEMAND
	0	32768	27671	02/22/08 07:51:51	02/22/08 07:51:42	02/23/08 07:44:13	ONDEMAND

- User calls help desk because he/she cannot connect to an application.
- The user is logged in to a secured z/OS system and the application he cannot connect to is also on a secured z/OS system.
- The operator looks at the IPsec Status workspace for the system the user is logged in to and sees that situation N3T\_IPSec\_Dyn\_Act\_Fail has triggered.
- Looking at the statistics for the stack shows that the number of failed activations is increasing.



## Scenario 3: Application unavailable due to mismatched encryption algorithm at endpoints (cont)

- The operator looks at the situation event workspace for more information about the event.
- He/She contacts the systems programmer for assistance.

The screenshot displays the IBM Tivoli Monitoring console. The top window, titled 'Initial Situation Values', contains a table with the following data:

Origin Node	Sysplex Name	System ID	TCPIP STC Name	Collection Time	Active IKE Tunnels	IKE Tunnels In Progress	Expired IKE Tunnels	Total Successful Local IKE Tunnel Activations	Total Successful Remote IKE Tunnel Activations
TCPIP:IP01	PLEX1	IP01	TCPIP	02/23/08 13:38:00	6	0	13	1163	

The bottom window, titled 'Current Situation Values', shows an 'Expert Advice' panel for the event 'N3T\_IPSec\_Dyn\_Act\_Fail'. The panel includes the following information:

- Situation Description:** Dynamic IP tunnel activations have failed.
- Suggested Actions:** Evaluate the IKE daemon logs to understand the nature of the failures. Failures could be due to either a configuration mismatch where one of the peers is rejecting the other peer's proposals or a network problem such as retransmissions.

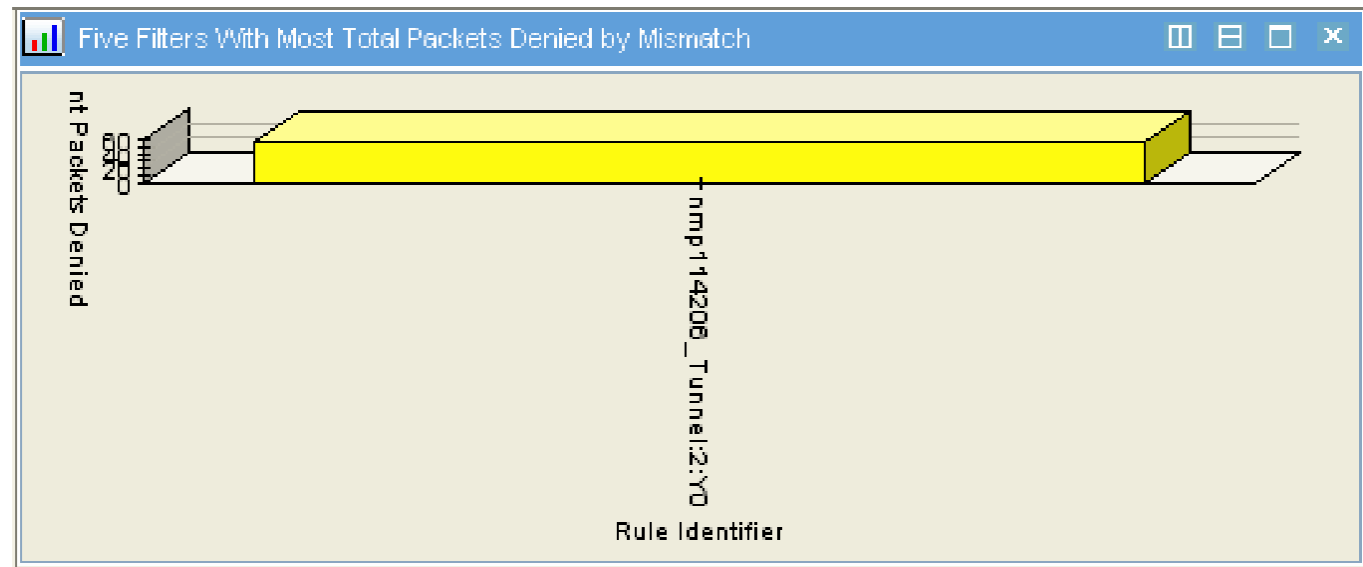
## Scenario 3: Application unavailable due to mismatched encryption algorithm at endpoints *(cont)*

- The systems programmer looks at /tmp/syslogd/debug.log and sees the error messages below
  - ▶ ZD1093I Policy mismatch : IpDataOffer (1) requires parameter (HowToEncrypt) with value (AES) but proposal (1) value is (DES)
  - ▶ ZD1022I No proposal chosen with IpFilterRule (nmp114206\_Tunnel) and IpDynVpnAction (DynAction3)



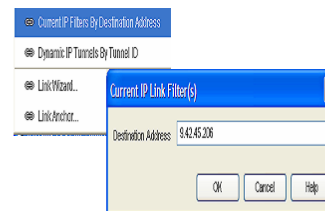
## Scenario 3: Application unavailable due to mismatched encryption algorithm at endpoints (*cont*)

- The systems programmer looks at the Current IP Filters workspace of the system hosting the application.
- He/She sees that some packets have been denied due to policy mismatch.



## Scenario 3: Application unavailable due to mismatched encryption algorithm at endpoints (*cont*)

- The systems programmer displays the filters that may match traffic from the user's system by using the link to Current IP Filters By Destination Address and specifying the IP address of the user's system.



## Scenario 3: Application unavailable due to mismatched encryption algorithm at endpoints (cont)

- He/She sees that two of the filters that would match traffic from the user's system were recently updated.
- The systems programmer corrects the encryption algorithm specification for the data offer referenced by VPN Action DynAction3 and corrects the problem.

	02/23/08 14:00:45	Permit_OSPF6	1			02/21/08 15:06:44	02/21/08 15:06:44
	02/23/08 14:00:45	Permit_OSPF6	2			02/21/08 15:06:44	02/21/08 15:06:44
	02/23/08 14:00:45	nmp114206_Tunnel	1	Y0		02/21/08 15:06:44	02/23/08 13:34:45
	02/23/08 14:00:45	nmp114206_Tunnel	2	Y0		02/21/08 15:06:44	02/23/08 13:34:45
	02/23/08 14:00:45	nmp114206_Tunnel_v6	1	Y0		02/21/08 15:06:44	02/21/08 15:06:44
	02/23/08 14:00:45	nmp114206_Tunnel_v6	2	Y0		02/21/08 15:06:44	02/21/08 15:06:44
	02/23/08 14:00:45	nmp206 Tunnel	1	Y0		02/21/08 15:06:44	02/21/08 15:06:44

	Policy	nmp114206_StartAction	DynAction3	DYNANCHOR	ACTIVE	IPSEC	SCOPEALL	OUTBOUND
	Policy	nmp114206_StartAction	DynAction3	DYNANCHOR	ACTIVE	IPSEC	SCOPEALL	INBOUND
	Policy	nmp114206_StartAction_v6	DynAction	DYNANCHOR	ACTIVE	IPSEC	SCOPEALL	OUTBOUND
	Policy	nmp114206_StartAction_v6	DynAction	DYNANCHOR	ACTIVE	IPSEC	SCOPEALL	INBOUND
	Policy	nmp206_StartAction	DynAction	DYNANCHOR	ACTIVE	IPSEC	SCOPEALL	OUTBOUND
	Policy	nmp206_StartAction	DynAction	DYNAMIC	ACTIVE	IPSEC	SCOPEALL	OUTBOUND



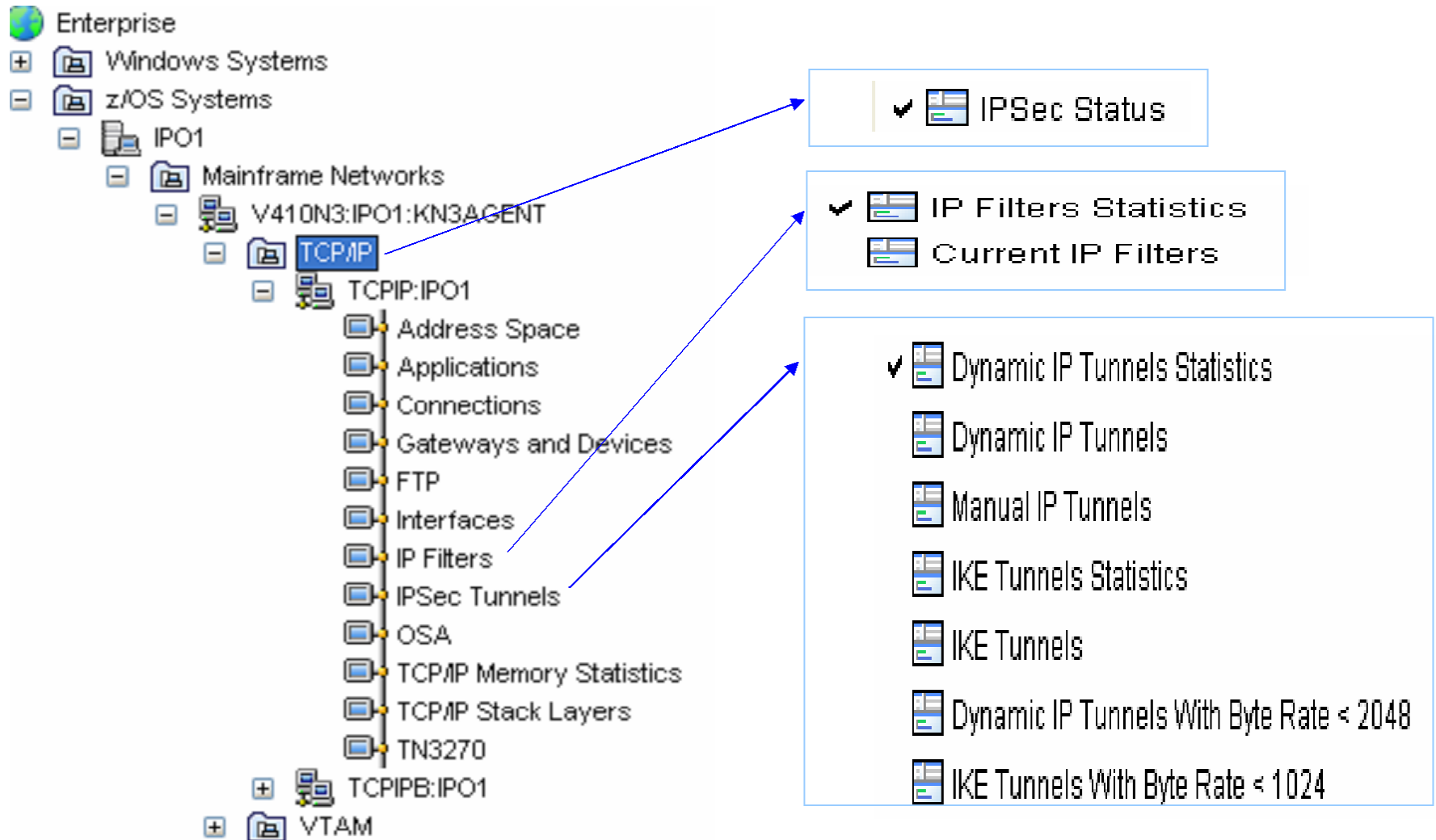
# Agenda

- Introduction
- IP Security Concepts and Terminology
- OMEGAMON XE for Mainframe Networks IP Security Monitoring Application
  - ▶ Tivoli Management Services Common Features
  - ▶ OMEGAMON XE for Mainframe Networks
  - ▶ Common IP Security Problems
  - ▶ IP Security Status – The Dashboard
  - ▶ IP Security Situations and Thresholds
  - ▶ IP Security Historical Views
- **Sample Scenarios**
  - Description of IP Security Workspaces
  - Reference





# IP Security Workspaces

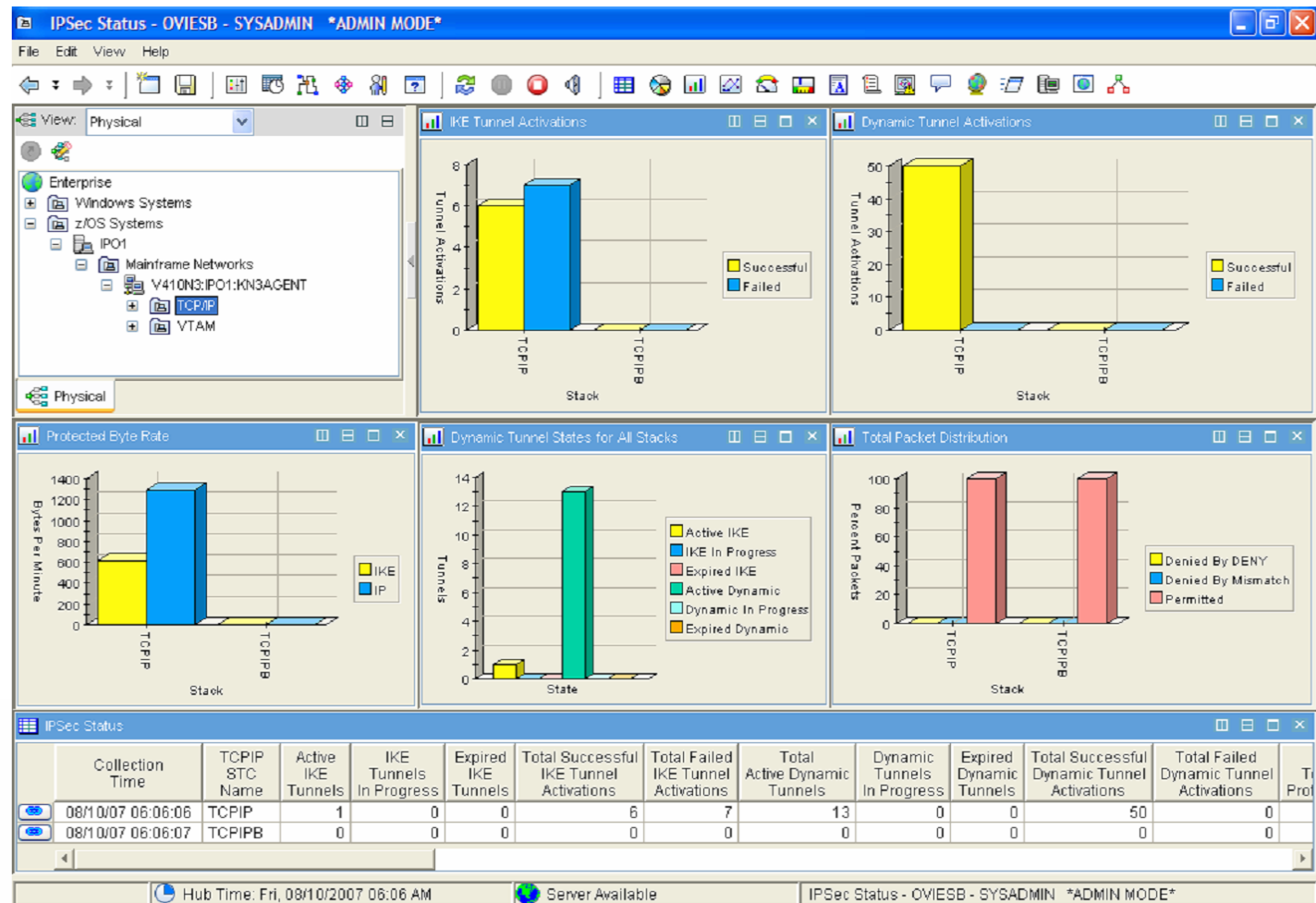


# IPSec Status – The Dashboard

- Tunnel activation statistics
- Tunnel throughput statistics
- Tunnel state analysis
- Packet permit, deny and mismatch statistics

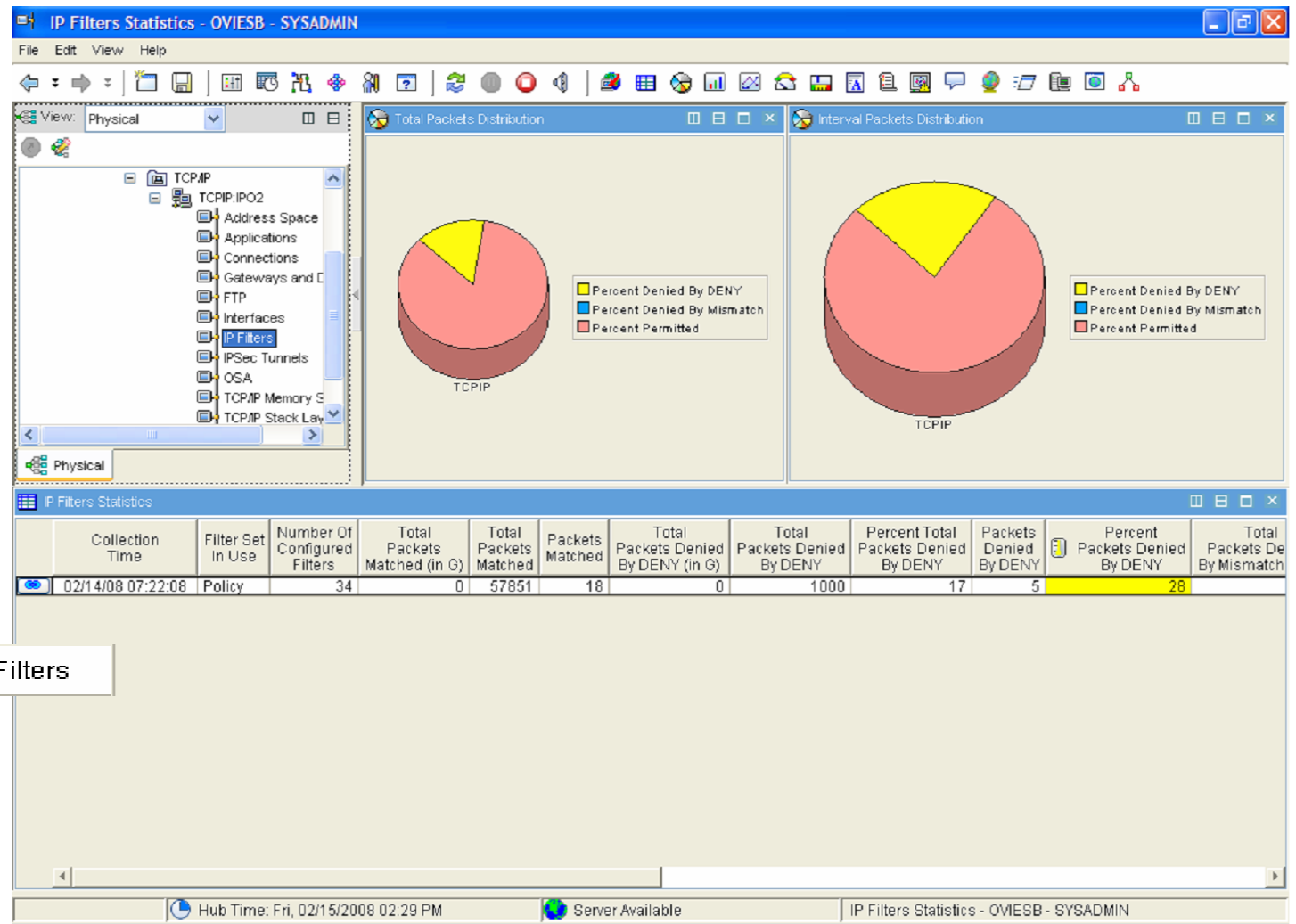
## Links

- [Dynamic IP Tunnels Statistics](#)
- [IKE Tunnels Statistics](#)
- [IP Filters Statistics](#)



# IP Filters Statistics

- Shows percentage of total packets permitted, denied and mismatched
- Shows percentage of packets permitted, denied and mismatched per collection interval
- Shows filters statistics for a stack



Li Current IP Filters

# Current IP Filters

- Identifies most matched filters
- Identifies filters denying most packets
- Identifies most mismatched filters
- Provides filters statistics and configuration information
- Displays filters in the order they are scanned by the stack

## Links

[Current IP Filters By Destination Address](#)

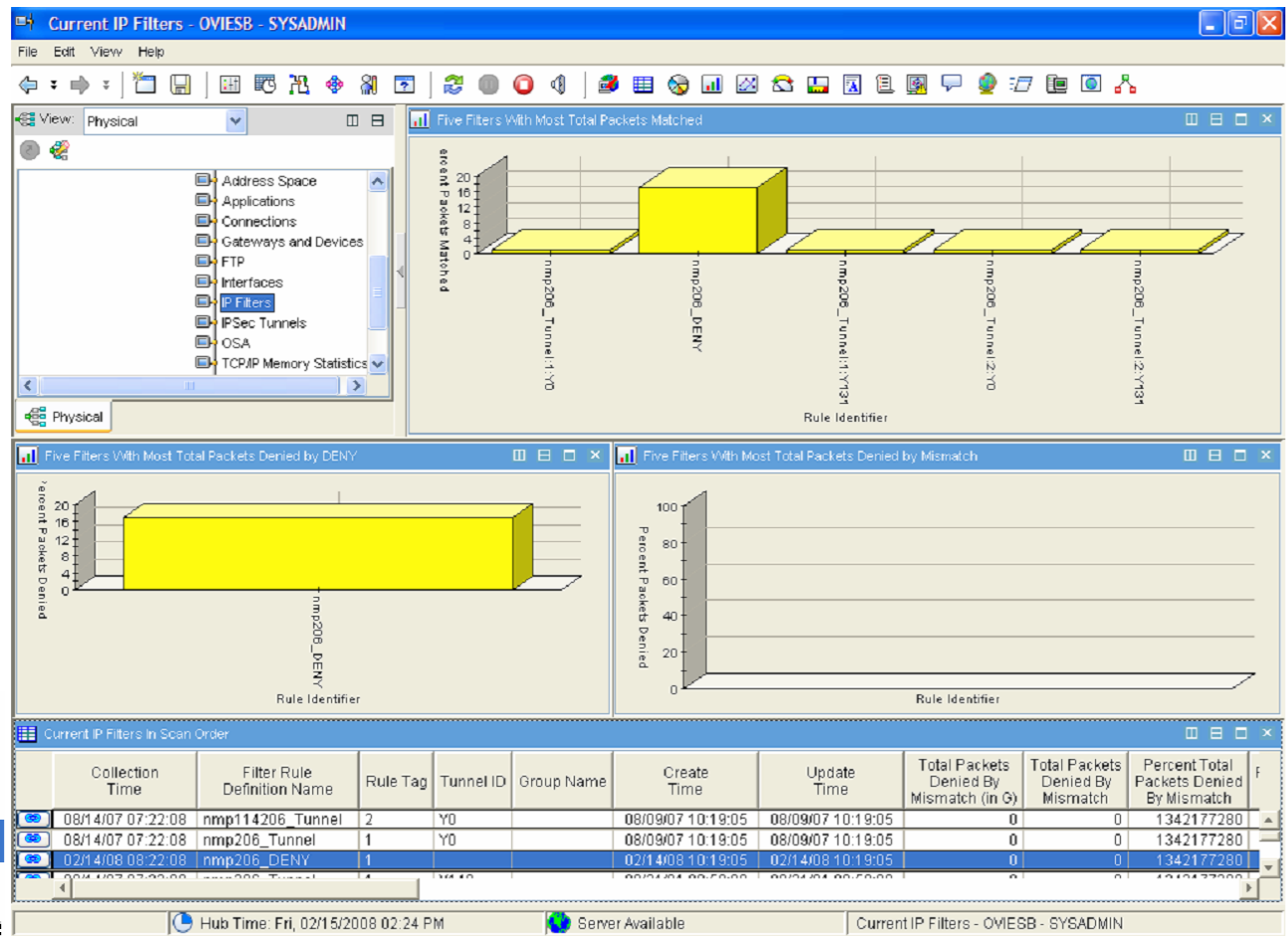
[Dynamic IP Tunnels By Tunnel ID](#)

[Manual IP Tunnels By Tunnel ID](#)

[Dynamic IP Tunnels By Filter Rule Definition Name](#)

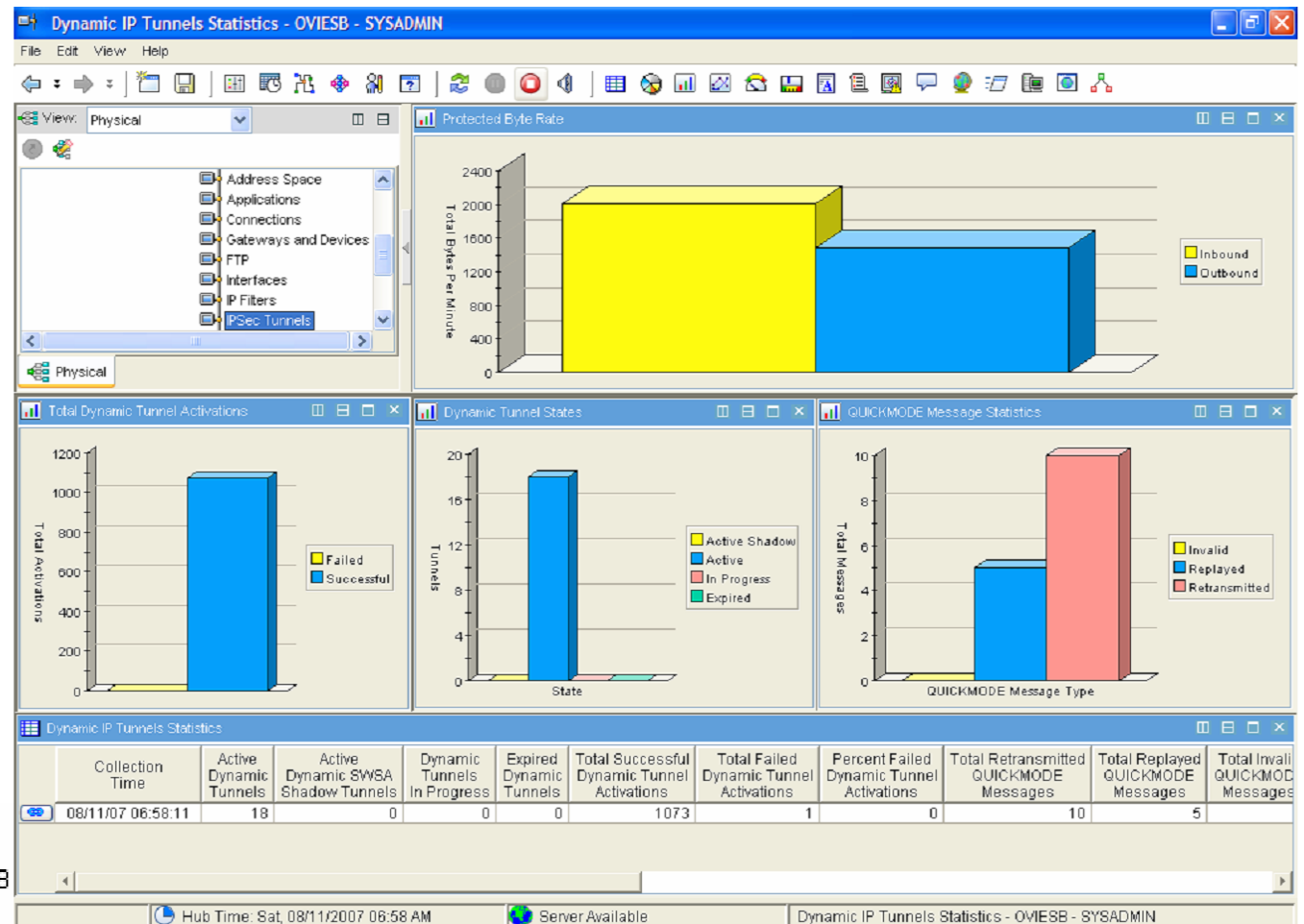
[Current IP Filters In Scan Order By Next Page](#)

[Current IP Filters In Scan Order By Previous Page](#)



# Dynamic IP Tunnels Statistics

- Total byte rate for all dynamic IP tunnels
- Dynamic IP tunnel activation statistics
- Dynamic IP tunnel state analysis
- Quickmode message statistics



## Links

- 🔗 [Dynamic IP Tunnels](#)
- 🔗 [Dynamic IP Tunnels With Byte Rate < 2048](#)
- 🔗 [Manual IP Tunnels](#)

# Dynamic IP Tunnels

- Tunnel State Analysis
- Identifies tunnels not being used
- Tunnel Statistics
  - Packet and byte counts
  - Packet and byte rates
- Tunnel configuration information
  - Traffic description
  - Associated filter rule definition name
  - VPN action name and SA information
  - Parent IKE tunnel ID
  - Refresh and expiration information
- NAT information

## Links

- [IKE Tunnels By Tunnel ID](#)
- [Current IP Filters By Filter Rule Definition Name](#)
- [Dynamic IP Tunnels By Destination Address](#)

The screenshot displays the 'Dynamic IP Tunnels - OVIESB - SYSADMIN' interface. It features a tree view on the left, a 'Tunnel States' bar chart in the center, and two data tables on the right. The bar chart shows a single bar for 'TCP/IP' with a value of approximately 75, categorized as 'Active'. The top table lists 15 tunnels with columns for Collection Time, Tunnel ID, Local Security Endpoint, Remote Security Endpoint, and Total Inbound Packets. The bottom table provides detailed statistics for tunnel Y56, including Total Inbound/Outbound Packets, Total Packets, and Packets/Rate.

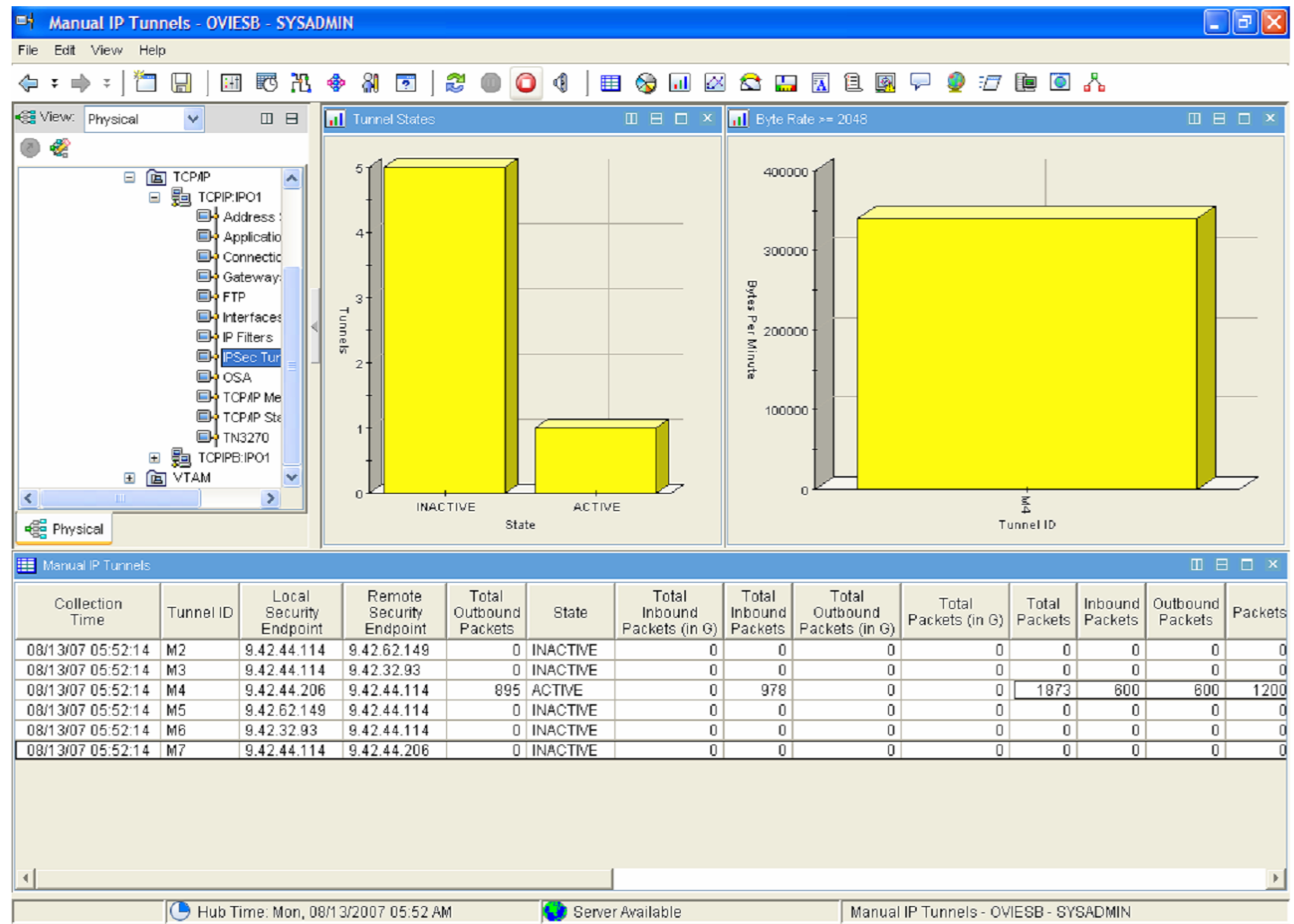
Collection Time	Tunnel ID	Local Security Endpoint	Remote Security Endpoint	Total Inbound Packets
08/11/07 07:39:12	Y58	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y63	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y61	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y60	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y57	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y76	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y70	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y72	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y74	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y75	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y73	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y62	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y69	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y71	9.42.44.206	9.42.44.114	
08/11/07 07:39:12	Y59	9.42.44.206	9.42.44.114	

Collection Time	Tunnel ID	Local Security Endpoint	Remote Security Endpoint	Total Inbound Packets (in G)	Total Inbound Packets	Total Outbound Packets (in G)	Total Outbound Packets	Total Packets (in G)	Total Packets	Inbound Packets	Outbound Packets	Packets	Packets Rate
08/11/07 07:39:12	Y56	9.42.44.206	9.42.44.114	0	2400	0	2400	0	4800	1200	1200	2400	240

# Manual IP Tunnels

- Tunnel state analysis
- Identifies tunnels with high byte rates
- Tunnel statistics
  - Packet and byte counts
  - Packet and byte rates
- Tunnel configuration information
  - Identifies endpoints
  - VPN action name and SA information



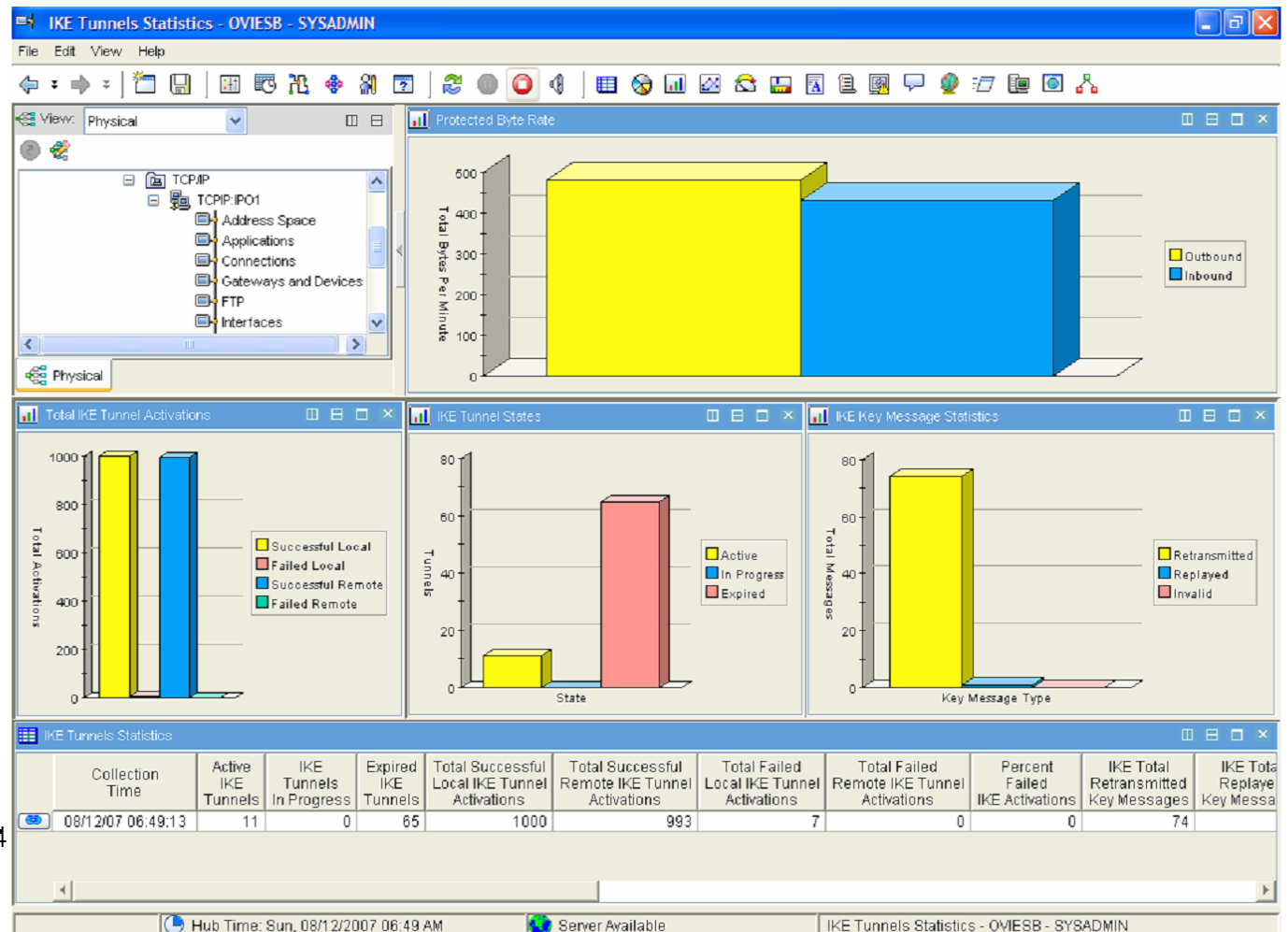
# IKE Tunnels Statistics

- Total byte rate for all IKE tunnels
- IKE tunnel activation statistics
- IKE tunnel state analysis
- Key message statistics

## Links

[IKE Tunnels](#)

[IKE Tunnels With Byte Rate < 1024](#)





# IKE Tunnels

- IKE Tunnel Statistics
  - Dynamic IP tunnel activation statistics
  - Dynamic IP tunnel state analysis
  - Byte rate statistics
- Configuration information
  - Identifies endpoints
  - Refresh and expiration information
  - SA information
- NAT information

## Links

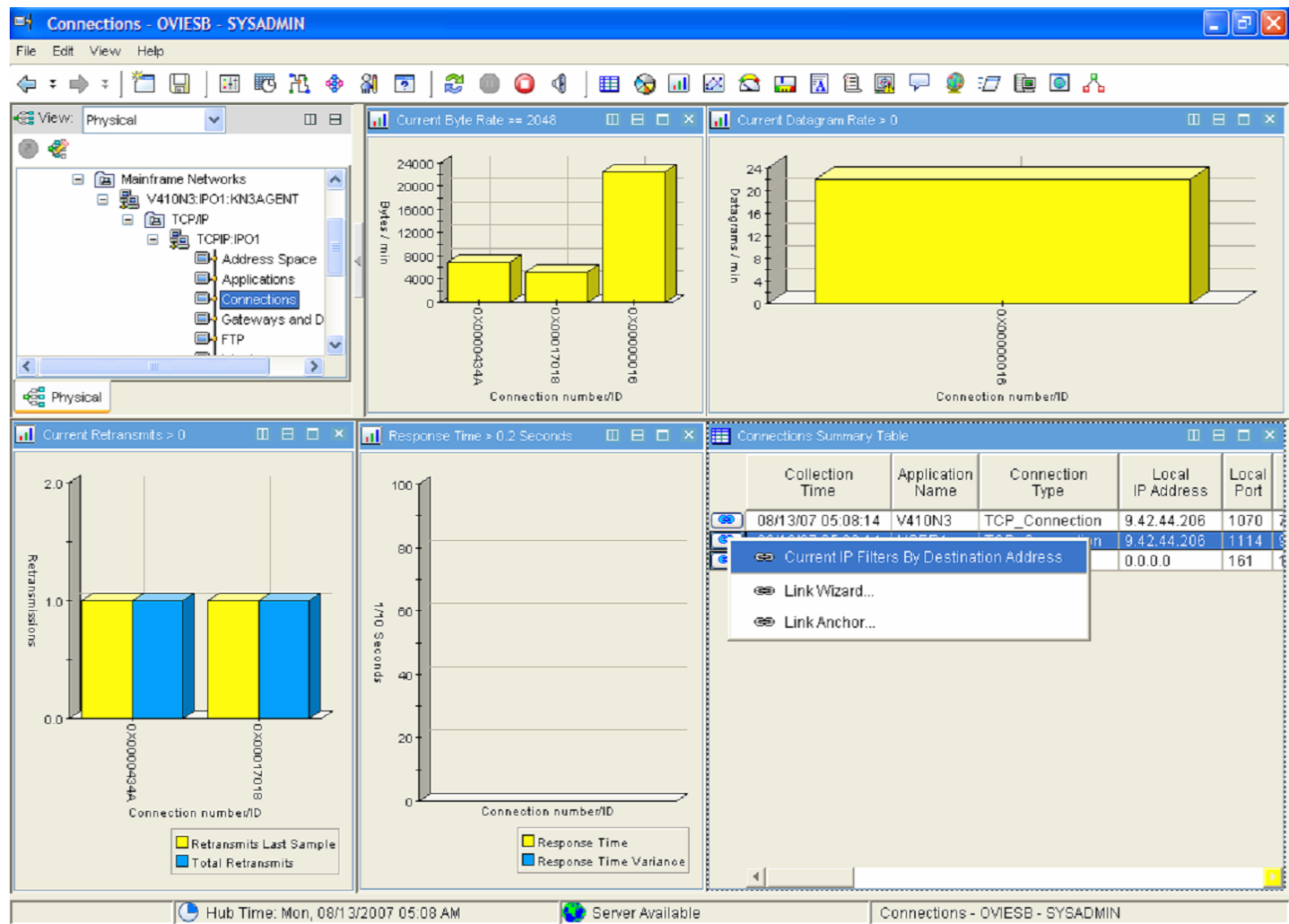
[IKE Tunnels By Security Endpoint](#)

The screenshot shows the 'IKE Tunnels With Byte Rate < 1024 - OVIESB - SYSADMIN' window. It features a navigation tree on the left, a main data table, and two charts. The 'Percent Failed Activations' chart shows a single yellow bar for tunnel K118. The 'Tunnel States' chart shows one yellow bar (Active) and one blue bar (In Progress). The bottom table provides detailed statistics for each tunnel.

Collection Time	Tunnel ID	Key Exchange Rule Name	Key Exchange Action Name	Local Security Endpoint	Remote Security Endpoint	State	Extended State	Total Bytes (in G)	Total Bytes	Bytes	Byte Rate	Active Dynamic Tunnels	In Pr Dyr Tur
08/12/07 08:17:13	K118	ker_nmp206_name	kea1	9.42.44.206	9.42.44.114	INCOMPLETE	WAIT_SA	0	0	0	0	0	
08/12/07 08:17:13	K118	ker_nmp206_name	kea1	9.42.44.206	9.42.44.114	ACTIVE	DONE	0	2248	0	0	7	

# Connections

- New links in existing TCP/IP connections workspaces allow users to examine IP filters that match a specified destination address
- Links in IP filters workspaces allow users to examine tunnels that connections might be using



# Agenda

- Introduction
- IP Security on z/OS
  - ▶ Network Security Deployment Trends and Requirements
  - ▶ IP Security Support on z/OS
  - ▶ IP Filtering
  - ▶ Tunnels and SAs
  - ▶ IP Security Monitoring Architecture
- **OMEGAMON XE for Mainframe Networks IP Security Monitoring Application**
  - ▶ Tivoli Management Services Overview
  - ▶ OMEGAMON XE for Mainframe Networks
  - ▶ IP Security Workspaces
  - ▶ IP Security Situations and Thresholds
  - ▶ IP Security Historical Views
- Scenarios
- Reference



## Reference

- **OMEGAMON XE for Mainframe Networks home page**
  - ▶ <http://www.ibm.com/software/tivoli/products/omegamon-xe-mainframe/>
  
- **OMEGAMON XE for Mainframe Networks 4.1 documentation**
  - ▶ <http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?toc=/com.ibm.omegamon.mn.doc/toc.xml>
    - Planning Guide – SC32-1924-00
    - Configuration Guide – SC32-1923-00
    - User's Guide – SC32-1925-00
    - Problem Determination Guide – SC32-1926-00
    - OMEGAMON II for Mainframe Networks
  
- **OMEGAMON XE for Mainframe Networks 4.1 Program Directory**
  - ▶ <http://www.elink.ibm.com/publications/servlet/pbi.wss?CTY=US&FNC=SRX&PBL=GI11-4116-01#>
  
- **OMEGAMON XE on z/OS 4.1 User's Guide**
  - ▶ [http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.omegamon\\_xezos.doc/welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.omegamon_xezos.doc/welcome.htm)





# Backup Slides



# Tivoli Enterprise Portal (TEP)

**Easy to use Browser controls**

**Situations**

**Historical Views**

**Intelligent Linking**

**Plug and Play components**

**View Zoom**

**Splitter controls**

**Personalized Views**

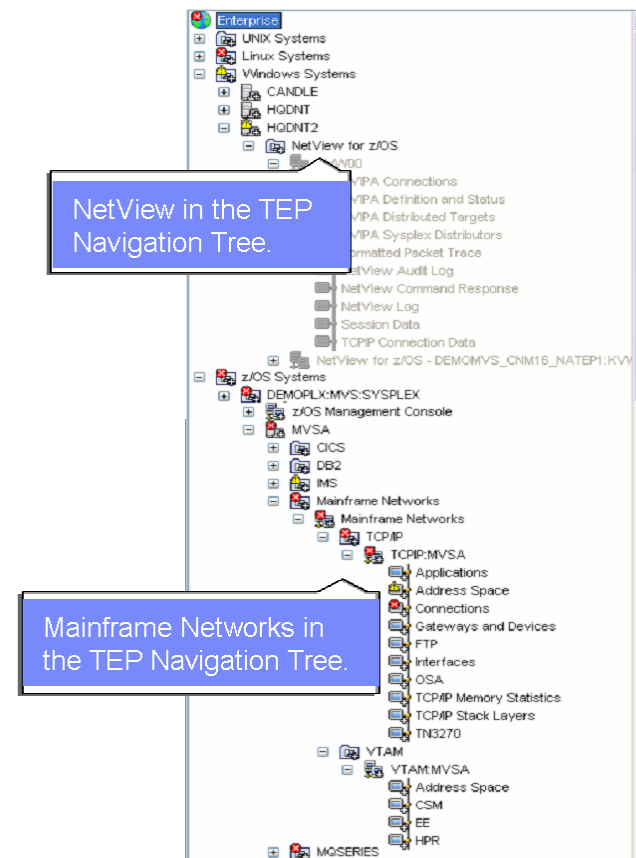
**Thresholds**

**Persistent customized workspaces**

Collection Time	Active IKE Tunnels	IKE Tunnels In Progress	Expired IKE Tunnels	Total Successful Local IKE Tunnel Activations	Total Successful Remote IKE Tunnel Activations	Total Failed Local IKE Tunnel Activations	Total Failed Remote IKE Tunnel Activations	Percent Failed IKE Activations	IKE Total Retransmitted Key Messages	IKE Total Replayed Key Messages	IKE Total Invalid Key Messages
08/10/07 04:08:06	0	0	0	4	1	7	1	58	71	71	71

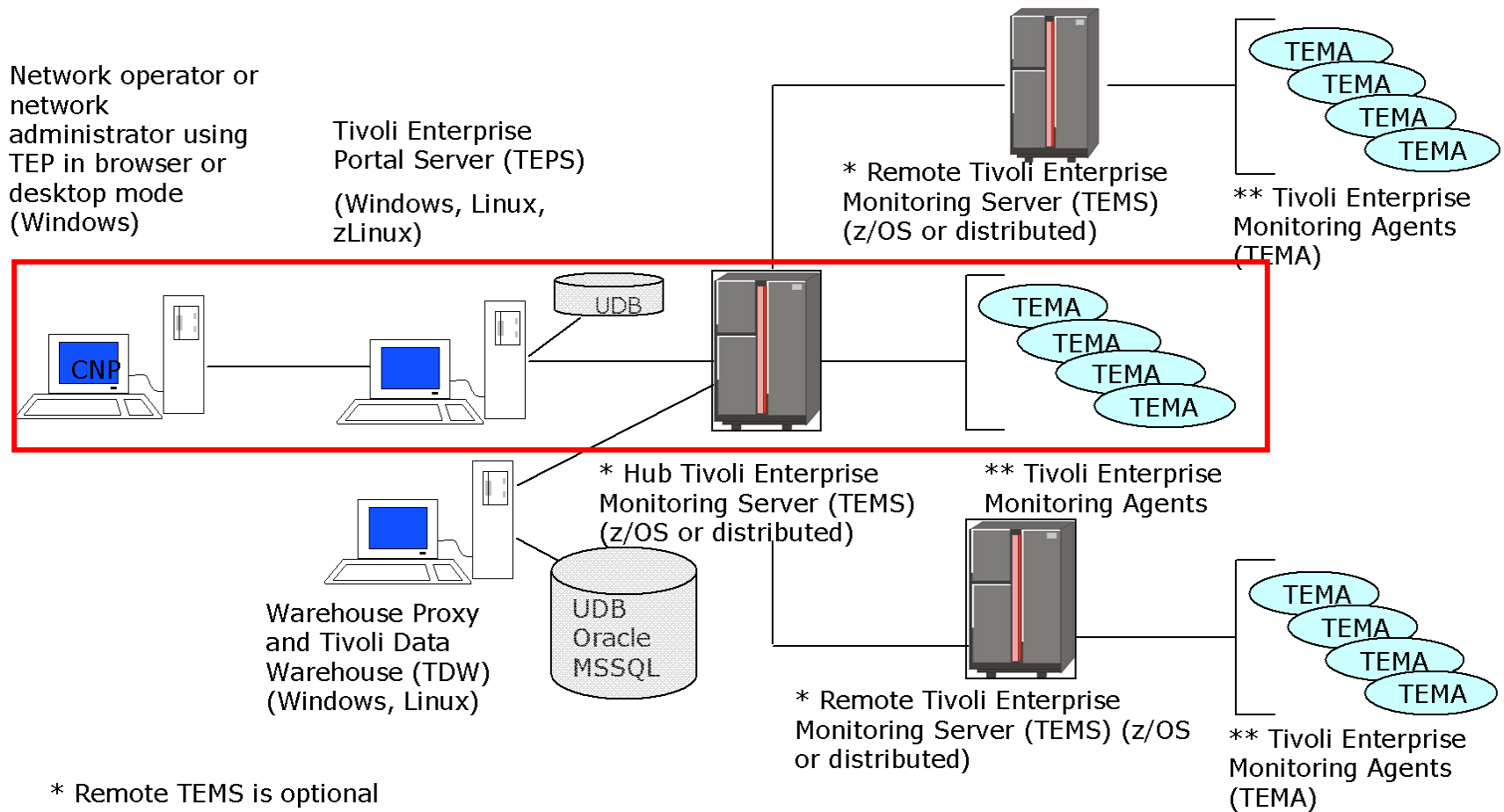
# TEP - ONE User Interface

- OMEGAMON XE for ...
  - ▶ z/OS (includes Sysplex and Crypto)
  - ▶ CICS (includes CICSplex)
  - ▶ DB2 (includes DB2plex)
  - ▶ IMS (includes IMSplex)
  - ▶ Linux on System z
  - ▶ Mainframe Networks
  - ▶ Storage
  - ▶ NetView for z/OS





# Tivoli Management Services (TMS) V6.1 Common Architecture



- \* Remote TEMS is optional
- \*\* TEMA runs on system being monitored (except NetView 5.2 management agent runs on a distributed system)



# Mainframe Networks Use of z/OS IPsec NMI

