



VANGUARD
Integrity Professionals
Information Security Experts

Implementing SERVAUTH Class Profiles

Jim McNeill



© 2011 Vanguard Integrity Professionals

TRADEMARKS



VANGUARD
Integrity Professionals
Information Security Experts


- The following are trademarks or registered trademarks of the International Business Machines Corporation:
 - IBM z/OS
 - z/OS MVS/DFP
 - MVS/ESA RACF
 - SecureWay VTAM
 - S/390
- UNIX is a registered trademark of The Open Group in the United States and other countries.




2




Unit Topics




1. Basic OSI models
2. IP sub-netting basics
3. Stacks
4. Ports
5. Networks
6. Misc controls
7. SERVAUTH Profiles




3




Open Systems Interconnection Model



	OSI Layers	TCP/IP Layers
Layer 7	Application	Application Programs and Protocols for file transfer, electronic mail, etc. (Telnet, FTP,SMTP, etc.)
Layer 6	Presentation	
Layer 5	Session	
Layer 4	Transport	Internet Protocol (IP)
Layer 3	Network	
Layer 2	Data Link	Network Interface Cards: Ethernet, Token-Ring, etc NIC Drivers: Open Datalink Interface (ODI), Network Independent Interface Specification (NDIS)
Layer 1	Physical	Transmission Media: Twisted Pair, Coax, Fiber Optic, Wireless Media, etc.



4



Addressing without Subnets

172.16.1.2 172.16.1.3 172.16.2.1 172.16.254.254

172.16.0.0

- A class B “Flat Network”, has one network and 65534 hosts (Computing Devices) available
 - How to manage that number of devices?
 - Performance?

5

Addressing with Subnets

- A class B “Subdivided Network”, has Smaller Manageable number of devices and can be controlled (routed, firewalled, etc.)

6

Subnetwork Benefits

Smaller networks are easier to troubleshoot

Smaller networks are easier to manage Overall traffic

Increase the network manager's control over the address space

Subnetwork

- Subdivide on IP network number is an important initial task of network managers
- Understanding how your System Z is connected and what is connected to is important to knowing how to protect it.

7

Default Subnet Masking

Class A	255.0.0.0	1.0.0.0 – 127.0.0.0				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: yellow; padding: 2px;">1111 1111</td> <td style="background-color: yellow; padding: 2px;">0000 0000</td> <td style="background-color: yellow; padding: 2px;">0000 0000</td> <td style="background-color: yellow; padding: 2px;">0000 0000</td> </tr> </table>			1111 1111	0000 0000	0000 0000	0000 0000
1111 1111	0000 0000	0000 0000	0000 0000			
Class B	255.255.0.0	128.0.0.1 – 191.255.0.0				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: yellow; padding: 2px;">1111 1111</td> <td style="background-color: yellow; padding: 2px;">1111 1111</td> <td style="background-color: yellow; padding: 2px;">0000 0000</td> <td style="background-color: yellow; padding: 2px;">0000 0000</td> </tr> </table>			1111 1111	1111 1111	0000 0000	0000 0000
1111 1111	1111 1111	0000 0000	0000 0000			
Class C	255.255.255.0	192.0.0.0- 223.255.255.0				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: yellow; padding: 2px;">1111 1111</td> <td style="background-color: yellow; padding: 2px;">1111 1111</td> <td style="background-color: yellow; padding: 2px;">1111 1111</td> <td style="background-color: yellow; padding: 2px;">0000 0000</td> </tr> </table>			1111 1111	1111 1111	1111 1111	0000 0000
1111 1111	1111 1111	1111 1111	0000 0000			

8

Changing the Range

172	16	0	0
-----	----	---	---

Default Subnet

255.255.0.0

1111 1111	1111 1111	0000 0000	0000 0000
-----------	-----------	-----------	-----------

Our Subnet

255.255.255.0

1111 1111	1111 1111	1111 1111	0000 0000
-----------	-----------	-----------	-----------

Define a subnet mask by extending the network portion to the right, 8 bits in this example

9

Our subnet

Accounting

172.16.1.2	172.16.1.3
172.16.1.0	

Miami

172.16.2.2	172.16.2.3
172.16.2.0	

Server Farm

172.16.3.2	172.16.3.3
172.16.3.0	

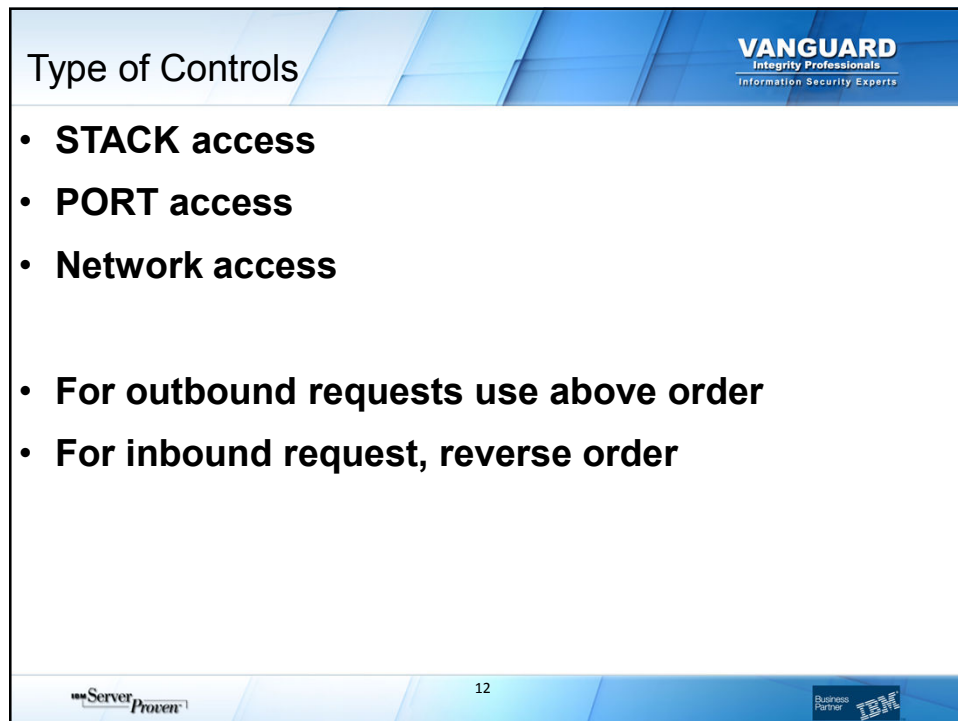
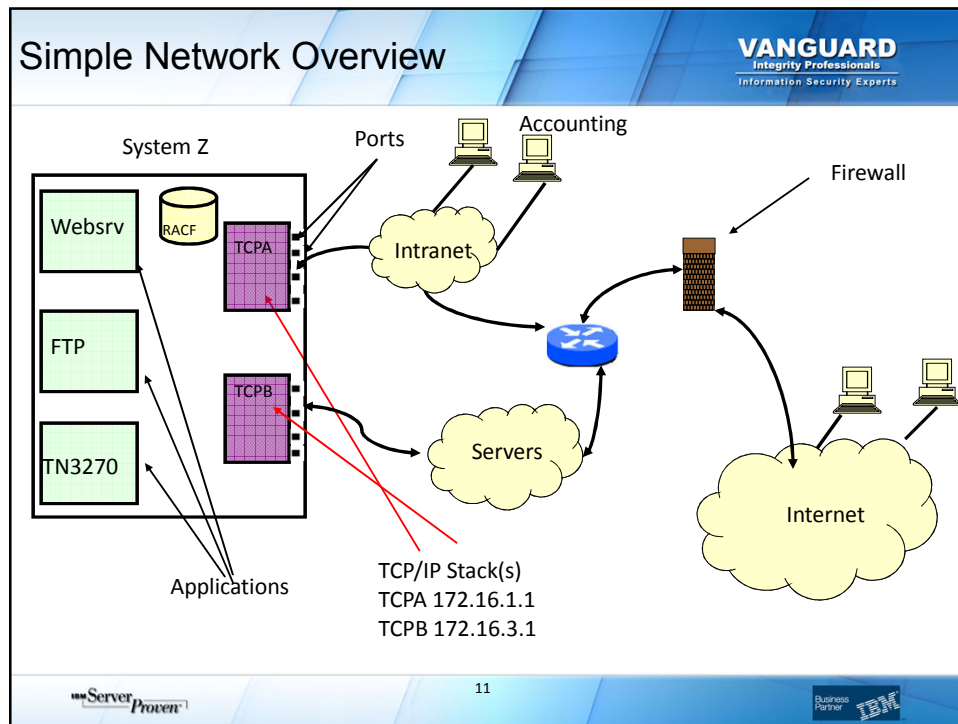
Chicago

172.16.4.2	172.16.4.3
172.16.4.0	

Class B	255.255.0.0	172.16.0.0– 172.16.255.255
----------------	--------------------	-----------------------------------

1111 1111	1111 1111	0000 0000	0000 0000
-----------	-----------	-----------	-----------

10



Controlling Stack Access

VANGUARD
Integrity Professionals
Information Security Experts

- Purpose to control who can access what from where.
- Applies to **USERS** on z/OS
- **HOW?**
 - Profiles in the **SERVAUTH Class**

Server Proven 13 Business Partner IBM

Controlling Stack Access

VANGUARD
Integrity Professionals
Information Security Experts

System Z

The diagram shows a dashed box representing System Z. Inside, there are three user boxes: John, Jim, and Finance HTTPD. Below them are two z/OS CS TCP/IP Stack boxes: one for TCP/IPA (Public Lan) and one for TCP/IPB (Protected Lan). A RACF database icon is also present. Arrows indicate access: John and Finance HTTPD have arrows pointing to both stacks. Jim has an arrow pointing to the TCP/IPA stack and a red 'X' over the arrow pointing to the TCP/IPB stack.

Stack access

- Define the stack resources with UACC(NONE) and permit groups or individual users to allow them to use the TCP/IP stack (open **ANY** socket on the stack).


{ RACF Profiles Protecting TCP/IP Stacks
EZB.STACKACCESS.sysname.tcpname. }

Server Proven Business Partner IBM

What are ports

VANGUARD
Integrity Professionals
Information Security Experts

- An easy way to understand ports is to imagine your **IP address** is a cable box and the ports are the different channels on that cable box.
- The cable company knows how to send cable to your cable box based upon a unique serial number associated with that box (**IP address**), and then you receive the individual shows on different channels (Ports).



Server ProvenSM 15 Business Partner **IBM**

Controlling Port Access

VANGUARD
Integrity Professionals
Information Security Experts

- Purpose to control who can access what from where.
- Applies to USERS on z/OS
- HOW?
 - Profiles in the SERVAUTH Class
- Resource name format:
 - EZB.PORTACCESS.sysname.tcpname.portname

Server ProvenSM 16 Business Partner **IBM**

Defining Reserved Ports

20	TCP	*	SAF FTPCTL	;	FTP SERVER
21	TCP	*	SAF FTPDATA	;	FTP SERVER
23	TCP	*	SAF TELNET	;	TELNET SERVER
25	TCP	*	SAF SMTP	;	SMTP SERVER
53	TCP		NAMESRV	;	Domain Name Server
53	UDP		NAMESRV	;	Domain Name Server
69	UDP		OMVS	;	OE TFTP SERVER
80	TCP		OMVS	;	OE WEB SERVER
81	TCP	*	SAF JIMWEB	;	OE WEB SERVER

Partial listing of TCPIP PROFILE Data

UDP=User Datagram Protocol

TCP=Transmission Control Protocol

TCP ports: 0-65535 UDP ports 0-65534

Low ports 0-1024 High ports 1025 -65535

17

Controlling port access (FTP)

The diagram illustrates a z/OS 1.6 system (SYSA 192.168.5.5) with components Websrv, FTP, and TN3270. A RACF database and a TCPA (Transmission Control Profile Access) component are also shown. The system is connected to an Intranet and the Internet. Bob's workstation is shown with a callout for 'FTP 192.168.5.5'.

FTP calls RACF and asks:
 Does BOB have READ access To
EZB.PORTACCESS.SYSA.TCPA.FTPCTL

NOTE: Passive FTP bypasses PORTACCESS Because it uses dynamic PORTS

18

Controlling Access to HFS file System

VANGUARD
Integrity Professionals
Information Security Experts

192.168.5.5 SYSA

System z

FTP calls RACF and asks:
Does BOB have READ access To
EZB.FTP.SYSA.FTPD%.ACCESS.HFS

Server Proven

19

Business Partner IBM

Controlling Network Access

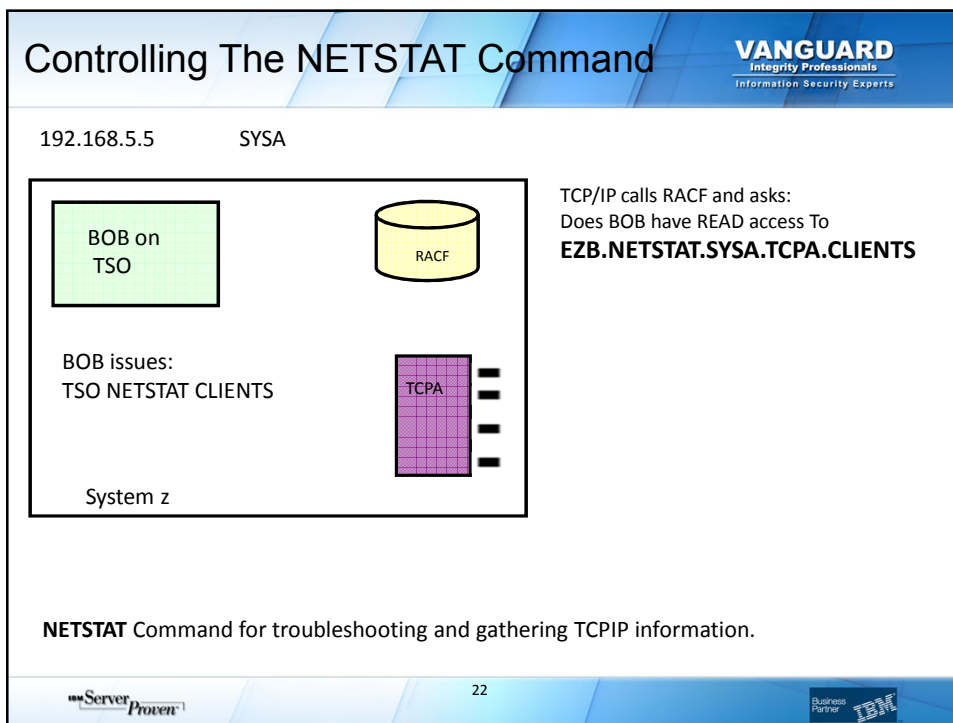
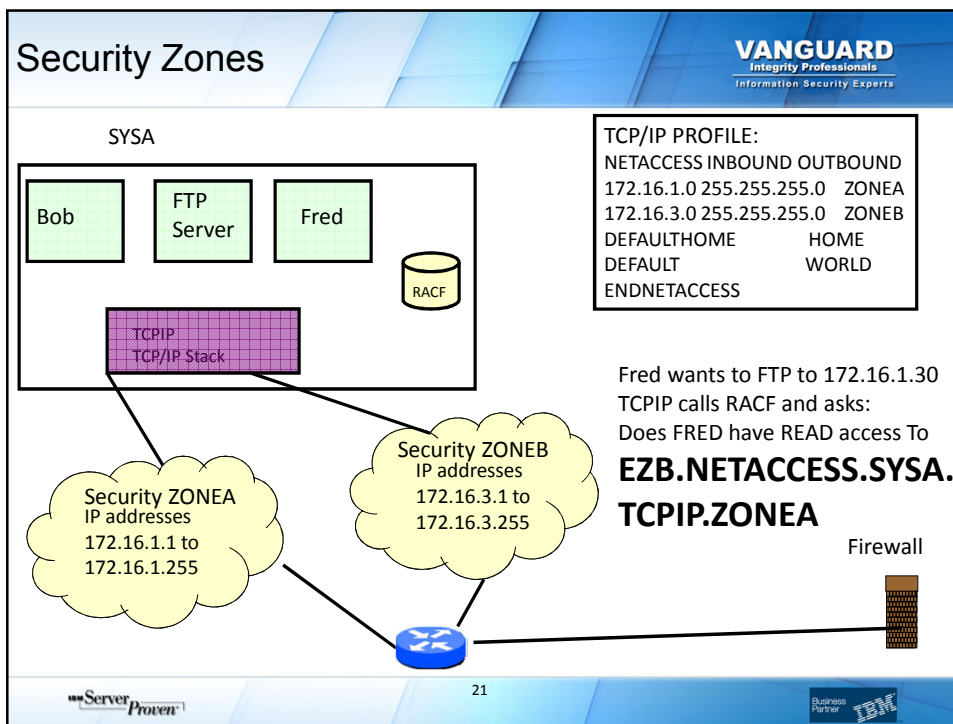
VANGUARD
Integrity Professionals
Information Security Experts

- Purpose to control who can access what from where.
- Applies to USERS on z/OS
- HOW?
 - Profiles in the SERVAUTH Class
- Resource name format:
 - EZB.NETACCESS.sysname.tcpname.zone

Server Proven

20

Business Partner IBM



Controlling TCP/IP Packet Trace

192.168.5.5 SYSA

Packet trace Monitor Application

RACF

TCPA

System Z

Bob is running the packet trace monitor application.
TCP/IP calls RACF and asks:
Does BOB have READ access To

EZB.NETMGMT.SYSA.TCPA.SYSTCPDA

Note: this can be applied system wide or stack wide.

23

Controlling TCP Connection Information

192.168.5.5 SYSA

Connection Information Monitor Application

RACF

TCPA

z/OS 1.6

Bob is running the TCP Connection monitor application.
TCP/IP calls RACF and asks:
Does BOB have READ access To

EZB.NETMGMT.SYSA.TCPA.SYSTPCPN

24

Controlling Real-Time SMF Information

192.168.5.5 SYSA

SMF Information Monitor Application

RACF

TCPA

System z

Bob is running the SMF Information monitor application.
 TCP/IP calls RACF and asks:
 Does BOB have READ access To
EZB.NETMGMT.SYSA.TCPA.SYSTCPSM

25

SERVAUTH Profiles

Function	Description	SERVAUTH profile
TN3270 server access control	Controls ability to access TN3270 server based on SAF user ID associated with TLS-authenticated X.509 client certificate	EZB.TN3270.sysname.tcpname.PORTxxxx
FTP server access control	Controls ability to access FTP server based on SAF user ID associated with TLS-authenticated X.509 client certificate	EZB.FTP.sysname.ftpdname.sysname.PORTxxxx
DCAS server access control	Controls ability to access DCAS server based on SAF user ID associated with TLS-authenticated X.509 client certificate	EZB.DCAS.cvtsysname
TCP stack access control	Controls user ability to open a socket and get host name or host ID	EZB.STACKACCESS.sysname.tcpname
TCP local port access control	Controls user ability to bind to a non-ephemeral TCP or UDP port	EZB.PORTACCESS.sysname.tcpname.port_safname
TCP netaccess access control	Controls local user inbound and outbound access to network resources, and local user access to local IP address when explicitly binding to local interface (or using job-specific source IP addresses)	EZB.NETACCESS.sysname.tcpname.security_zoneiname
Netstat command access control	Provides ability to restrict Netstat usage	EZB.NETSTAT.sysname.tcpname.netstat_option
Policy Agent command control	Provides ability to restrict pasearch command usage by policy type	EZB.PAGENT.sysname.tcpname.policy_type
FTP SITE command control	Provides ability to restrict usage of SITE DUMP and DEBUG commands (commands generate large amount of output)	EZB.FTP.sysname.ftpdname.SITE.DUMP EZB.FTP.sysname.ftpdname.SITE.DEBUG
SNMP agent control	Provides ability to control usage of SNMP subagents that connect to the TCP/IP SNMP agent	EZB.SNMPAGENT.sysname.tcpname
MODDVIPA utility program control	Provides ability to restrict usage of MODDVIPA utility program (creates new DVIPA on system)	EZB.MODDVIPA.sysname.tcpname
Fast Response Cache Accelerator (FRCA) Access Control	Provides ability of user to create FRCA cache (FRCA used by Web servers for caching static Web pages in the stack)	EZB.FRCAACCESS.sysname.tcpname
TCP connection information service access control	Provides ability to restrict access to the TCP connection information using TCP connection information service; intended for network management applications	EZB.NETMGMT.sysname.tcpname.SYSTCPCN

26

SERVAUTH Profiles		VANGUARD Integrity Professionals Information Security Experts
Function	Description	SERVAUTH profile
Real-time SMF information service access control	Provides ability to restrict access to select real-time SMF records accessible using the SMF information service; intended for network management applications	EZB.NETMGMT.sysname.tcpname.SYSTCPSM
TCP/IP packet trace service access control	Provides ability to restrict access to select real-time packet trace records accessible using the TCP/IP packet trace service; intended for network management applications	EZB.NETMGMT.sysname.tcpname.SYSTCPDA
FTP HFS access control	Provides ability to generally restrict FTP user access to HFS	EZB.FTP.sysname.ftpddaemonname.ACCESS.HFS
Broadcast access control	Provides ability to control whether an application is permitted to set the SO_BROADCAST socket option needed to send broadcast datagrams	EZB.SOCKOPT.sysname.tcpname.SO_BROADCAST
IPv6 Advanced Socket API access control	Provides ability to control whether an application is permitted to set IPv6 advanced socket API options: IPv6_NEXTHOP IPv6_TCLASS IPv6_RTHDR IPv6_HOPOPTS IPv6_DSPOPTS IPv6_RTHDRDSTOPT IPv6_PKTINFO IPv6_HOPLIMIT	EZB.SOCKOPT.sysname.tcpname.IPV6_NEXTHOP EZB.SOCKOPT.sysname.tcpname.IPV6_TCLASS EZB.SOCKOPT.sysname.tcpname.IPV6_RTHDR EZB.SOCKOPT.sysname.tcpname.IPV6_HOPOPTS EZB.SOCKOPT.sysname.tcpname.IPV6_DSPOPTS EZB.SOCKOPT.sysname.tcpname.IPV6_RTHDRDSTOPT EZB.SOCKOPT.sysname.tcpname.IPV6_PKTINFO EZB.SOCKOPT.sysname.tcpname.IPV6_HOPLIMIT
TCP/IP stack initialization access control	Controls ability of applications to open a socket before AT-TLS policy is loaded into the TCP/IP stack	EZB.INITSTACK.sysname.tcpname
CIM provider access control	Provides ability to restrict access to CIM data	EZB.CIMPROV.sysname.tcpname
ipsec command access control	Provides ability to control ipsec command usage ²⁷	EZB.IPSECCMD.sysname.tcpname

Reference Manuals		VANGUARD Integrity Professionals Information Security Experts
z/OS V1R1.13 CS: IP CONFIGURATION GUIDE	SC31-8775-5	
z/OS V1R1.13 CS: IP CONFIGURATION REFERENCE	SC31-8776-6	