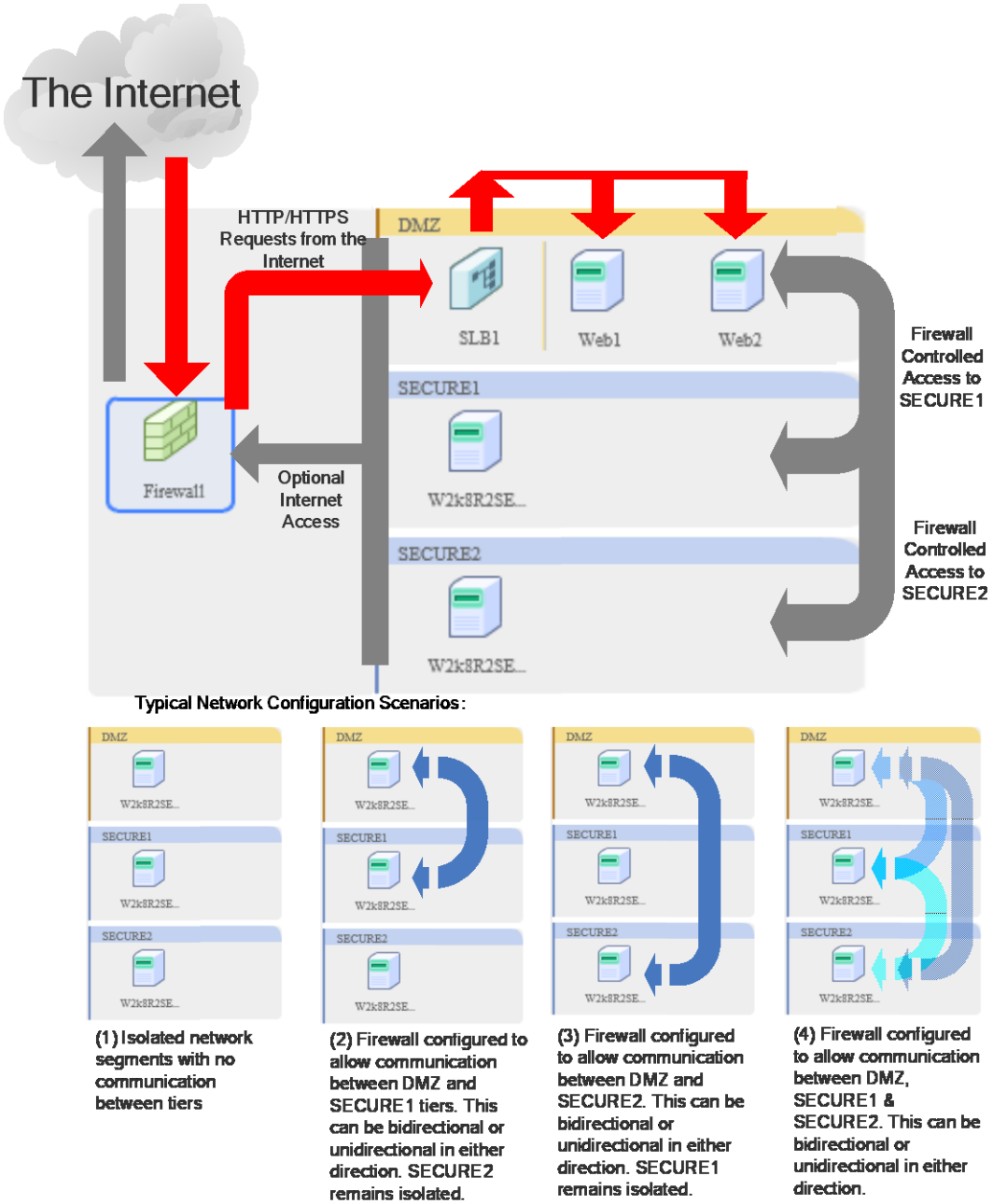
Understanding and Configuring Network Connectivity

Between VLAN Segments within and between multiple Virtual Systems (vSYS)s

The below diagram depicts an example 3-tier networked VSYS within the FUJITSU Cloud Service S5 and shows the possible configuration options.



The larger diagram shows an environment that has been configured to accept HTTP/HTTPS access from the Internet. These requests are load balanced between two Web servers in the DMZ zone. Access from the Internet to SECURE1 or SECURE2 is not possible. Communication has also been configured to access servers in SECURE1 and SECURE2, with all servers across all three tiers being able to access the Internet if required.

The lower diagrams depict other typical configuration options that can be configured between tiers, this includes no connectivity (1), limited connectivity (2 & 3) and full all way connectivity (4).

The following firewall rules would allow full, unrestricted two-way TCP and UDP communication between network segments within a vSYS as depicted in the lower right hand diagram above.

FROM	TO	ID	SOURCE	SOURCE PORT	TARGET SERVICE	TARGET PORT	PROTOCOL	ACTION	LOG
DMZ	SECURE1	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF
DMZ	SECURE2	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF
SECURE1	DMZ	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF
SECURE2	DMZ	xx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF
SECURE1	SECURE2	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF
SECURE2	SECURE1	xx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF

These rules could of course be restricted to certain ports, IP addresses or segments (one/two way) as required within your deployment.

Another benefit of connecting networks like this, is that it allows Virtual Servers across all three segments to be accessed remotely via RDP, without the need to disconnect and establish a VPN to a specific network segment. E.g. a RDP connection can be made to a server in SECURE2, with a VPN connection to DMZ network. (If after configuring these rules, RDP across tiers cannot be achieved, try disconnecting and reconnecting the VPN connection to another tier and retry).

vSYS to vSYS communication (within a contract)

The firewall rules for a vSYS can be configured to allow one vSYS to connect to another over the Intranet connection. This does not require the addition of either 'Intranet' or 'Internet' to your network configuration.

When Intranet is specified in the TO address, the rule must contain an IP address of a target server. Therefore a firewall rule must be added for each destination server. i.e. if there is more than one server on the destination network segment, then add an additional firewall rule for each.

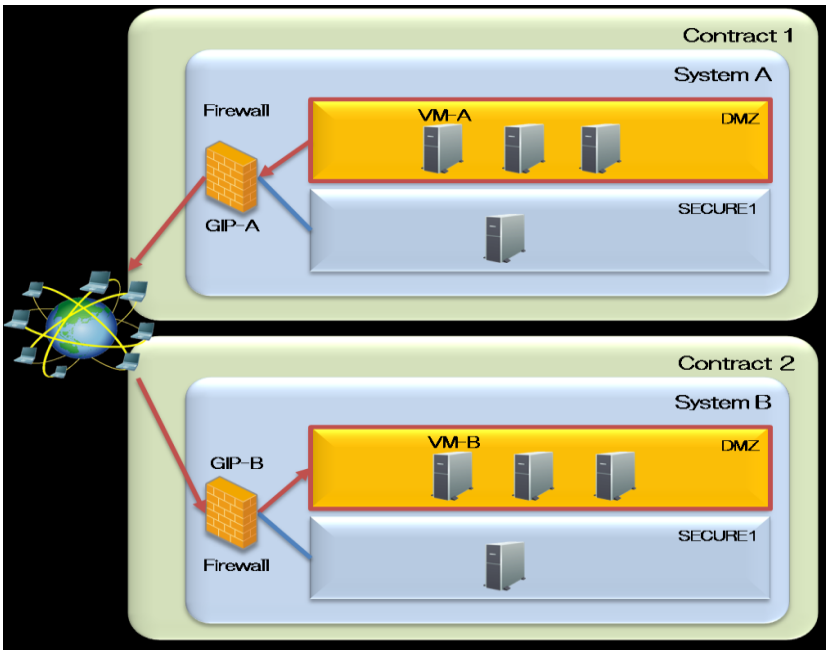
The following firewall rules when configured on the firewall of two separate vSYS's, will allow full two way TCP-UDP communication between network segments.

FROM	TO	ID	SOURCE	SOURCE PORT	TARGET SERVICE	TARGET PORT	PROTOCOL	ACTION	LOG	Comment
DMZ	Intranet	xxx	ANY	ANY	<IP ADDRESS>	ANY	TCP-UDP	ACCEPT	ON/ OFF	Repeat for each destination server
SECURE1	Intranet	xxx	ANY	ANY	<IP ADDRESS>	ANY	TCP-UDP	ACCEPT	ON/ OFF	Repeat for each destination server
SECURE2	Intranet	xxx	ANY	ANY	<IP ADDRESS>	ANY	TCP-UDP	ACCEPT	ON/ OFF	Repeat for each destination server
Intranet	DMZ	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF	
Intranet	SECURE1	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF	
Intranet	SECURE2	xxx	ANY	ANY	ANY	ANY	TCP-UDP	ACCEPT	ON/ OFF	

These rules could of course be restricted to certain ports and IP addresses as required within your deployment.

vSYS to vSYS communication (across a contract)

This can be configured via Global IP address to Virtual Machines in the DMZ network segment only, over the Internet. It is advised to lock down the firewalls to specific source/target IP addresses and required ports.



Both the source and destination must have "Internet" connection and Global IP Addresses, with NAT settings configured in both systems. The following tables summarise the rules that can be configured on both source and target firewall to allow a VM in all 3 network tiers, to access a VM in the DMZ zone of a different contract.

Source to Target Firewall Rules:

FROM	TO	ID	SOURCE	SOURCE PORT	TARGET SERVICE	TARGET PORT	PROTOCOL	ACTION	LOG	Comment
DMZ	Internet	xxx	<IP ADDRESS>	<REQUIRED PORT>	<IP ADDRESS>	<REQUIRED PORT>	<REQUIRED PROTOCOL>	ACCEPT	ON/ OFF	Repeat for each rule required
SECURE1	Internet	xxx	<IP ADDRESS>	<REQUIRED PORT>	<IP ADDRESS>	<REQUIRED PORT>	<REQUIRED PROTOCOL>	ACCEPT	ON/ OFF	Repeat for each rule required
SECURE2	Internet	xxx	<IP ADDRESS>	<REQUIRED PORT>	<IP ADDRESS>	<REQUIRED PORT>	<REQUIRED PROTOCOL>	ACCEPT	ON/ OFF	Repeat for each rule required

Target to Source Firewall Rules:

Internet	DMZ	xxx	<IP ADDRESS>	<REQUIRED PORT>	<IP ADDRESS>	<REQUIRED PORT>	<REQUIRED PROTOCOL>	ACCEPT	ON/ OFF	Repeat for each rule required

Contact
Fujitsu Global Cloud Team
FUJITSU
E-mail: cloud_gsd@au.fujitsu.com
Website: au.fujitsu.com