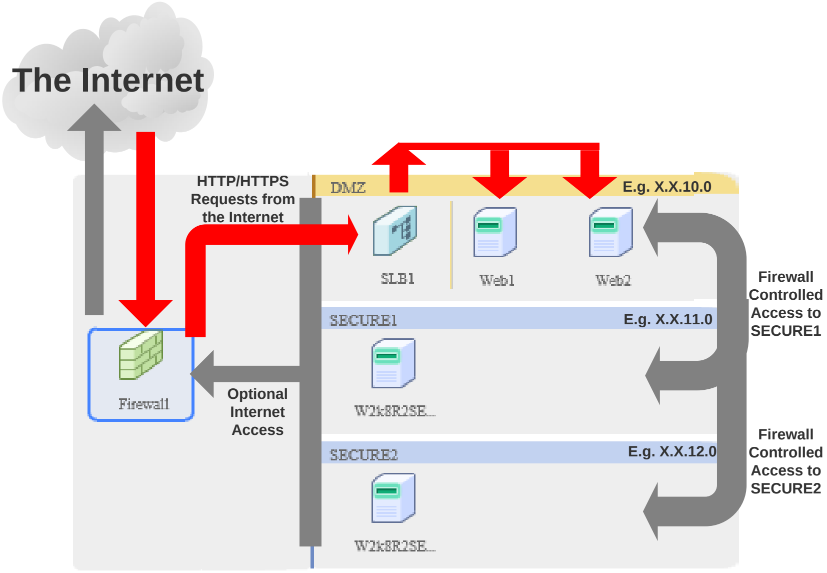
Understanding the FUJITSU Cloud Service S5 Tiered Network Topology

Choosing between the 1, 2 & 3 Tier Network Security Models

At the point of creation, it is possible to specify the number of network segments (vNETs) that the Virtual System (vSYS) will have. The default option is a single DMZ segment, which is accessible from the Internet when enabled via the FUJITSU Cloud Service S5 Firewall. A further 1 or 2 SECURE (no inbound Internet access) vNETs can be specified, providing the customer with a choice of 1, 2 or 3 tier networks. **Note, once the vNET topology has been configured, it cannot be changed**. Each network segment will have its own IP subnet, which will be sequential in order and based on the IP address range previously chosen by the customer.

The below diagram depicts an example of a full 3-tier networked VSYS within FUJITSU Cloud Service S5



The DMZ acronym of the default 1-tier network stands for De-Militarised Zone. This is an analogy for an area or strip of land that safely separates two opposing forces, during conflict. In computing terms, this refers to a network segment that is specifically intended to host public facing services, and is isolated from the rest of the internal network. It sits behind a firewall and acts as a buffer between the Internet and Internal-only services.

For security reasons, the default configuration of each new virtual firewall is to block all traffic into and out of the vSYS, meaning the DMZ network has no connectivity with anything else. It is the customer's decision to assign any required Global IP addresses and allow the required inbound and outbound communications through the firewall.

Without any firewall configuration, there is very little difference between the DMZ, SECURE 1 and SECURE 2 networks, as all segments are isolated. The DMZ only really becomes a De-Militarised Zone with the additional of one or more SECURE internal networks and the configuration of Internet communication with the DMZ zone.

There is no cost difference between each topology so the decision on which vNET topology to go for, is entirely dependent on the intended current and future use of the vSYS and the perceived security threat.

If the vSYS is intended to provide public Internet Facing Web Services such as a static Web Page, and there is no sensitive data on the servers, then a single DMZ network may suffice. This topology may also be suitable if deploying a basic system, where no external connectivity is required and provision for future growth is not required.

The perceived risk of a single vNET, is that it only provides one layer of protection for all servers. Although a Firewall goes some way to protect the DMZ network, it is possible that an attacker can gain access via a legitimate port by exploiting a security vulnerability or other means. This would then enable the attacker to attempt further penetrative attacks, in an attempt to gain access to other sensitive data or services, via the full range of ports and IP addresses on that subnet.

To protect against this, FUJITSU Cloud Service S5 allows the provision of two additional secure networks that cannot be accessed directly from the Internet. This adds extra layers of protection for servers that do not have to be public facing, by allowing them to be hosted on a separate subnet and limiting communication between vNets.

The decision to deploy a 2 or 3 tier model should therefore be considered when security is a concern, and to isolate services and sensitive data from externally facing networks.

If services in the DMZ require access to data in the SECURE networks, e.g. such as a Web Server requiring a SQL database back end, then the firewall can be specifically opened to allow **only** the required ports and servers to enable communication between segments.

In the event that your DMZ network is compromised, then the attacker is still isolated from your sensitive data and has limited options for further attack.

Other than security concerns, a multi-tier topology also allows each network segment to be treated in isolation, e.g. each network assigned to a department or team, or to model a customer's existing hierarchy of services or systems. Two network segments can also provide two mutual exclusive environments, with one containing all live services, and the second mirroring the first for pre-production testing and development.

If further guidance is required then please contact the Fujitsu Global Cloud Team for information on the consultancy services offered by Fujitsu.

Contact

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