|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question No | Action | Source | Port | Destination | Port | Flags | Direction | comment |
| 1 | allow | Our DMZ mail gateway | \* | \* | SMTP Submission port (25,465) |  | egress | Assuming this policy (and the next one) is on a firewall that is between the internet and the DMZ, in front of the internal network. The internal network must communicate with the DMZ and beyond via another firewall. |
| 1 | Allow | \* | \* | Our DMZ mail server | SMTP |  | Ingress | Allow any SMTP server, using port 25, or by any client to send emails to our DMZ mail server. |
| 2 | Allow | \* | \* | DMZ Mail Gateway | POP3/POP3S |  | Egress/ingress | This policy should exist on a separate firewall from above between the DMZ and the internal network, where the user authenticates themselves (Egress from internal to DMZ) and Emails are sent to user (Ingress) From the gateway. |
| 3 | Allow | \* | \* | DMZ mail Gateway | POP3S |  | Egress/Ingress | Policy exists on the firewall mentioned in row one. Users must authenticate (Ingress from outside to DMZ) with mail gateway using said protocol, and the mail server can send (Egress) the mail to that user. |
| 4 | Allow | \* | \* | DMZ Web Proxy | 80/443 |  | Egress/ Ingress | This policy exists in the internal firewall (mentioned in row 3) and allows internal network to send and receive web requests/data from/to the DMZ Web proxy. |
| 4 | Allow | DMZ Web Proxy | \* | \* | 80/443 |  | Egress/ Ingress | This ruleset exists in the external firewall that is between DMZ and the internet, where any web host can communicate with the DMZ web proxy. The proxy can then relay these messages to the client using the previous ruleset. |
| 5 | Allow | \* | DNS | DMZ DNS Server | DNS |  | Egress/Ingress | Internal firewall ruleset where the user can query the DMZ DNS Server. This server can also reply to the user with information, on the same port. |
| 5 | Allow | DMZ DNS Server | DNS | \* | DNS |  | Egress/Ingress | External firewall ruleset that allows the DNS server to query the internet and receive DNS records. |
| 6 | Allow | \* | DNS | DMZ DNS Server | DNS |  | Egress/Ingress | External firewall ruleset that allows DNS server to respond to DNS queries from the internet. |

* External firewall refers to the firewall between the internet and the DMZ servers
* Internal firewall refers to the firewall between DMZ and the internal network.