

**Custom Firewall Configuration**

|  |  |  |  |
| --- | --- | --- | --- |
| **Account** | cavbrem | **Date** | 21/03/13 |

**Introduction**

This document is used to define security rules for your custom firewall. Please complete the attached Inbound and Outbound Firewall Rules sheets and return once completed to Web Drive for implementation. Should you require further changes to your custom firewall after implementation, standard charges will apply. If you require assistance in completing this document, please email Web Drive Support (support@webdrive.co.nz) or contact your account manager.

**Inbound Firewall Rules**

Inbound rules are for connections **from** “the internet” or specific IP addresses destined for your server(s). Examples include HTTP access from the internet or SSH / Remote Desktop access from your office. The standard firewall configuration blocks ALL inbound connections. The comment column can be used to specify any additional information you feel is pertinent to your firewall configuration.

|  |  |
| --- | --- |
| *Source Address:* | This is the IP address(es) that connections will come from. If connections should be allowed from anywhere, please use ‘ANY’ in the source address column. You may specify a range of IP addresses to allow if required (for example 119.47.119.1 - 119.47.119.8 or 119.47.119.1/29) |
| *Destination Address:* | This is the IP address(es) that connections are destined for. In most cases this is the IP address of your server or another IP address that has been assigned to you. If connections should be allowed to all of your IP addresses or servers, please use ‘ANY’ in the destination address column. |
| *Port:* | This is the port number that connections will be made to. For example if you wish to allow incoming HTTP access to your website, specify ’80’ in the port column. If you do not know the port number you require, please simply put the name of the service you wish to allow (for example HTTPS) |

**Outbound Firewall Rules**

Outbound rules are for connections **to** “the internet” or specific IP addresses. Examples include FTP access to a remote backup server or SMTP if you are running a mail server. The standard firewall configuration blocks ALL outbound connections. The comment column can be used to specify any additional information you feel is pertinent to your firewall configuration.

|  |  |
| --- | --- |
| *Source Address:* | This is the IP address(es) that connections will come from. In most cases this is the IP address of your server or another IP address that has been assigned to you. If connections should be allowed from all of your IP addresses or servers, please use ‘ANY’ in the source address column. |
| *Destination Address:* | This is the IP address(es) that connections are destined for. If connections should be allowed to anywhere, please use ‘ANY’ in the source address column. You may specify a range of IP addresses to allow if required (for example 119.47.119.1 - 119.47.119.8 or 119.47.119.1/29) |
| *Port:* | This is the port number that connections will be made to. For example if you wish to allow outbound SSH access to a remote server, specify ’22’ in the port column. If you do not know the port number you require, please simply put the name of the service you wish to allow (for example HTTPS) |

**Inbound Firewall Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rule** | **Source Address** | **To Address** | **Port** | **Comments** |
| Example | 192.168.1.1 | 192.168.100.1 | 80 | HTTP access from my office to my server |
| 1 | Web Drive Management | Internal | Various | Web Drive Standard Ruleset (SSH/RDP/SNMP/Monitoring) |
| 2 | Any | Cavbrem-app-internal | 21 | FTP |
| 3 | Any | Cavbrem-app-internal | 80/443 | HTTP/HTTPS |
| 4 | Any | Internal Network | 3389 | Remote Desktop |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 |  |  |  |  |
| 18 |  |  |  |  |
| 19 |  |  |  |  |
| 20 |  |  |  |  |

**Outbound Firewall Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rule** | **Source Address** | **To Address** | **Port** | **Comments** |
| Example | 192.168.100.1 | ANY | 25 | SMTP access from my server to the internet |
| 1 | Internal | Various | Various | Web Drive Standard Ruleset (DNS/SMTP/NTP/Windows Updates) |
| 2 | Cavbrem-app-internal | Any | 80/443 | Outbound HTTP/HTTPS initiated from cavbrem-app server |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 |  |  |  |  |
| 18 |  |  |  |  |
| 19 |  |  |  |  |
| 20 |  |  |  |  |