Firewall Configuration File Supported Customizations

In order to support any 3rd party firewall vendor, we do not do any error checking on supplied firewall configuration files. The firewall configuration file supplied must be in a format supported by your firewall vendor. The firewall vendor must also support the firewalls configuration being loaded using the AWS EC2 `User data` capabilities. If your firewall vendor does not support loading its configuration in this manner, the Accelerator can still deploy the firewall AMI, but it will contain no pre-loaded configuration. Users will need to configure the firewall post-installation.

- Before feeding the provided configuration file to the firewall during deployment, the Accelerator will replace the below variables
- The currently provided sample configuration file is for a Fortinet Fortigate firewall
- Key firewall selection characteristics:
  - Active/Active firewall configuration using BGP and ECMP
  - Unicast layer 3 firewall clustering capabilities (no multicast requirement)
  - Support for NAT rules targeting DNS names rather than IP address

Notes:

- The variables and values are reflective of the sample configuration file for the first AZ
- For example:
  - Variable names change based on subnet names
  - Variable values change based on subnet names, fw instance (i.e. AZ), etc.
- In our example:
  - Interface 1 is: Public
  - Interface 2 is: OnPremise
  - Interface 3 is: FWMgmt
  - Interface 4 is: Proxy
  - Source templatePath: firewall/firewall-example.txt
  - Boot outputPath: fgtconfig-init-Firewall_azA-0.txt

Supported Replacement Variables and Sample Values:

Variable	Value
${Hostname}	Firewall_azA
VPC Info	-
${VpcMask}	255.255.252.0
${VpcCidr}	10.7.4.0/22
${VpcNetworkIp}	10.7.4.0
${VpcRouterIp}	10.7.4.1
${VpcMask2}	255.255.254.0
${VpcCidr2}	100.96.250.0/23

Variable	Value
${VpcNetworkIp2}	100.96.250.0
${VpcRouterIp2}	100.96.250.1
Subnet 1 Info	-
${PublicIp1}	FirewallInstance0Eni-PrimaryPrivateIpAddress
${PublicNetworkIp}	100.96.250.0
${PublicRouterIp}	100.96.250.1
${PublicCidr}	100.96.250.0/25
${PublicMask}	255.255.255.128
Tunnel1	-
${PublicCgwTunnelOutsideAddress1}	35.182.44.198
${PublicCgwTunnelInsideAddress1}	169.254.251.78
${PublicCgwBgpAsn1}	”65523”
${PublicVpnTunnelOutsideAddress1}	52.60.81.49
${PublicVpnTunnelInsideAddress1}	169.254.251.77
${PublicVpnBgpAsn1}	”65521”
${PublicPreSharedSecret1}	the-secret
Tunnel2	-
${PublicCgwTunnelOutsideAddress2}	3.97.104.182
${PublicCgwTunnelInsideAddress2}	169.254.76.153
${PublicCgwBgpAsn2}	”65523”
${PublicVpnTunnelOutsideAddress2}	52.60.103.19
${PublicVpnTunnelInsideAddress2}	169.254.76.154
${PublicVpnBgpAsn2}	”65521”
${PublicPreSharedSecret2}	the-secret
Subnet 2 Info	-
${OnPremiseIp1}	FirewallInstance0Eni-PrimaryPrivateIpAddress
${OnPremiseNetworkIp}	100.96.251.0
${OnPremiseRouterIp}	100.96.251.1
${OnPremiseCidr}	100.96.251.0/27
${OnPremiseMask}	255.255.255.224
Subnet 3 Info	-
${FWMgmtIp1}	FirewallInstance0Eni-PrimaryPrivateIpAddress
${FWMgmtNetworkIp}	100.96.251.32
${FWMgmtRouterIp}	100.96.251.33
${FWMgmtCidr}	100.96.251.32/27
${FWMgmtMask}	255.255.255.224
Subnet 4 Info	-
${ProxyIp1}	FirewallInstance0Eni-PrimaryPrivateIpAddress
${ProxyNetworkIp}	100.96.251.64
${ProxyRouterIp}	100.96.251.65
${ProxyCidr}	100.96.251.64/26
${ProxyMask}	255.255.255.192

...Return to Customization Table of Contents