```
# A template for creating a Google Cloud project to protect any web service hosted on any platform.
# Utilizees Load Balancing, Cloud CDN, and Cloud Armor for in-depth DDoS defense and performance boosting.


# Make sure to replace the following values with your own:
# - project_id (replace "shield-blog-example" with your desired project ID)
# - project_name (replace "shield-blog-example" with your desired project name)
# - billing_account (replace "012345-ABCDEF-678901" with your billing account)
# - origin address (replace "8.8.8.8" with your origin address)
# - ip_address (replace "1.2.3.4" with your desired IP address, or leave blank to auto-assign one.)


resource "google_project" "shield_blog_example" # Replace this with your desired project ID {
auto_create_network = true
billing_account = "012345-ABCDEF-678901" # Replace this with your billing account
name = "shield-blog-example" # Replace this with your desired project name
project_id = "shield-blog-example" # Replace this with your desired project ID
}
# terraform import google_project.shield_blog_example projects/shield-blog-example
resource "google_compute_backend_service" "my_http_bes" {
cdn_policy {
cache_key_policy {
include_host = true
include_protocol = true
include_query_string = true
}
cache_mode = "CACHE_ALL_STATIC"
client_ttl = 3600
default_ttl = 3600
max_ttl = 86400
signed_url_cache_max_age_sec = 0
}
connection_draining_timeout_sec = 0
```

```
enable_cdn = true
load_balancing_scheme = "EXTERNAL_MANAGED"
locality_lb_policy = "ROUND_ROBIN"
name = "my-http-bes"
port_name = "http"
project = "shield-blog-example"
protocol = "HTTP"
security_policy = "https://www.googleapis.com/compute/beta/projects/shield-blog-example/global/securityPolicies/default-security-policy-for-backend-service-my-http-bes"
session_affinity = "NONE"
timeout_sec = 30
}
# terraform import google_compute_backend_service.my_http_bes projects/shield-blog-example/global/backendServices/my-http-bes
resource "google_compute_backend_service" "my_https_bes" {
cdn_policy {
cache_key_policy {
include_host = true
include_protocol = true
include_query_string = true
}
cache_mode = "CACHE_ALL_STATIC"
client_ttl = 3600
default_ttl = 3600
max_ttl = 86400
signed_url_cache_max_age_sec = 0
}
connection_draining_timeout_sec = 0
enable_cdn = true
load_balancing_scheme = "EXTERNAL_MANAGED"
locality_lb_policy = "ROUND_ROBIN"
name = "my-https-bes"
port_name = "http"
project = "shield-blog-example"
```

```
protocol = "HTTPS"
security_policy = "https://www.googleapis.com/compute/beta/projects/shield-blog-example/global/securityPolicies/default-security-policy-for-backend-service-my-http-bes"
session_affinity = "NONE"
timeout_sec = 30
}
# terraform import google_compute_backend_service.my_https_bes projects/shield-blog-example/global/backendServices/my-https-bes
resource "google_compute_firewall" "default_allow_internal" {
allow {
ports = ["0-65535"]
protocol = "tcp"
}
allow {
ports = ["0-65535"]
protocol = "udp"
}
allow {
protocol = "icmp"
}
description = "Allow internal traffic on the default network"
direction = "INGRESS"
name = "default-allow-internal"
network = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/networks/default"
priority = 65534
project = "shield-blog-example"
source_ranges = ["10.128.0.0/9"]
}
# terraform import google_compute_firewall.default_allow_internal projects/shield-blog-example/global/firewalls/default-allow-internal
resource "google_compute_firewall" "default_allow_ssh" {
allow {
ports = ["22"]
protocol = "tcp"
}
```

```
description = "Allow SSH from anywhere"
direction = "INGRESS"
name = "default-allow-ssh"
network = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/networks/default"
priority = 65534
project = "shield-blog-example"
source_ranges = ["0.0.0.0/0"]
}
# terraform import google_compute_firewall.default_allow_ssh projects/shield-blog-example/global/firewalls/default-allow-ssh
resource "google_compute_firewall" "default_allow_icmp" {
allow {
protocol = "icmp"
}
description = "Allow ICMP from anywhere"
direction = "INGRESS"
name = "default-allow-icmp"
network = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/networks/default"
priority = 65534
project = "shield-blog-example"
source_ranges = ["0.0.0.0/0"]
}
# terraform import google_compute_firewall.default_allow_icmp projects/shield-blog-example/global/firewalls/default-allow-icmp
resource "google_compute_global_forwarding_rule" "my_http_lb" {
ip_address = "1.2.3.4" # Replace this with your desired IP address, or leave blank to auto-assign one.
ip_protocol = "TCP"
load_balancing_scheme = "EXTERNAL_MANAGED"
name = "my-http-lb"
port_range = "80-80"
project = "shield-blog-example"
target = "https://www.googleapis.com/compute/beta/projects/shield-blog-example/global/targetHttpProxies/my-http-lb-target-proxy"
}
# terraform import google_compute_global_forwarding_rule.my_http_lb projects/shield-blog-example/global/forwardingRules/my-http-lb
resource "google_compute_global_forwarding_rule" "my_https_lb" {
```

```
ip_address = "1.2.3.4" # Replace this with your desired IP address, or leave blank to auto-assign one.
ip_protocol = "TCP"
load_balancing_scheme = "EXTERNAL_MANAGED"
name = "my-https-lb"
port_range = "443-443"
project = "shield-blog-example"
target = "https://www.googleapis.com/compute/beta/projects/shield-blog-example/global/targetHttpsProxies/my-https-lb-target-proxy"
}
# terraform import google_compute_global_forwarding_rule.my_https_lb projects/shield-blog-example/global/forwardingRules/my-https-lb
resource "google_compute_firewall" "default_allow_rdp" {
allow {
ports = ["3389"]
protocol = "tcp"
}
description = "Allow RDP from anywhere"
direction = "INGRESS"
name = "default-allow-rdp"
network = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/networks/default"
priority = 65534
project = "shield-blog-example"
source_ranges = ["0.0.0.0/0"]
}
# terraform import google_compute_firewall.default_allow_rdp projects/shield-blog-example/global/firewalls/default-allow-rdp
resource "google_compute_global_address" "my_lb_static_ip" {
address = "1.2.3.4" # Replace this with your desired IP address, or leave blank to auto-assign one.
address_type = "EXTERNAL"
ip_version = "IPV4"
name = "my-lb-static-ip"
project = "shield-blog-example"
}
# terraform import google_compute_global_address.my_lb_static_ip projects/shield-blog-example/global/addresses/my-lb-static-ip
resource "google_compute_ssl_certificate" "my_cert" {
name = "my-cert"
```

```
project = "shield-blog-example"
}
# terraform import google_compute_ssl_certificate.my_cert projects/shield-blog-example/global/sslCertificates/my-cert
resource "google_compute_security_policy" "default_security_policy_for_backend_service_my_http_bes" {
adaptive_protection_config {
layer7_ddos_defense_config {
enable = true
}
}
advanced_options_config {
json_parsing = "DISABLED"
}
description = "Default security policy for: my-http-bes"
name = "default-security-policy-for-backend-service-my-http-bes"
project = "shield-blog-example"
rule {
action = "allow"
match {
config {
src_ip_ranges = ["*"]
}
versioned_expr = "SRC_IPS_V1"
}
priority = 2147483647
}
rule {
action = "deny(403)"
match {
expr {
expression = "evaluateAdaptiveProtectionAutoDeploy()"
}
}
priority = 0
```

```
}
rule {
action = "throttle"
description = "Default rate limiting rule"
match {
config {
src_ip_ranges = ["*"]
}
versioned_expr = "SRC_IPS_V1"
}
priority = 2147483646
rate_limit_options {
conform_action = "allow"
enforce_on_key = "IP"
exceed_action = "deny(403)"
rate_limit_threshold {
count = 500
interval_sec = 60
}
}
}
type = "CLOUD_ARMOR"
}
# terraform import google_compute_security_policy.default_security_policy_for_backend_service_my_http_bes projects/shield-blog-example/
global/securityPolicies/default-security-policy-for-backend-service-my-http-bes
resource "google_compute_target_http_proxy" "my_http_lb_target_proxy" {
name = "my-http-lb-target-proxy"
project = "shield-blog-example"
url_map = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/urlMaps/my-http-lb"
}
# terraform import google_compute_target_http_proxy.my_http_lb_target_proxy projects/shield-blog-example/global/targetHttpProxies/my-
http-lb-target-proxy
resource "google_compute_target_https_proxy" "my_https_lb_target_proxy" {
```

```
name = "my-https-lb-target-proxy"
project = "shield-blog-example"
quic_override = "NONE"
ssl_certificates = ["https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/sslCertificates/my-cert"]
url_map = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/urlMaps/my-https-lb"
}
# terraform import google_compute_target_https_proxy.my_https_lb_target_proxy projects/shield-blog-example/global/targetHttpsProxies/my-https-lb-target-proxy
resource "google_compute_url_map" "my_http_lb" {
default_service = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/backendServices/my-http-bes"
name = "my-http-lb"
project = "shield-blog-example"
}
# terraform import google_compute_url_map.my_http_lb projects/shield-blog-example/global/urlMaps/my-http-lb
resource "google_compute_url_map" "my_https_lb" {
default_service = "https://www.googleapis.com/compute/v1/projects/shield-blog-example/global/backendServices/my-https-bes"
name = "my-https-lb"
project = "shield-blog-example"
}
# terraform import google_compute_url_map.my_https_lb projects/shield-blog-example/global/urlMaps/my-https-lb


### BELOW THIS LINE ARE SERVICES THAT ARE REQUIRED TO BE ENABLED IN THE PROJECT.
### THESE SERVICES ARE NOT DIRECTLY RELATED TO THE NETWORKING SETUP
resource "google_project_service" "serviceusage_googleapis_com" {
project = "148336249154"
service = "serviceusage.googleapis.com"
}
# terraform import google_project_service.serviceusage_googleapis_com 148336249154/serviceusage.googleapis.com
resource "google_project_service" "dataplex_googleapis_com" {
project = "148336249154"
service = "dataplex.googleapis.com"
}
```

```
# terraform import google_project_service.dataplex_googleapis_com 148336249154/dataplex.googleapis.com
resource "google_project_service" "dataform_googleapis_com" {
project = "148336249154"
service = "dataform.googleapis.com"
}
# terraform import google_project_service.dataform_googleapis_com 148336249154/dataform.googleapis.com
resource "google_project_service" "storage_googleapis_com" {
project = "148336249154"
service = "storage.googleapis.com"
}
# terraform import google_project_service.storage_googleapis_com 148336249154/storage.googleapis.com
resource "google_project_service" "oslogin_googleapis_com" {
project = "148336249154"
service = "oslogin.googleapis.com"
}
# terraform import google_project_service.oslogin_googleapis_com 148336249154/oslogin.googleapis.com
resource "google_project_service" "monitoring_googleapis_com" {
project = "148336249154"
service = "monitoring.googleapis.com"
}
# terraform import google_project_service.monitoring_googleapis_com 148336249154/monitoring.googleapis.com
resource "google_project_service" "cloudapis_googleapis_com" {
project = "148336249154"
service = "cloudapis.googleapis.com"
}
# terraform import google_project_service.cloudapis_googleapis_com 148336249154/cloudapis.googleapis.com
resource "google_project_service" "servicemanagement_googleapis_com" {
project = "148336249154"
service = "servicemanagement.googleapis.com"
}
# terraform import google_project_service.servicemanagement_googleapis_com 148336249154/servicemanagement.googleapis.com
resource "google_service_account" "148336249154_compute" {
account_id = "148336249154-compute"
```

```
display_name = "Compute Engine default service account"
project = "shield-blog-example"
}
# terraform import google_service_account.148336249154_compute projects/shield-blog-example/serviceAccounts/148336249154-
compute@shield-blog-example.iam.gserviceaccount.com
resource "google_logging_log_sink" "a_required" {
destination = "logging.googleapis.com/projects/shield-blog-example/locations/global/buckets/_Required"
filter = "LOG_ID(\"cloudaudit.googleapis.com/activity\") OR LOG_ID(\"externalaudit.googleapis.com/activity\") OR
LOG_ID(\"cloudaudit.googleapis.com/system_event\") OR LOG_ID(\"externalaudit.googleapis.com/system_event\") OR
LOG_ID(\"cloudaudit.googleapis.com/access_transparency\") OR LOG_ID(\"externalaudit.googleapis.com/access_transparency\")"
name = "_Required"
project = "148336249154"
unique_writer_identity = true
}
# terraform import google_logging_log_sink.a_required 148336249154###_Required
resource "google_logging_log_sink" "a_default" {
destination = "logging.googleapis.com/projects/shield-blog-example/locations/global/buckets/_Default"
filter = "NOT LOG_ID(\"cloudaudit.googleapis.com/activity\") AND NOT LOG_ID(\"externalaudit.googleapis.com/activity\") AND NOT
LOG_ID(\"cloudaudit.googleapis.com/system_event\") AND NOT LOG_ID(\"externalaudit.googleapis.com/system_event\") AND NOT
LOG_ID(\"cloudaudit.googleapis.com/access_transparency\") AND NOT LOG_ID(\"externalaudit.googleapis.com/access_transparency\")"
name = "_Default"
project = "148336249154"
unique_writer_identity = true
}
# terraform import google_logging_log_sink.a_default 148336249154###_Default
resource "google_project_service" "storage_api_googleapis_com" {
project = "148336249154"
service = "storage-api.googleapis.com"
}
# terraform import google_project_service.storage_api_googleapis_com 148336249154/storage-api.googleapis.com
resource "google_project_service" "compute_googleapis_com" {
project = "148336249154"
service = "compute.googleapis.com"
```

```
}
# terraform import google_project_service.compute_googleapis_com 148336249154/compute.googleapis.com
resource "google_project_service" "logging_googleapis_com" {
project = "148336249154"
service = "logging.googleapis.com"
}
# terraform import google_project_service.logging_googleapis_com 148336249154/logging.googleapis.com
```