Transitioning from Appliance to Container Gateway

Gary Vermeulen – Layer7 Platform Architect

September 13, 2022

Disclaimer

Certain information in this presentation may outline the general product direction of CA Technologies, a Broadcom Company (CA). This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of December 2019 and **is subject to change or withdrawal by CA at any time without notice**. **The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion**.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

Copyright © 2021 CA Technologies, a Broadcom Company. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

BROADCOM®

Transitioning from Appliance to Container Gateway

- What is the Container Gateway?

- Migration, Expansion or Green Field

- **Key Differences** between the Appliance and Container Gateway

- The Gateway Helm Chart
  - Network Topology
  - Port Configuration

- Basic Migration Process

BROADCOM®

Migration, Expansion or Green Field

It's unlikely that the role of your appliance gateways will change overnight. They represent a significant investment of time and resources.

- Migration
  - Migrating your entire Layer7 API Gateway estate.
  - Best done in parallel with your existing environment

- Expansion
  - Expanding into Kubernetes to take advantage of fast provisioning and scaling.
  - The Gateway Helm Chart allows you to configure a HPA (Horizontal Pod Autoscaler)

- Green field
  - Taking advantage of the Gateway's features to secure new applications and or microservices in Kubernetes.
  - May be a good use case for running the Gateway in Ephemeral mode.

BROADCOM®

What is the Container Gateway?

The Container Gateway is a slimmed down, platform agnostic, containerized version of the Layer7 API Gateway. It's around 700 MB uncompressed, currently runs on Centos7 and is available on DockerHub.

caapim/gateway ☆

By caapim • Updated 5 days ago

CA API Gateway

Image

BROADCOM®

Key Differences

The biggest benefit of using the Container Gateway vs. Appliance is **time**. That relates to **provisioning**, **maintenance (patches), scaling** and **upgrades**.
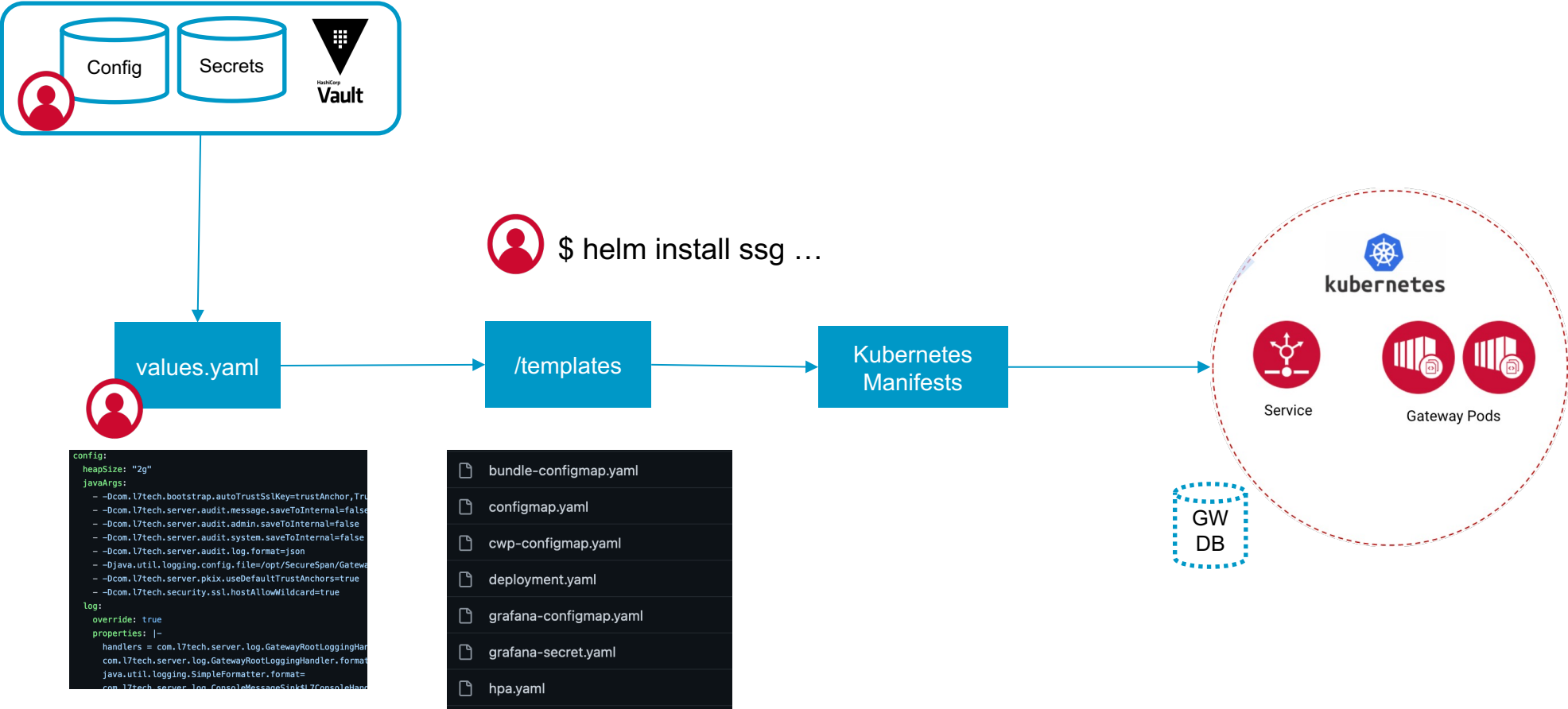
- Architectural Differences
  - No included MySQL
  - Single Network Interface
  - Limited access to the underlying host
  - Full list

- Operational Differences
  - Administration
  - Logging
  - Metrics
  - Debugging
  - Custom Assertions/Java Libraries
  - Full list

- Thinking in Kubernetes
- Logging/Audits/Metrics Office Hours

BROADCOM®

Gateway Helm Chart

Config   Secrets   HashiCorp Vault

$ helm install ssg …

kubernetes

Service   Gateway Pods

values.yaml → /templates → Kubernetes Manifests →

GW DB

```
config:
  heapSize: "2g"
  javaArgs:
    - -Dcom.l7tech.bootstrap.autoTrustSslKey=trustAnchor,Tru
    - -Dcom.l7tech.server.audit.message.saveToInternal=false
    - -Dcom.l7tech.server.audit.admin.saveToInternal=false
    - -Dcom.l7tech.server.audit.system.saveToInternal=false
    - -Dcom.l7tech.server.audit.log.format=json
    - -Djava.util.logging.config.file=/opt/SecureSpan/Gatewa
    - -Dcom.l7tech.server.pkix.useDefaultTrustAnchors=true
    - -Dcom.l7tech.security.ssl.hostAllowWildcard=true
  log:
    override: true
    properties: |-
      handlers = com.l7tech.server.log.GatewayRootLoggingHan
      com.l7tech.server.log.GatewayRootLoggingHandler.format
      java.util.logging.SimpleFormatter.format=
      com.l7tech.server.log.ConsoleMessageSink$L7ConsoleHan
```

- bundle-configmap.yaml
- configmap.yaml
- cwp-configmap.yaml
- deployment.yaml
- grafana-configmap.yaml
- grafana-secret.yaml
- hpa.yaml

BROADCOM®

Gateway Helm Chart

The Gateway Helm Chart was first released in 2020 and represents a supported Container Gateway deployment method.

- Simplified Gateway configuration (everything driven via a single configuration file).

- Separation of duty - each release can be independently maintained with its own configuration.

- Deployment and Upgrades can be integrated into CI/CD workflows making them repeatable and predictable.

- Configurable auto-scaling

- Creation of non prod/test environments is fast and simple

BROADCOM®

Network Topology

|
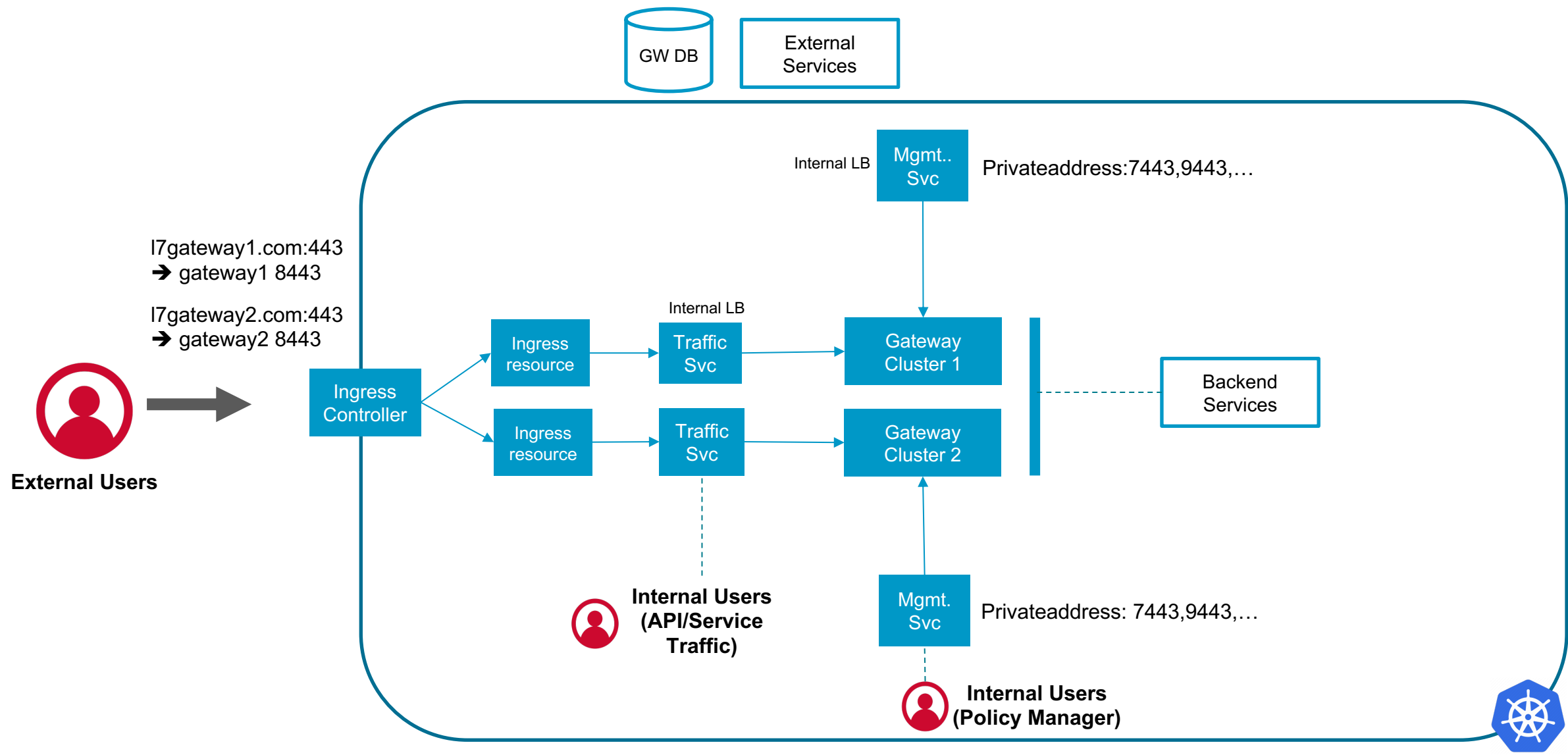
Network Topology
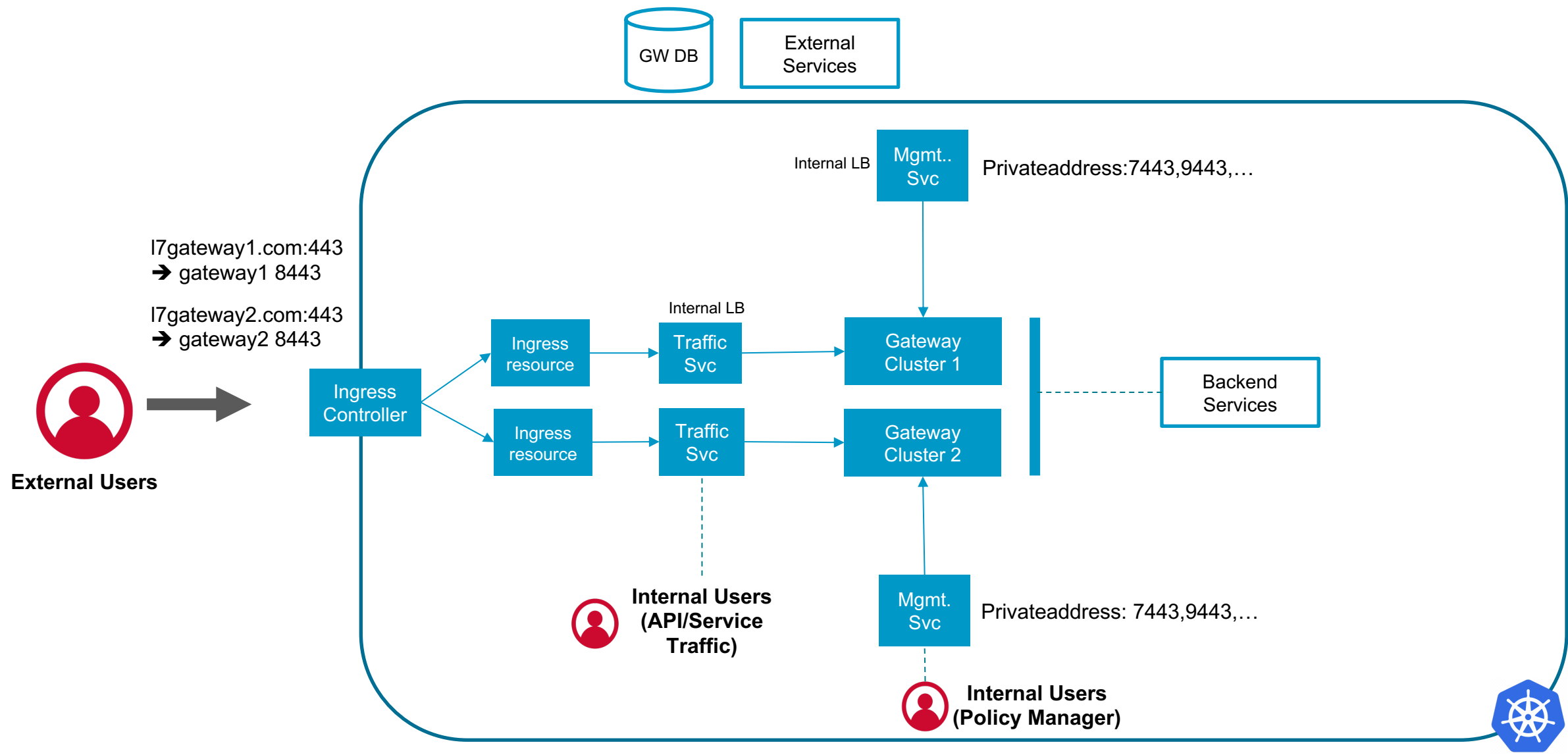
Port Configuration

Container Level

Traffic Svc

service.type would be LoadBalancer (with the Azure Internal annotation)

```
service:
  type: ClusterIP
  annotations: {}
  ports:
    - name: https
      internal: 8443
      external: 8443
      protocol: TCP
```
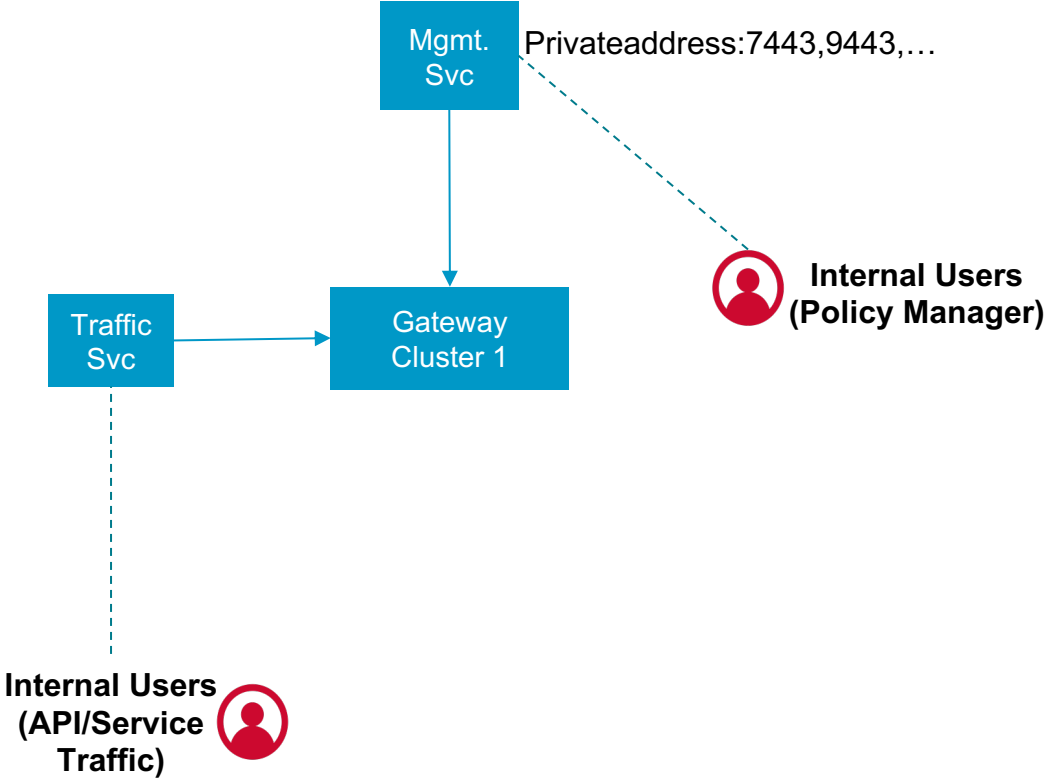
Mgmt. Svc

```
management:
...
  service:
    enabled: true
    type: LoadBalancer
    annotations: {}
      # cloud.google.com/load-balancer-type: "Internal"
      # service.beta.kubernetes.io/azure-load-balancer-internal: "true"
    ports:
      - name: management
        internal: 9443
        external: 9443
        protocol: TCP
```
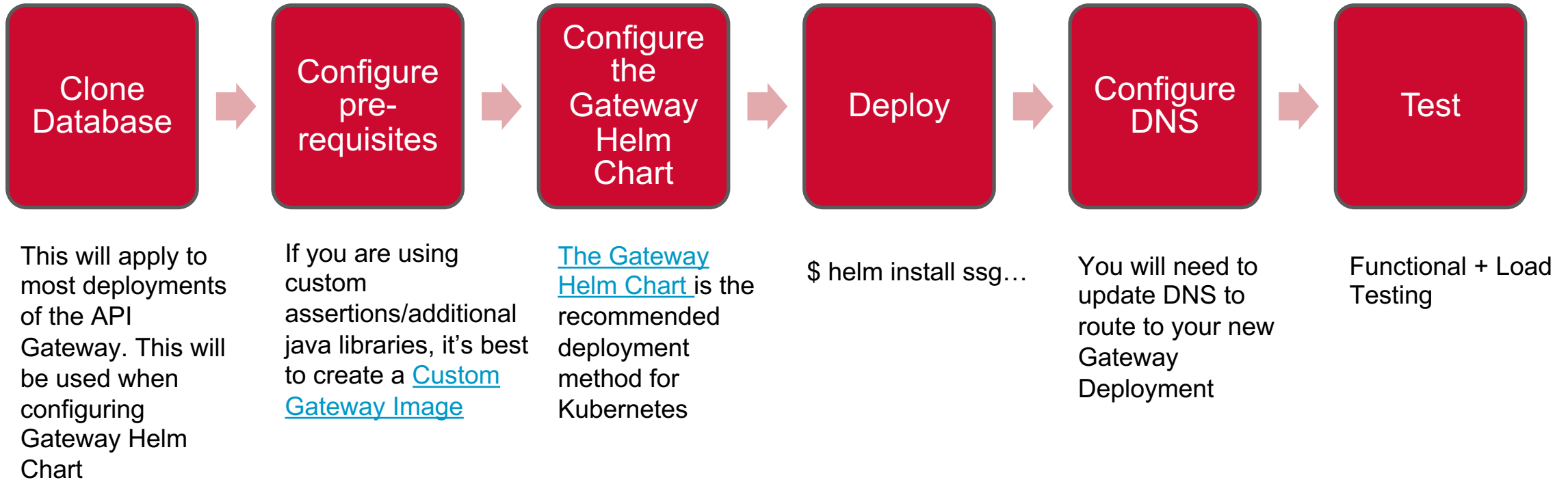
App Level

Gateway Cluster

```
config:
...
  listenPorts:
    custom:
      enabled: true
    ports:
      - name: Default HTTPS (8443)
        port: 8443
        enabled: true
        protocol: HTTPS
        managementFeatures:
        - Published service message input
        # - Administrative access
        # - Browser-based administration
        # - Built-in services
        properties:
        - name: server
          value: A
        tls:
          enabled: true
          clientAuthentication: Optional
          versions:
          #- TLSv1.0
          #- TLSv1.1
          - TLSv1.2
          - TLSv1.3
          cipherSuites:
          - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

Mgmt. Svc

Privateaddress:7443,9443,…

Traffic Svc → Gateway Cluster 1

Internal Users (Policy Manager)

Internal Users (API/Service Traffic)

BROADCOM®

Basic Migration Process

Clone Database	→	Configure pre-requisites	→	Configure the Gateway Helm Chart	→	Deploy	→	Configure DNS	→	Test

This will apply to most deployments of the API Gateway. This will be used when configuring Gateway Helm Chart

If you are using custom assertions/additional java libraries, it's best to create a Custom Gateway Image

The Gateway Helm Chart is the recommended deployment method for Kubernetes

$ helm install ssg…

You will need to update DNS to route to your new Gateway Deployment

Functional + Load Testing

BROADCOM®

Thank you

BROADCOM®
SOFTWARE