Servicios Transversales para IaaS

Agenda

- Catálogo de Servicios

Agenda

- Catálogo de Servicios
- Arquitectura de Referencia

Agenda

- Catálogo de Servicios
- Arquitectura de Referencia
- Servicios Transversales

Catálogo de Servicios

- Oferta Básica:
    - Data Center Virtual
    - Red Privada
    - Internet Segura
    - Catálogos públicos
    - Baas
    - WAF
    - Syslog
    - Certificados HTTPS
    - Servicios Profesionales (SSPP, 60 hrs)

Catálogo de Servicios

- Oferta Adicional:
    - Redes Privadas
    - Monitoreo Customizados en Zabbix
    - Dashboard Customizados de ELK
    - Adicionales BaaS
    - FSaaS
    - SSPP

Catálogo de Servicios

- Data Center Virtual:
    - CPU (GHz)
    - RAM (GB)
    - Storage (GB)
    - Firewall Virtual (NSX Edge)

Catálogo de Servicios

- Internet Segura:
  - A través de un virtual domain (vDOM) del cluster de firewalls en alta disponibilidad
  - Administrado por Antel
  - 4 IPs públicas
  - Servicios salientes habilitados: HTTP, HTTPS, 8080, DNS, NTP, SMTP e ICMP
  - Servicio entrante: SMTP
- RedUY:
  - Firewall de borde administrado por Agesic, “similar a Internet”

Catálogo de Servicios

- DNS:
  - Alojamiento de zonas autoritativas
  - Portal Web
- NTP:
  - Servicio para sincronizar las VMs del cliente
- Catálogo de Imágenes:
  - Catálogo público de Imágenes
  - Preconfigurado para SSTT
  - Hardening y actualizaciones automatizadas

Catálogo de Servicios

- WAF:
  - Servicios deben ser publicados a través de WAF
  - Administrados por NDG
  - Validados y monitoreados por AGESIC/CERTUy

- HIDS:
  - Detección de intrusiones
  - Detección de uso indebido de software
  - Detección de configuraciones de seguridad débiles
  - Chequeo de integridad de archivos
  - Aumenta la visibilidad de la seguridad de los sistemas

Servicios Transversales

- Monitoreo:
  - Contenedores de Zabbix para el Cliente.
  - Integración con Zabbix para proyectos administrados

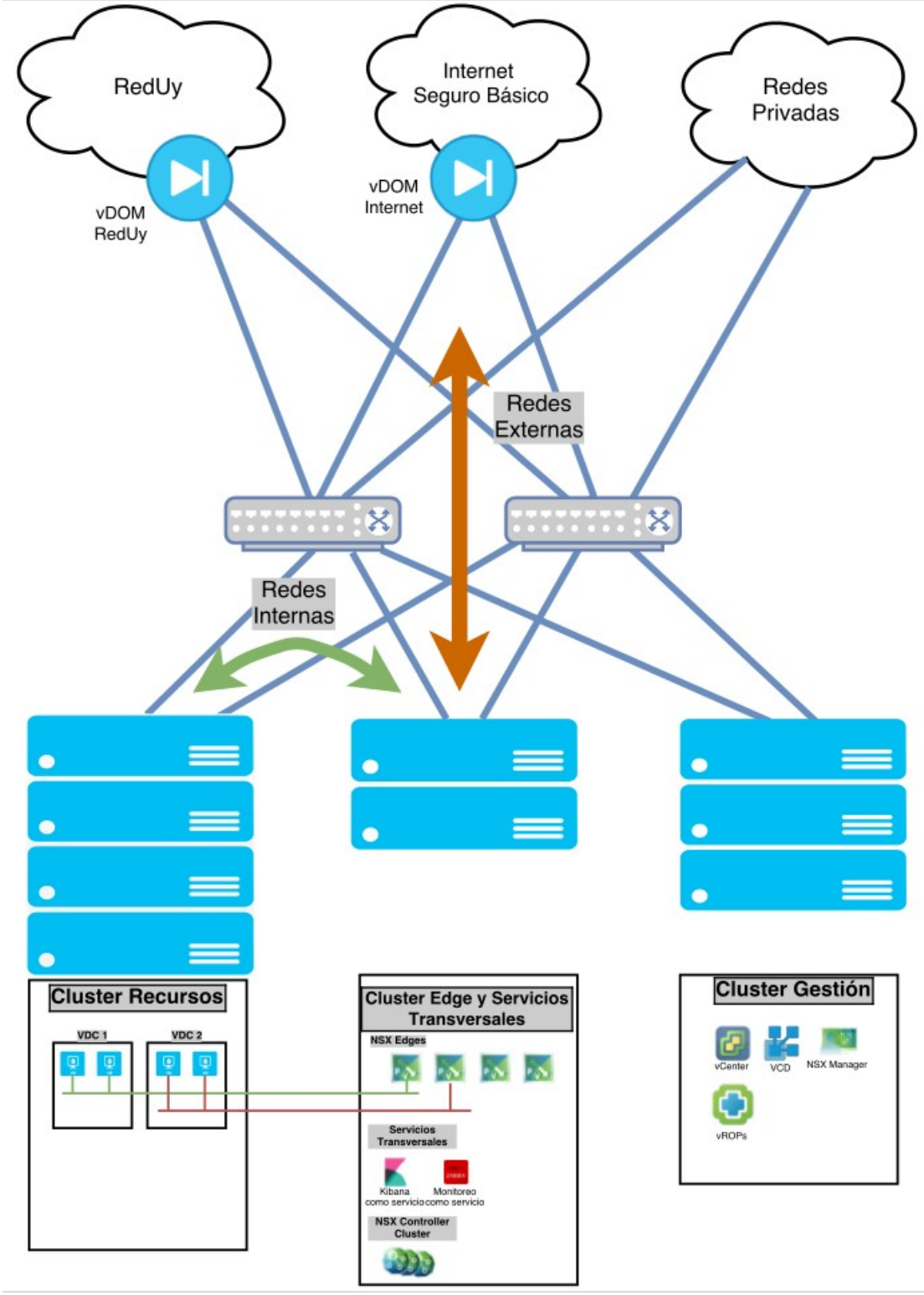
- Syslog:
  - Cluster ELK dockerizado
  - Pipelines y dashboards customizados

Agenda

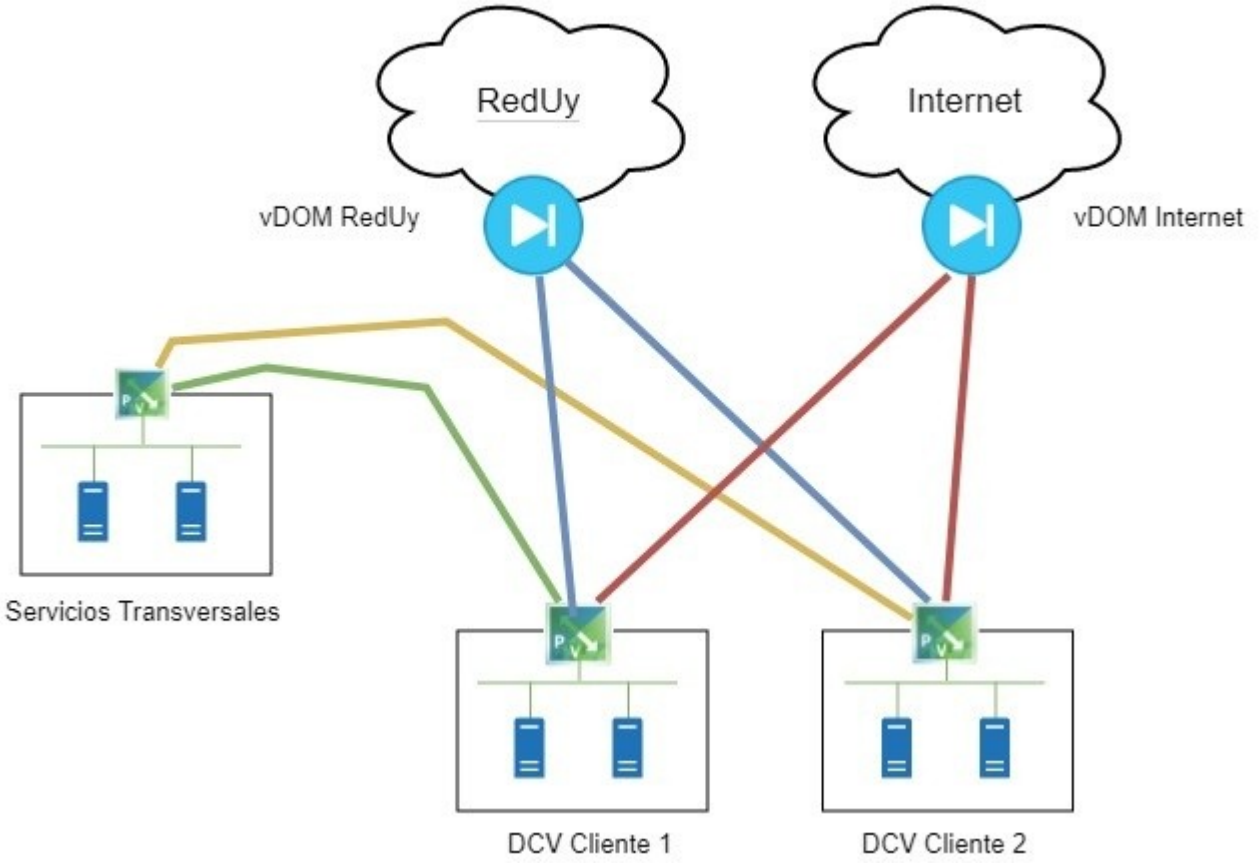
- Catálogo de Servicios
- Arquitectura de Referencia

Infraestructura

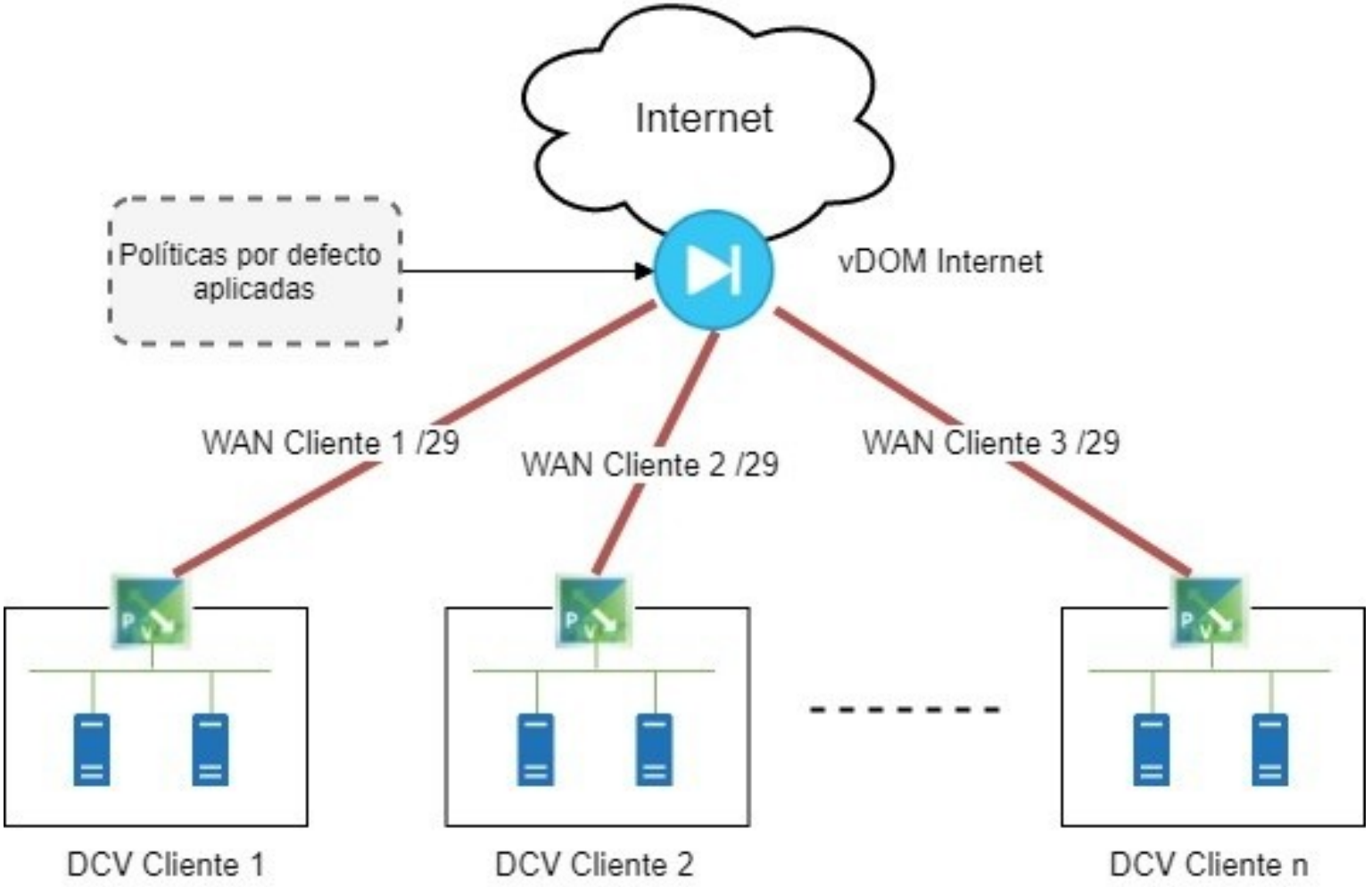
- Cluster de Recursos
- Cluster EDGE y Servicios Transversales
- Cluster de Gestión
- Redes SAN redundantes
- Storage High End


RedUy
Internet
Seguro Básico
Redes
Privadas
vDOM
RedUy
vDOM
Internet
Redes
Externas
Redes
Internas
Cluster Recursos
VDC 1
VDC 2
Cluster Edge y Servicios
Transversales
NSX Edges
Servicios
Transversales
Kibana
como servicio
Monitoreo
como servicio
NSX Controller
Cluster
Cluster Gestión
vCenter
VCD
NSX Manager
vROPs

Redes


RedUy
Internet
vDOM RedUy
vDOM Internet
Servicios Transversales
DCV Cliente 1
DCV Cliente 2

Internet


Internet
Políticas por defecto aplicadas
vDOM Internet
WAN Cliente 1 /29
WAN Cliente 2 /29
WAN Cliente 3 /29
DCV Cliente 1
DCV Cliente 2
DCV Cliente n

Internet

Se asigna para el cliente un rango de direcciones IP /29, que será distribuido de la siguiente forma:

- Una (1) IP, la primera del rango, en el firewall perimetral de la plataforma (gateway del cliente)

- Dos (2) IPs, para los WAF de producción y testing, a través de los que se publican los servicios Web hacia Internet.

- Tres (3) IPs, asignadas en el Edge del Data Center Virtual del cliente para navegación y publicación de otro tipo de servicios.

Red Privada

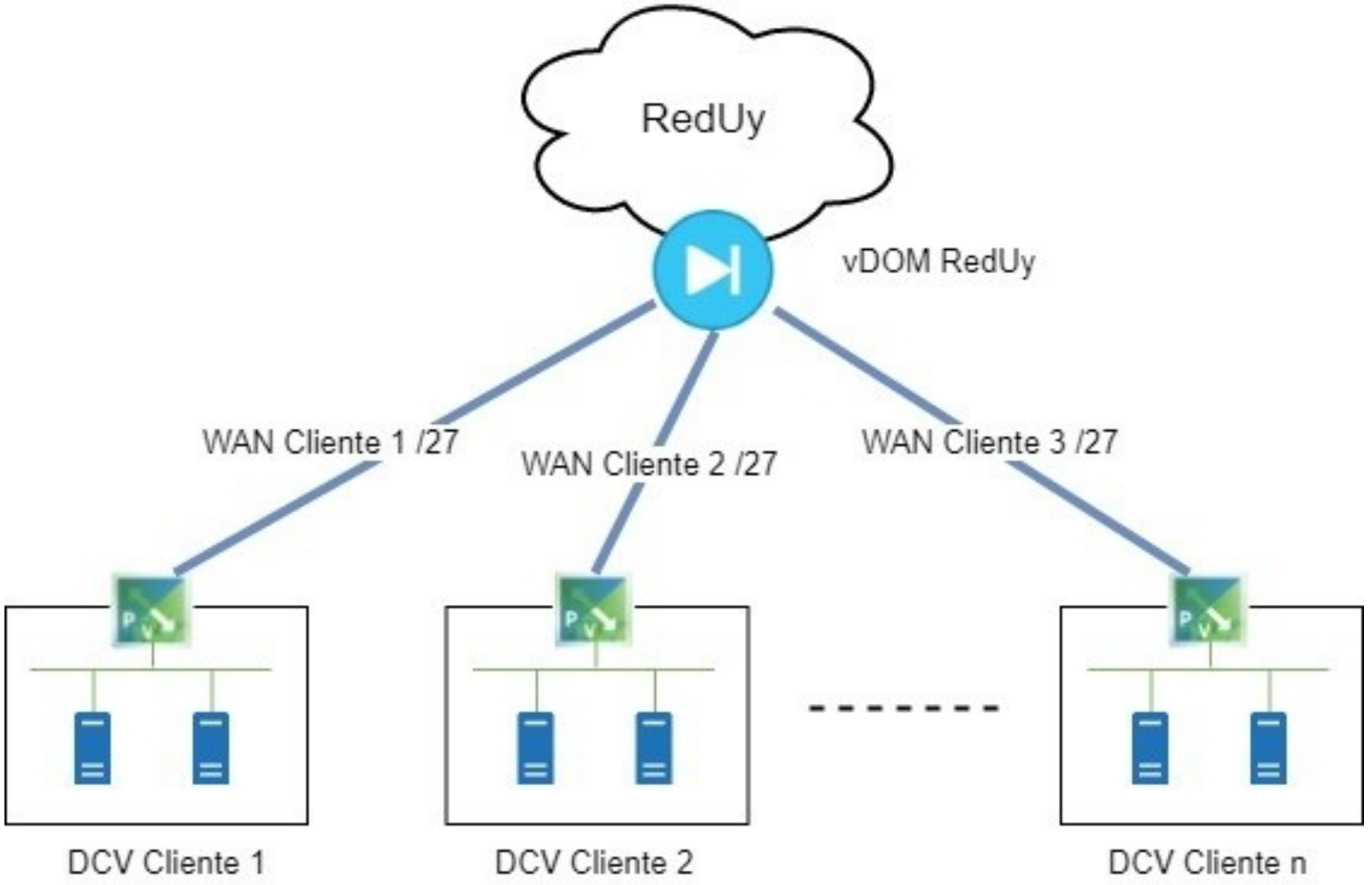
Se asigna para el cliente un rango de direcciones IP /28 dentro del direccionamiento privado de RedUy (10.8.0.0 /16), que será distribuido de la siguiente forma:

- Una (1) IP, la primera del rango, en el firewall perimetral de la plataforma (gateway del cliente)

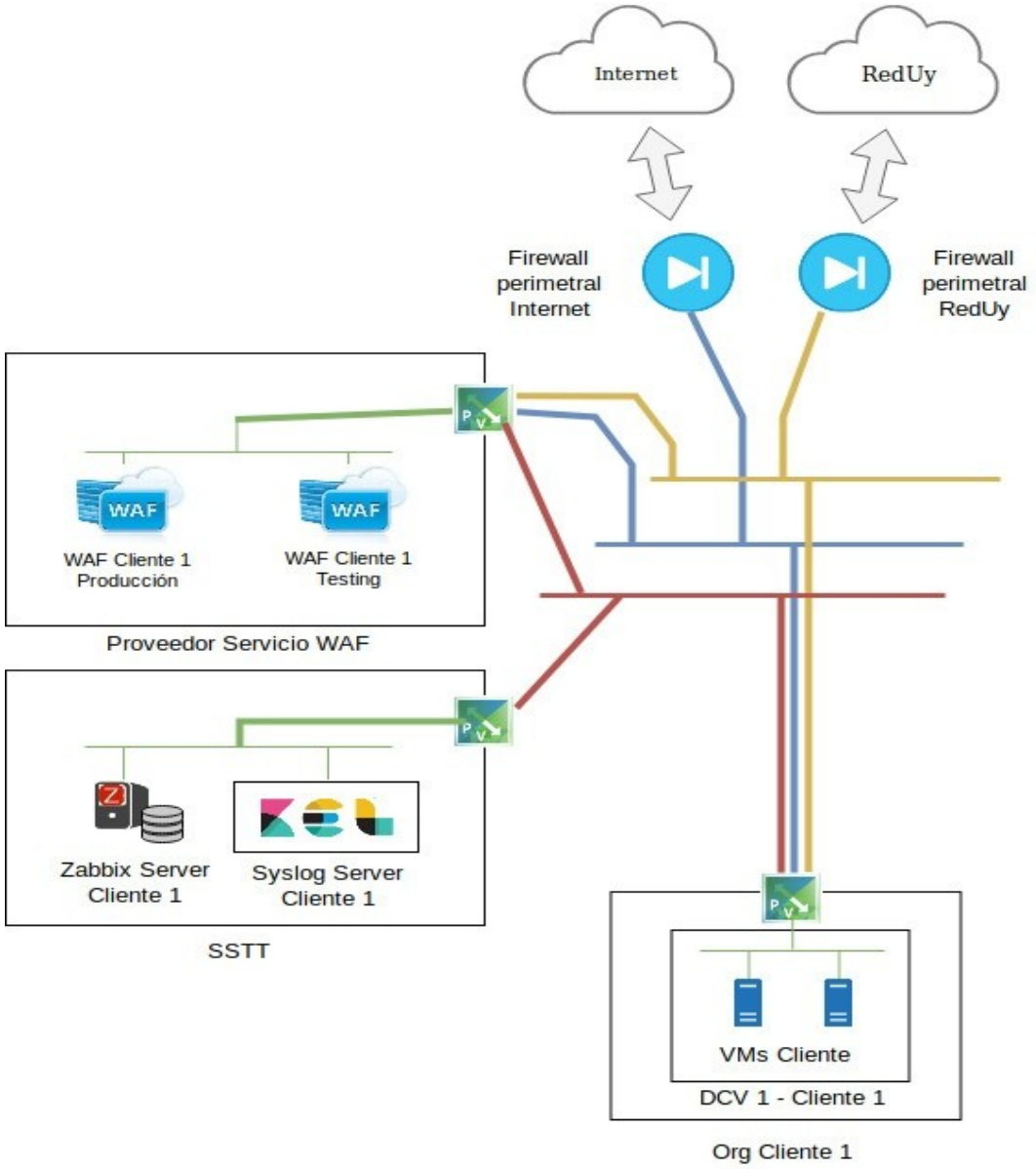
- Dos (2) IPs, para los WAF de producción y testing, a través de los que se publican los servicios Web hacia RedUy

- Once (11) IPs, asignadas en el Edge del Data Center Virtual del cliente para navegación y publicación de otro tipo de servicios.

Red Privada


RedUy
vDOM RedUy
WAN Cliente 1 /27
WAN Cliente 2 /27
WAN Cliente 3 /27
DCV Cliente 1
DCV Cliente 2
DCV Cliente n

Red de Servicios Transversales



Red de Servicios Transversales

Se asigna para el cliente un pool de 20 direcciones IP, dentro del direccionamiento privado de Servicios Transversales (192.168.xxx.0 /22), que serán presentadas en el Edge del cliente

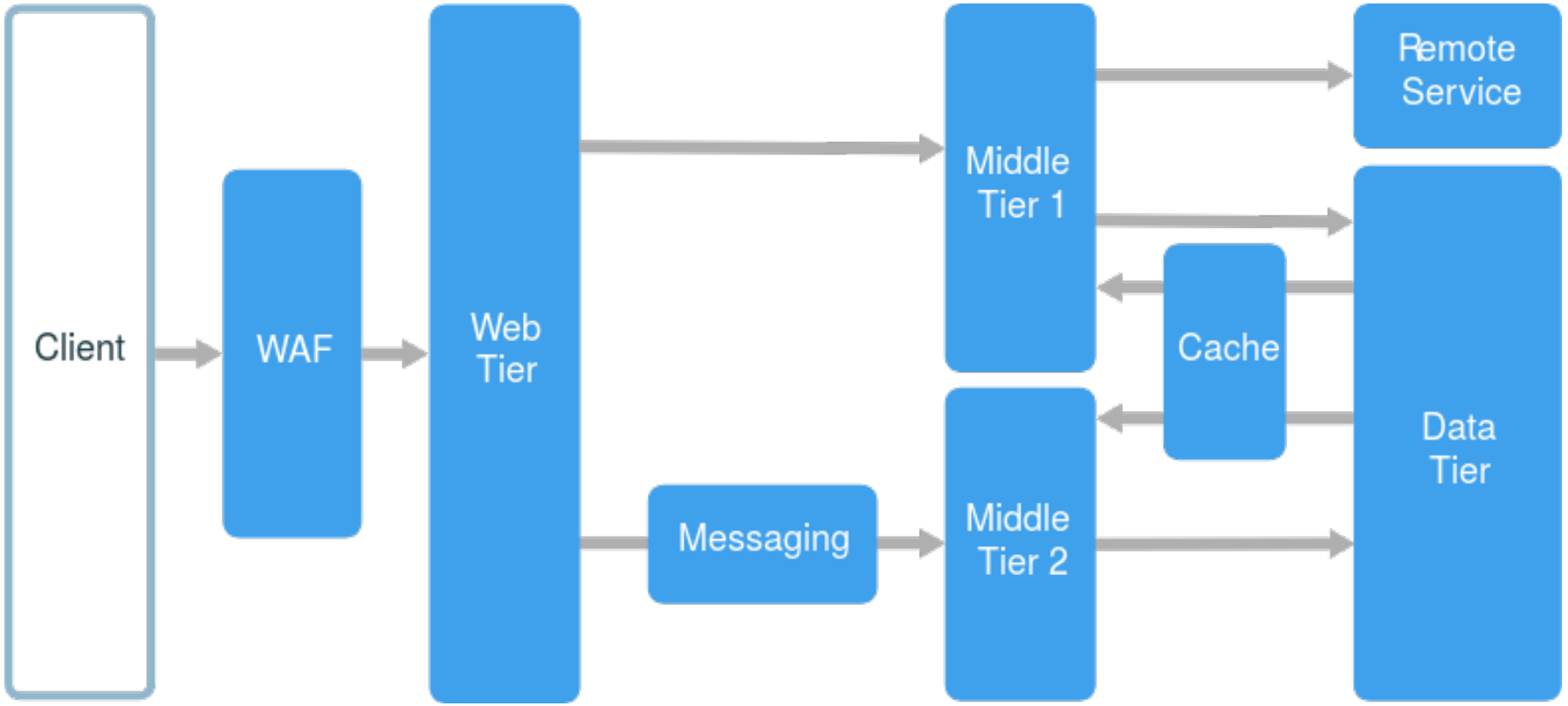
Tener en cuenta que el direccionamiento privado de servicios transversales (**192.168.xxx.0 /22) no podrá ser utilizado dentro del Data Center Virtual** del cliente.

DC Virtual del Cliente

- Despliegue y administración de sus VMs
- Creación y administración de redes virtuales internas
- Asignación de redes externas (Internet, RedUy)
- Configuración de políticas de seguridad en su firewall virtual

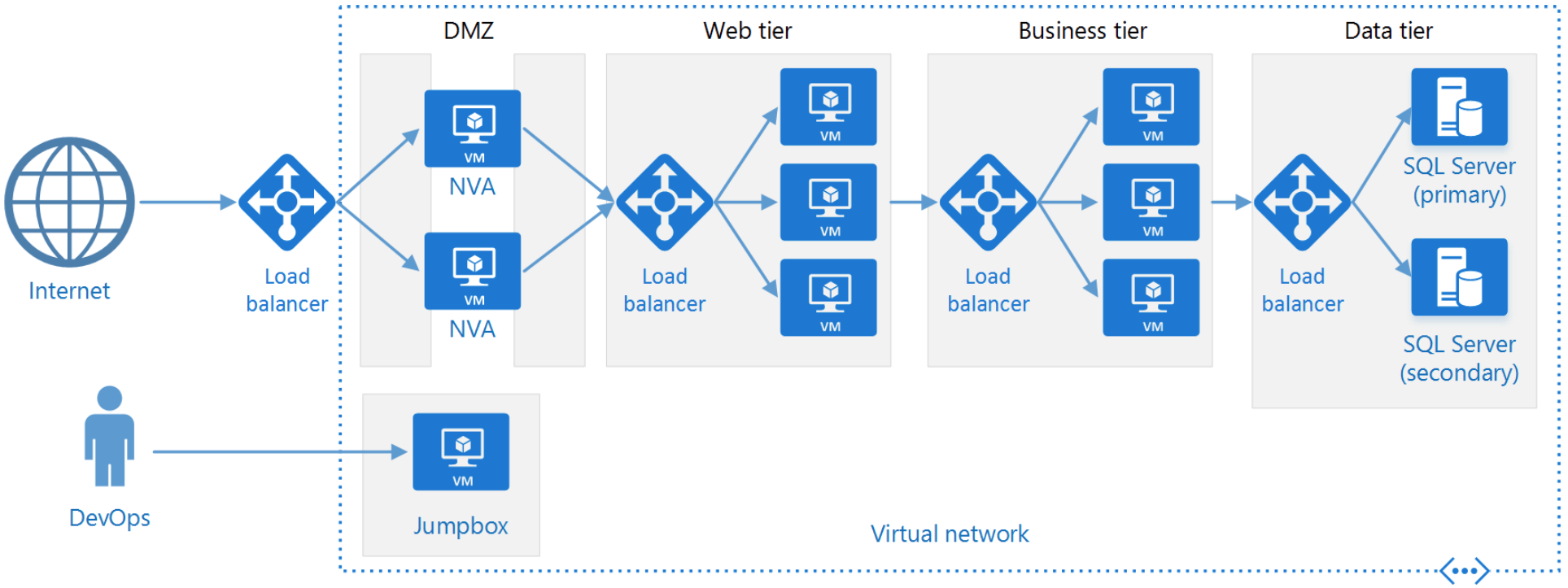
Arquitectura VDC Cliente

- Multi-tier Web App



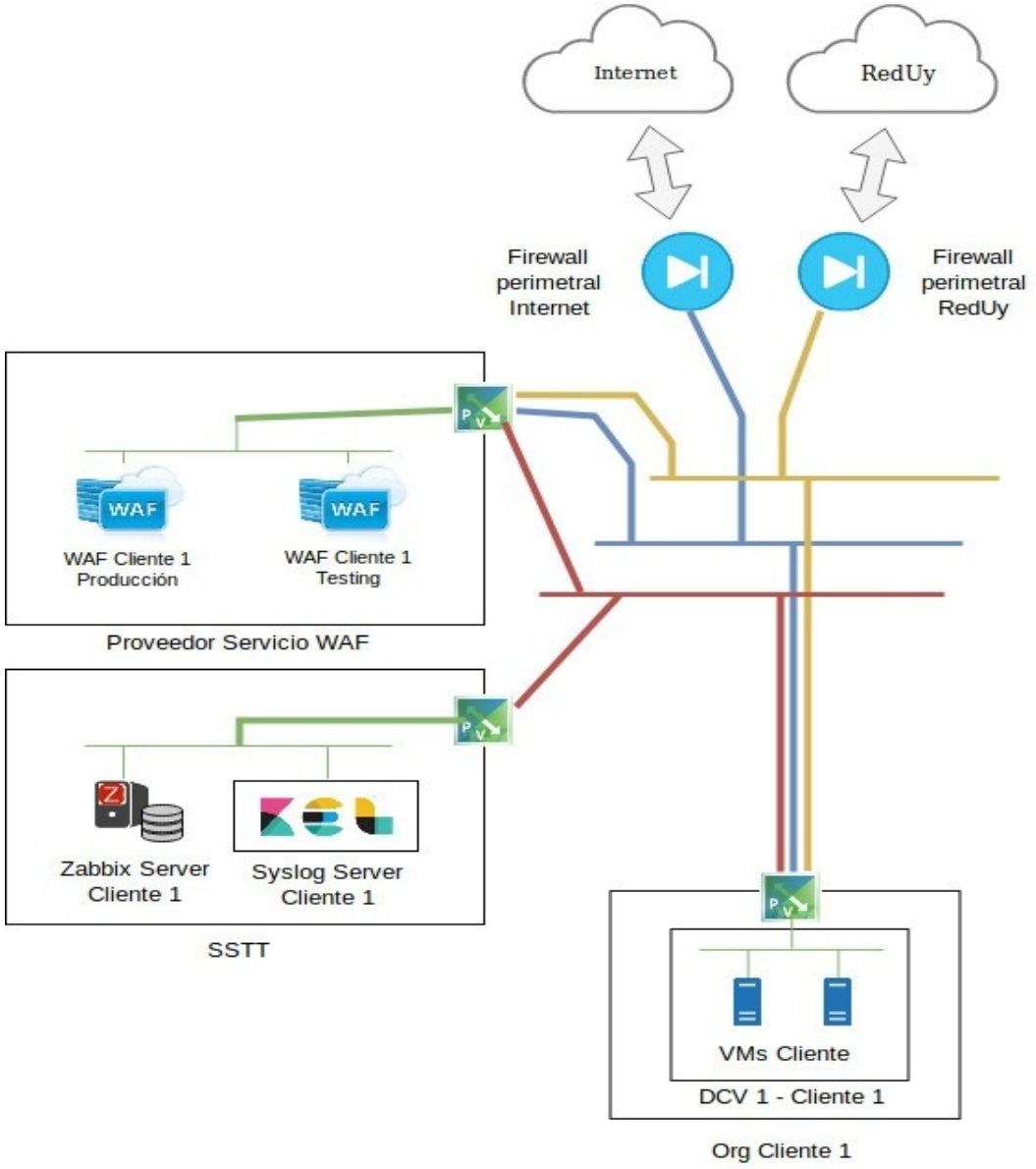
Arquitectura VDC Cliente

- Multi-tier



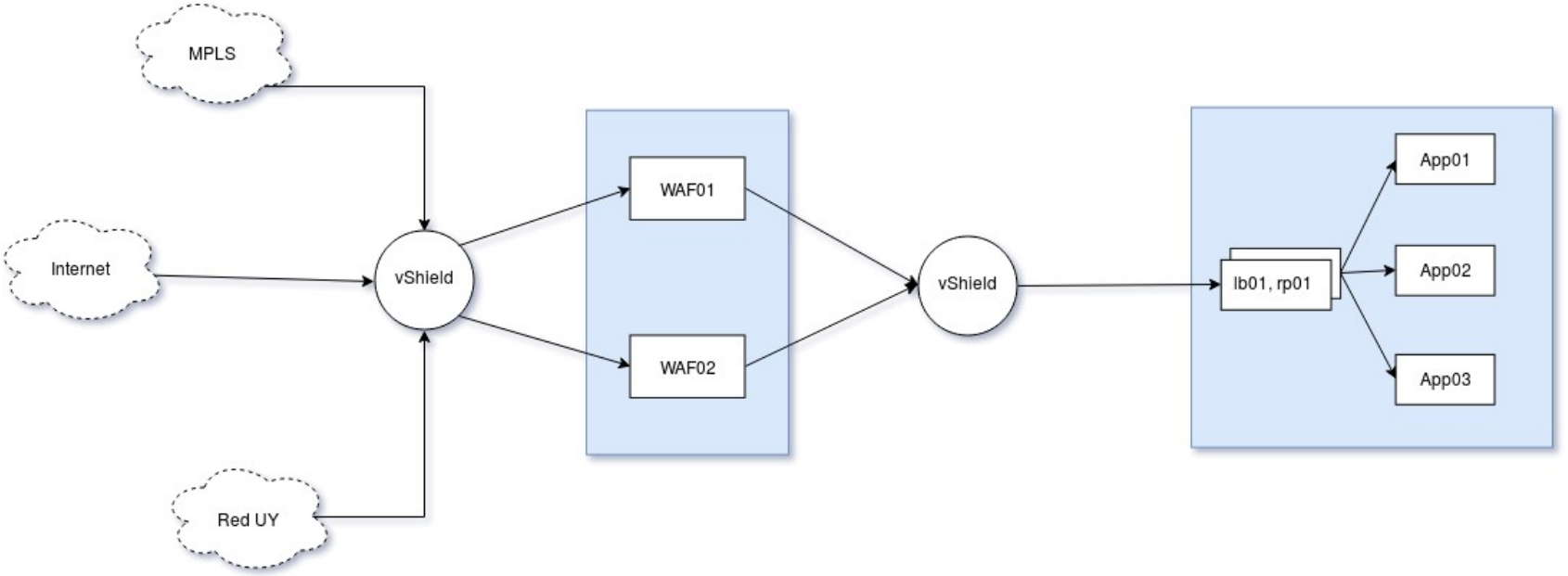
Arquitectura VDC Cliente

1. Firewalls
   - Edge vDom
   - vShield WAF Org
   - Apache/ModSec
   - vShield Client Org
   - Firewall VM



Arquitectura Interna

- Load Balancer y Reverse Proxy



Arquitectura Interna

Asignación de IPs (propuesta)

Layer	Prod	Prep	Test	Inte/Stag/Capa
Firewalling	192.168.0.0/24	192.168.1.0/24	192.168.2.0/24	
Web (LBs y RPs)	192.168.10.0/24	192.168.11.0/24	192.168.12.0/24	
Application	192.168.20.0/24	192.168.21.0/24	192.168.22.0/24	
Data	192.168.30.0/24	192.168.31.0/24	192.168.32.0/24	
Cache	192.168.40.0/24			
Messaging				

Ej: cliente-prod-app01-prod -> 192.168.0.11
cliente-prod-app02-prod -> 192.168.0.12

Las IPs 192.168.x.10 se reservan para las IP flotante en servicio activo-pasivo

Arquitectura Interna

Redes ruteadas:

- RedPrivada
- Internet
- SSTT
- MPLS
- DMZ Prod
- DMZ Prep
- DMZ Test
- App Prod
- App Test
- Datos Prod
- Datos Prep
- Datos Test

Agenda

- Catálogo de Servicios
- Arquitectura de Referencia
- Servicios Transversales

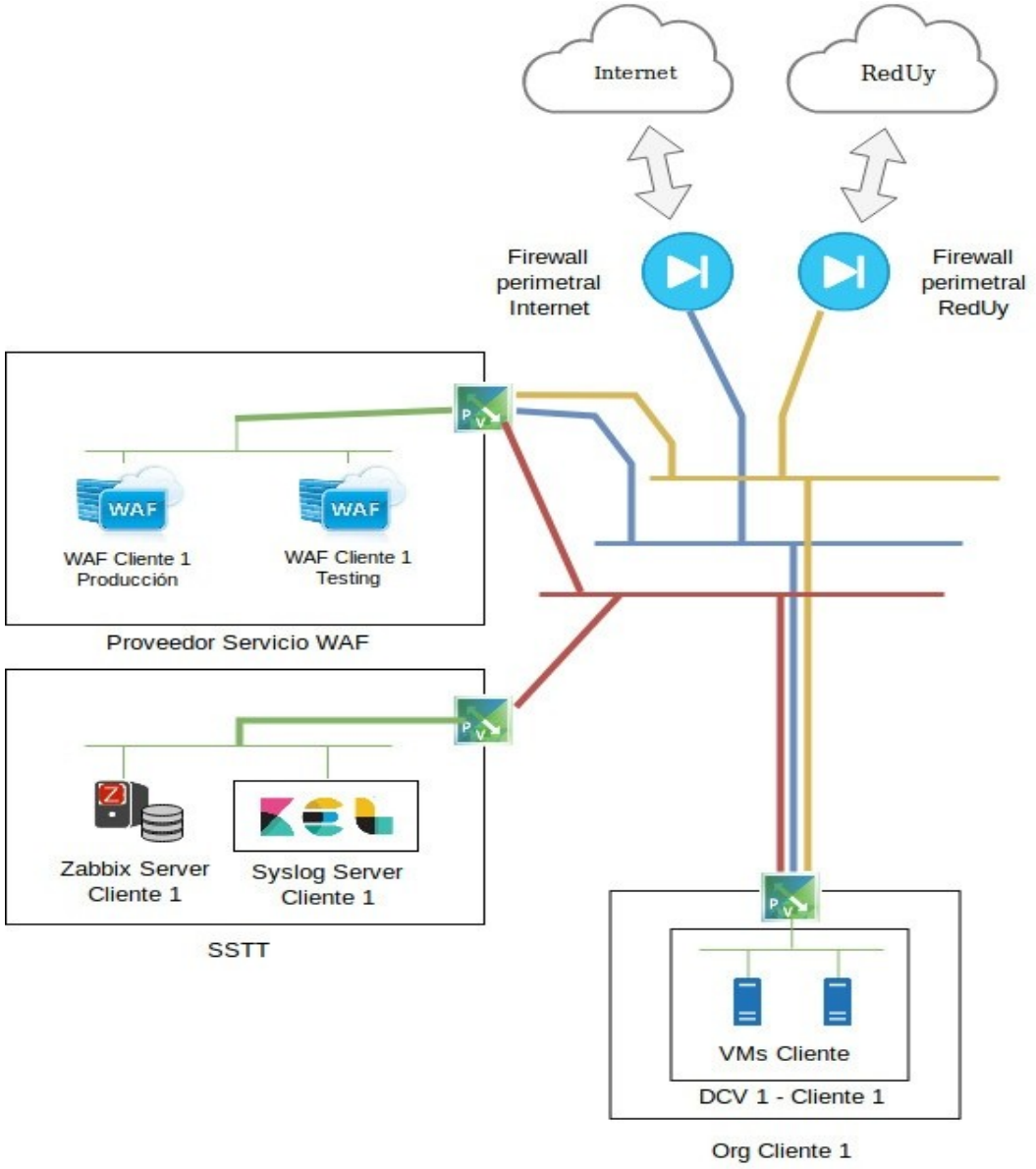
Introducción a Syslog con ELK

Servicio de Syslog

- Stack ELK desplegados
- Filebeat -> Elasticsearch Ingest Node
- Pipeline y Dashboards preconfigurados
- Dashboards por Capa: WAF, APP, DATA

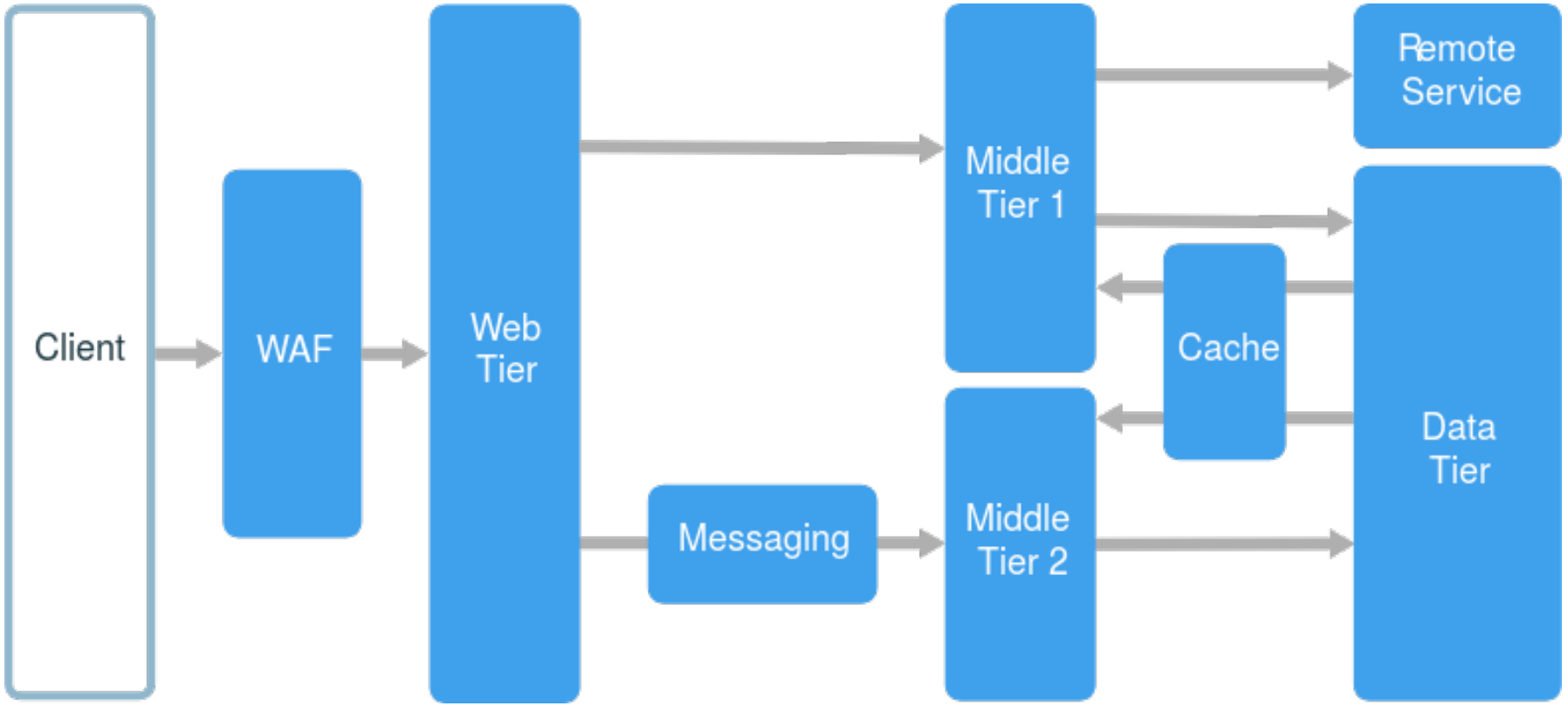
Arquitectura VDC Cliente

1. Firewalls
   - Edge vDom
   - vShield WAF Org
   - Apache/ModSec
   - vShield Client Org
   - Firewall VM

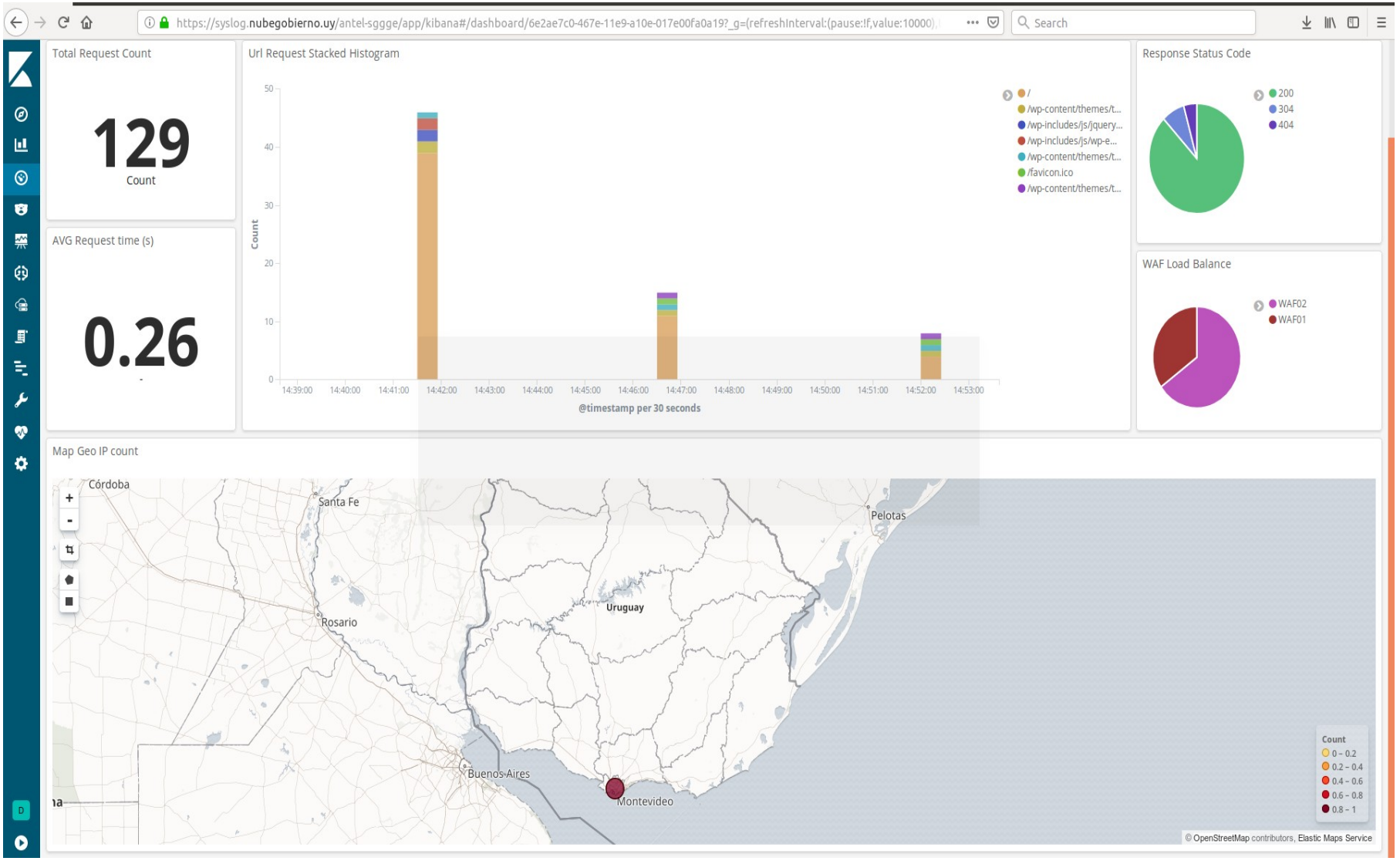


Arquitectura VDC Cliente

- Multi-tier Web App



Kibana Dashboard de Servicio



El camino del log

1. Generación
2. Envío
3. Ingesta
4. Visualización

Generación

Apache Custom Logs:

vim /etc/httpd/conf/httpd.conf

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio

LogFormat "%h %l %u %t \"%r\" %>s %D %b \"%{Referer}i\" \"%{Balancer-Worker-Route}i\" \"%{User-Agent}i\"" custom_full

vim /etc/httpd/vhost.d/gobierno-demo.conf

CustomLog logs/gobierno-demo.sva.antel.com.uy-access_log custom_full

tail /var/log/httpd/gobierno-demo_access_full_log

10.255.152.40 - - [13/Mar/2019:16:15:35 -0300] "GET /wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0 HTTP/1.1" 200 4244 7682 "http://gobierno-demo.sva.antel.com.uy/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20100101 Firefox/65.0

Envío

Filebeat:

- Modules vs Inputs
- 2 Input + 2 outputs = 2 Servicios
- Otros beats...

Envío

Filebeat: Inputs

```
# vim filebeat.yml

filebeat.config.inputs:
  enabled: true
  path: configs/*.yml

setup.template:
  name: "filebeat"
  pattern: "filebeat-prod-waf-*"
  overwrite: true

output.elasticsearch:
  hosts: ["192.168.200.1:9200"]
  pipeline: "filebeat-6.6.0-apache2-access-full"
  index: 'filebeat-prod-waf-%{+YYYY.MM.dd}'
```

```
# vim config/filebeat-client.yml

filebeat.inputs:
- type: log
  paths:
        - /var/log/httpd/*access_full_log
  exclude_files: ['(ssl_access)_log$']
  tags: ["WAF01"]
```

Envío

Filebeat: Modules

```
# vim filebeat.yml

filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml

setup.template:
  name: "filebeat"
  pattern: "filebeat-prod-waf-*"
  overwrite: true

setup.kibana:
  host: "192.168.200.1:5601"
  protocol: "http"
  path: /antel-sggge

output.elasticsearch:
  hosts: ["192.168.200.1:9200"]
  pipeline: "filebeat-6.6.0-apache2-access-full"
  index: 'filebeat-prod-waf-%{+YYYY.MM.dd}'
```

```
# vim modules.d/system.yml

- module: system
  syslog:
        enabled: true
        var.paths: ["/path/to/log/syslog*"]
  auth:
        enabled: true
        var.paths: ["/path/to/log/audi.log*"]
```

```
# filebeat modules enable system,iss

# filebeat setup --pipelines --modules system,iis

# filebeat  setup --dashboards
```

Ingesta

¿Qué es un pipeline?

1. Parsear líneas de logs (Grok)
2. Crear campos y asignar tipo de datos
3. Enriquecer los datos obtenidos

Ingesta

¿Cómo cargar un pipeline?

1. Usando beats:

   ```
   # metricbeat setup --pipeline
   ```

2. Elasticsearch:

   ```
   # curl -X PUT "localhost:9200/_ingest/pipeline/my-pipeline-id" -H 'Content-Type:
   application/json' -d' {}
   ```

3. Kibana Dev Tools

Visualizaciones

1. Usando beats:

   ```
   # filebeat setup --dashboards
   ```

2. Kibana Import/Export

Visualizaciones: Extra

1. Region maps

2. Custom layer

3. Cors enabled server

Visualizaciones: Extra

Custom layer:

```
# vim  kibana.yml

elasticsearch.url: "http://elasticsearch-coordinator:9200"
kibana.index: ".kibana"
regionmap:
  includeElasticMapsService: false
  layers:
   - name: "Departmentos de Uruguay"
        url: "http://gobierno-demo.sva.antel.com.uy/layer/Uruguay.GeoJson"
        attribution: "OpenMaps.layer"
        fields:
        - name: "name"
        description: "Departamentos de Uruguay"
```

Demo

Fin