Federal Symposium

F5's Public Sector Application Security and Delivery Conference

MARCH 19-21, 2024 | TYSONS CORNER, VA

App World

WASHINGTON, D.C.

Migrate F5 BIG-IP Applications to F5 Distributed Cloud Services

Nilesh Mistry
Principal Solutions Engineer, F5

Agenda

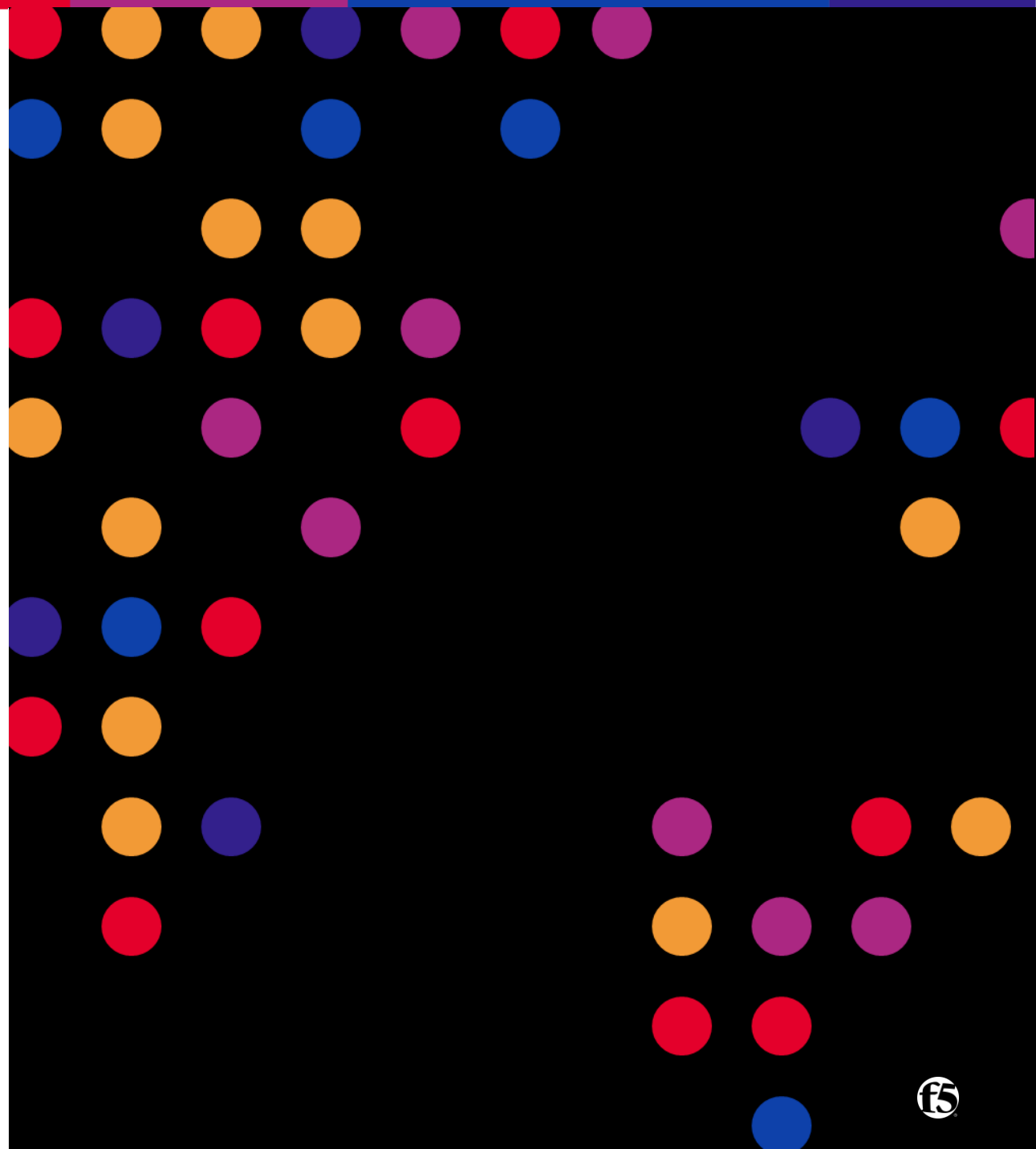
Applications in a BIG-IP World

Distributed Cloud Platform

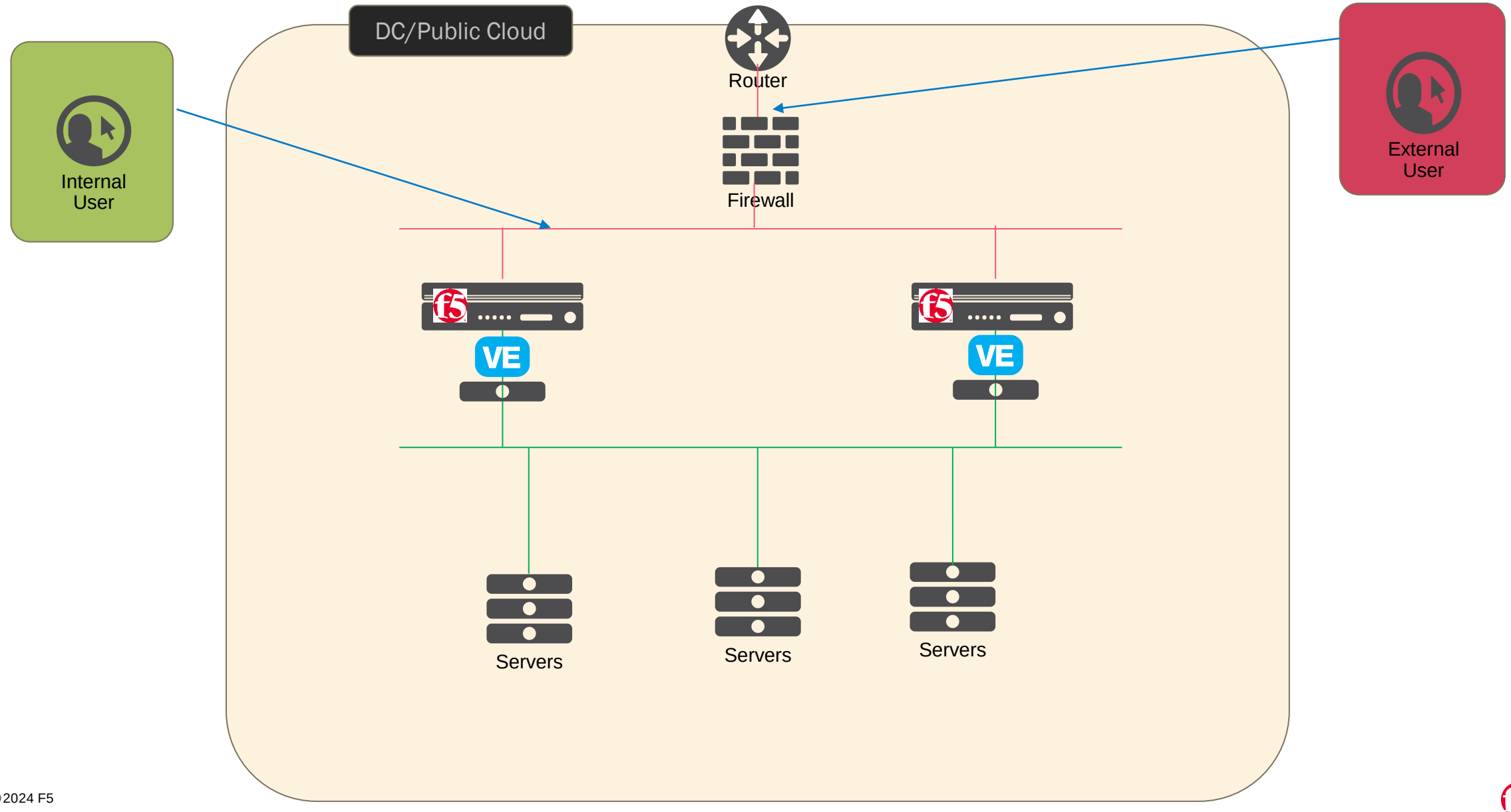
Architectures and Topologies

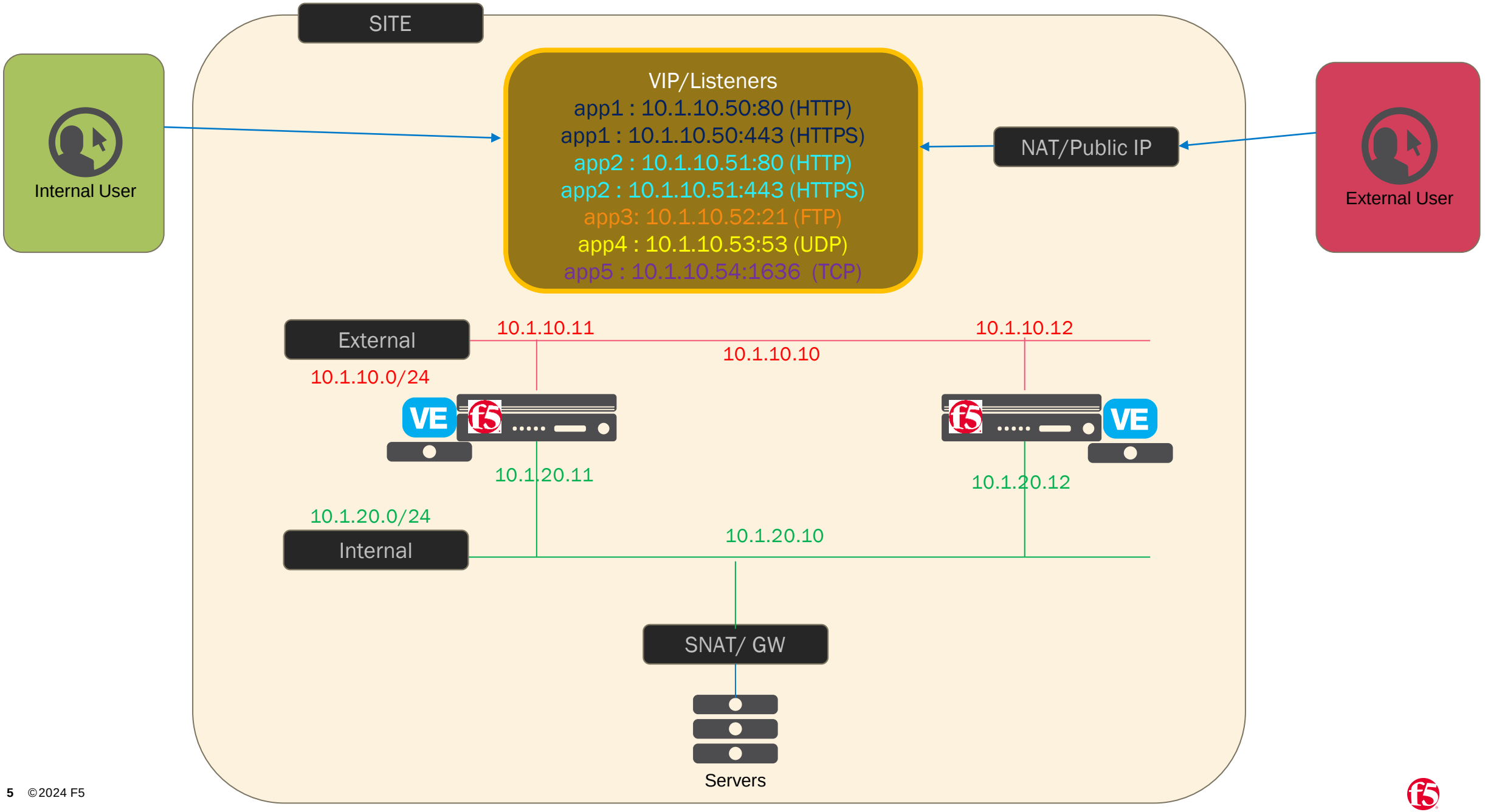
Demo/Walkthrough

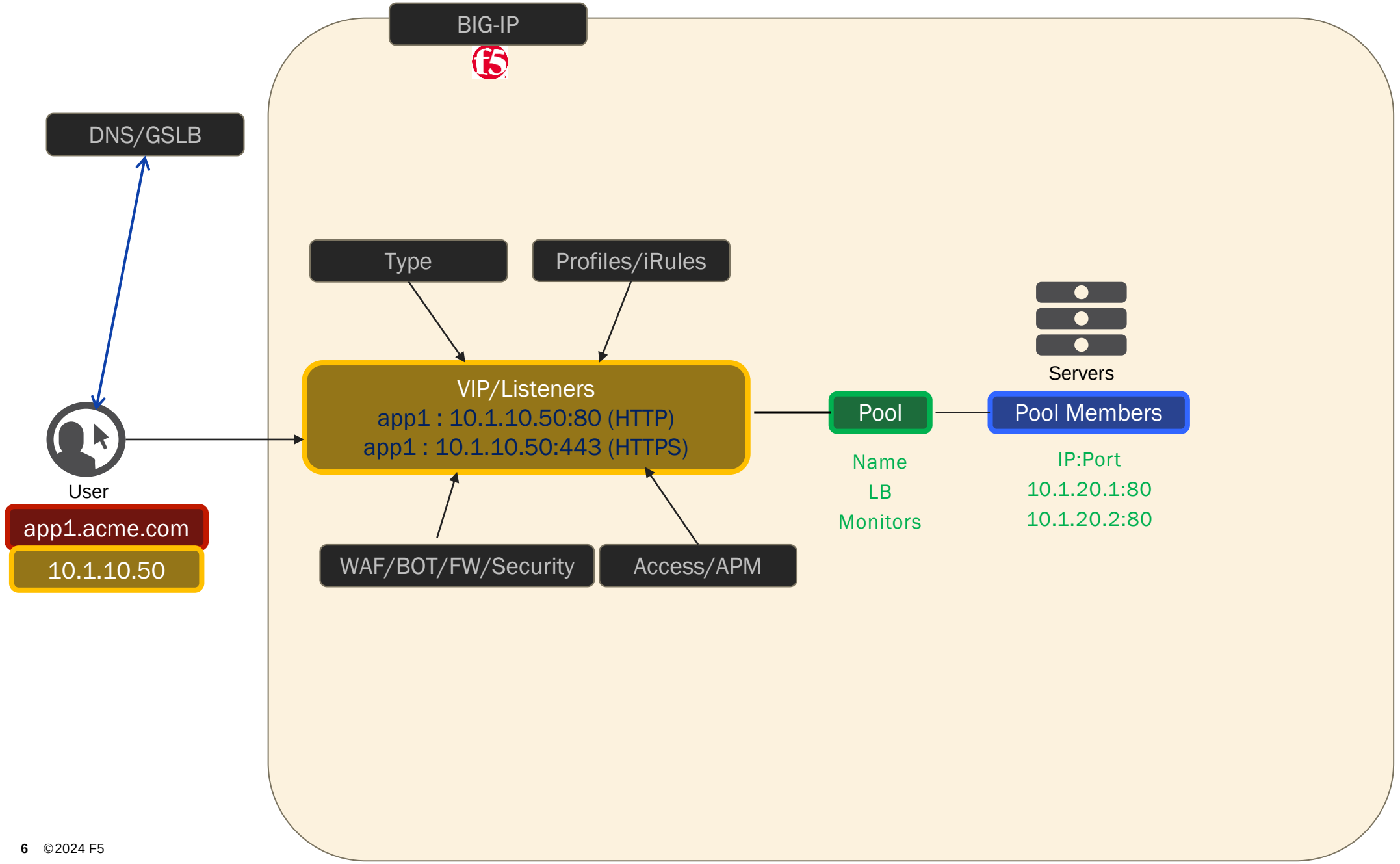
Open Discussion/Q&A

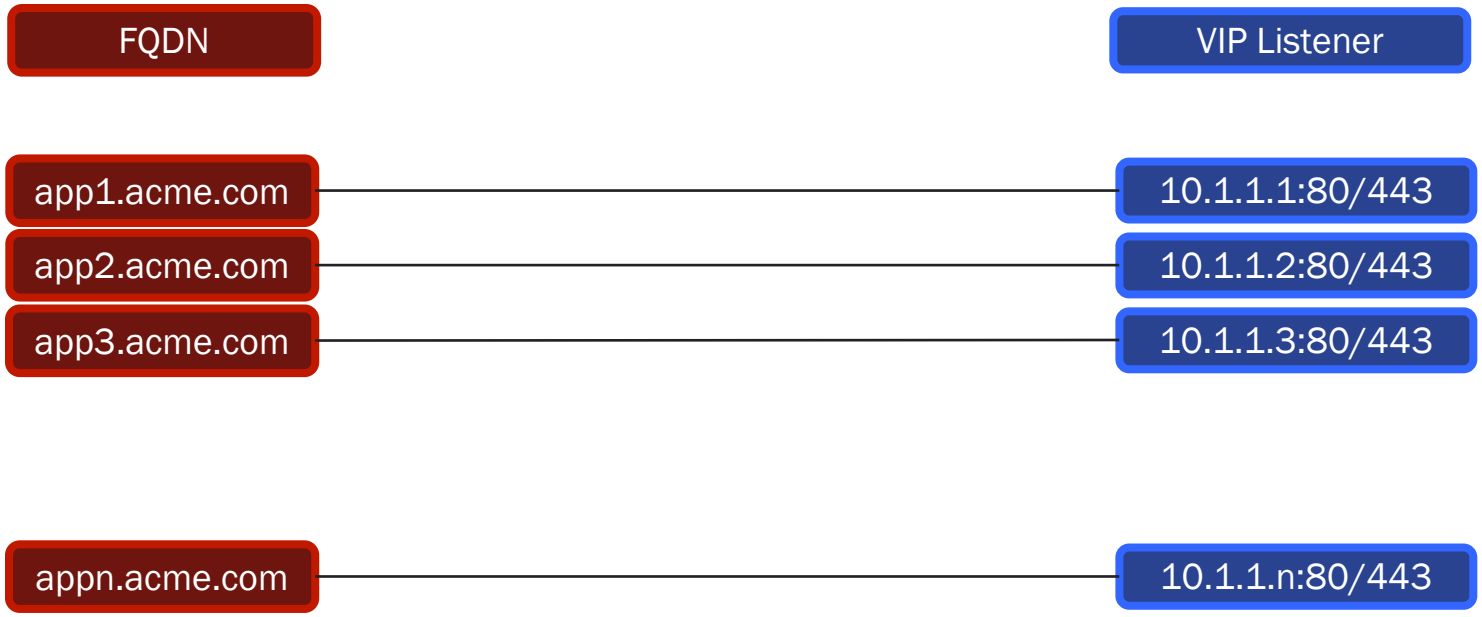


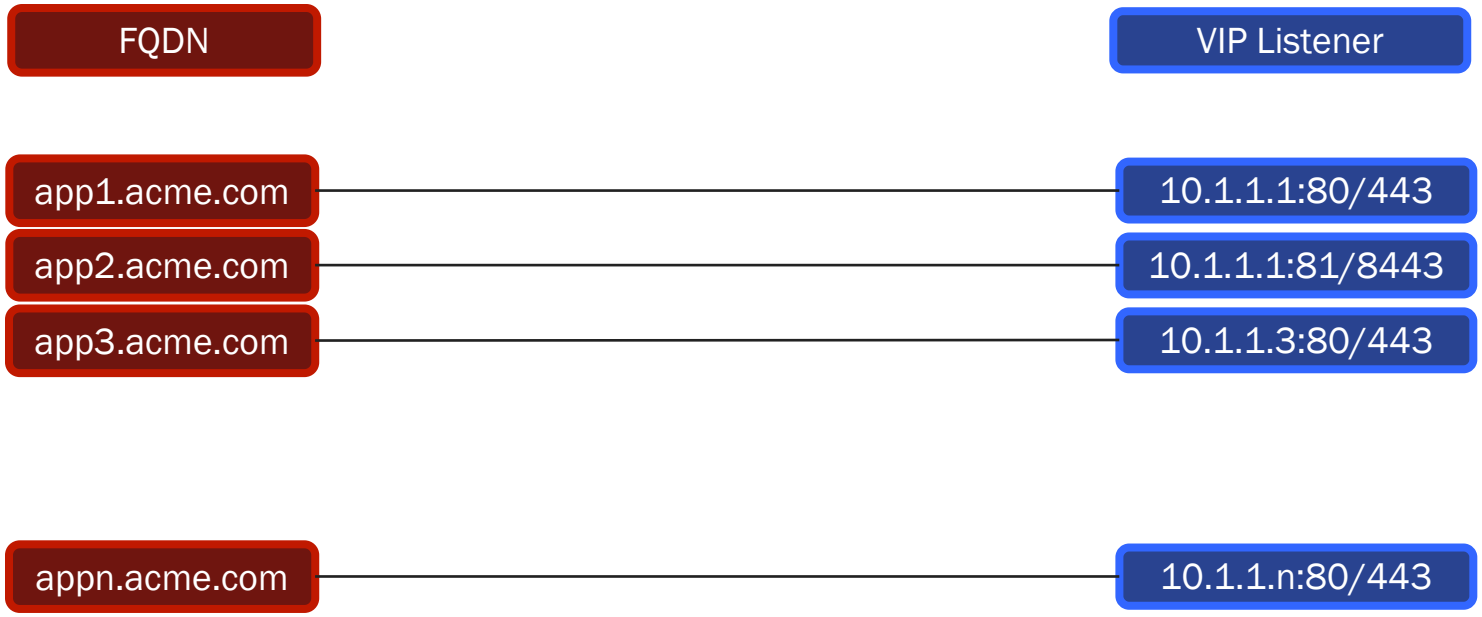
BIG-IP sites



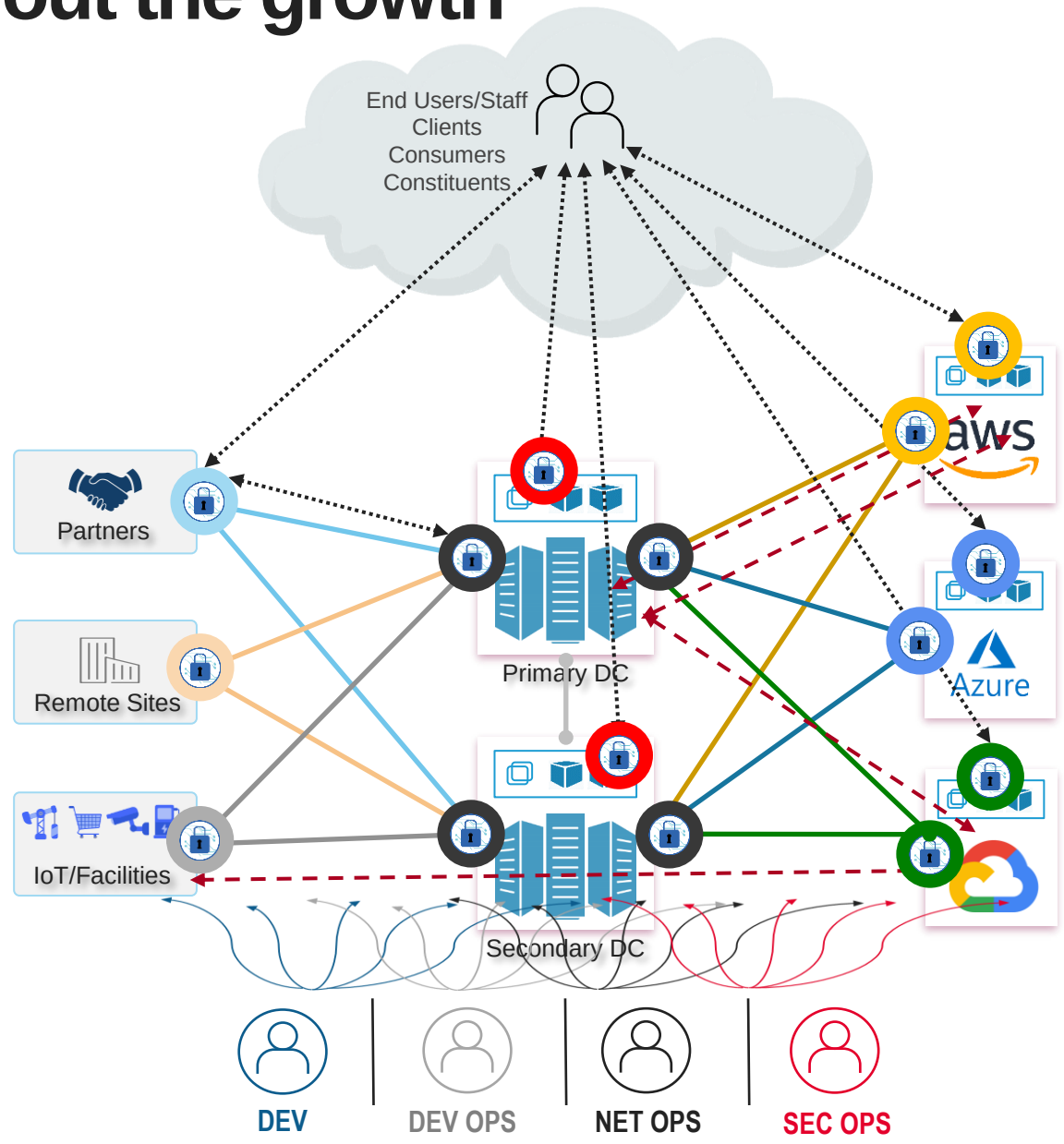

SITE
Internal User
VIP/Listeners
app1 : 10.1.10.50:80 (HTTP)
app1 : 10.1.10.50:443 (HTTPS)
app2 : 10.1.10.51:80 (HTTP)
app2 : 10.1.10.51:443 (HTTPS)
app3: 10.1.10.52:21 (FTP)
app4 : 10.1.10.53:53 (UDP)
app5 : 10.1.10.54:1636 (TCP)
NAT/Public IP
External User
External
10.1.10.11
10.1.10.10
10.1.10.12
10.1.10.0/24
VE
VE
10.1.20.11
10.1.20.12
10.1.20.0/24
Internal
10.1.20.10
SNAT/ GW
Servers


BIG-IP
DNS/GSLB
Type
Profiles/iRules
VIP/Listeners
app1 : 10.1.10.50:80 (HTTP)
app1 : 10.1.10.50:443 (HTTPS)
Servers
Pool
Pool Members
Name
LB
Monitors
IP:Port
10.1.20.1:80
10.1.20.2:80
User
app1.acme.com
10.1.10.50
WAF/BOT/FW/Security
Access/APM


FQDN
VIP Listener
app1.acme.com
app2.acme.com
app3.acme.com
appn.acme.com
10.1.1.1:80/443
10.1.1.2:80/443
10.1.1.3:80/443
10.1.1.n:80/443


FQDN
VIP Listener
app1.acme.com
app2.acme.com
app3.acme.com
appn.acme.com
10.1.1.1:80/443
10.1.1.1:81/8443
10.1.1.3:80/443
10.1.1.n:80/443

Let's “napkin” out the growth



Control-Plane
Data-Plane
Other

Distributed Cloud Platform

F5 Distributed Cloud

Global Controller – Console

- The control plane
- Multi-tenant
- Configurations and observability
- API/Web

Regional Edge (RE)

- SaaS data plane
- F5 managed facilities (hosted)
- Provide L3-L7 services to tenants
- Multi-tenant
- Host virtual K8s workloads

Customer Edge (CE)

- Customer-owned data plane
- Deployed in customer networks
- Peers with regional edge
- Provide L3-L7 services to tenants
- Single-tenant (typically)
- Host K8s workloads

Global Application Delivery Network (ADN)

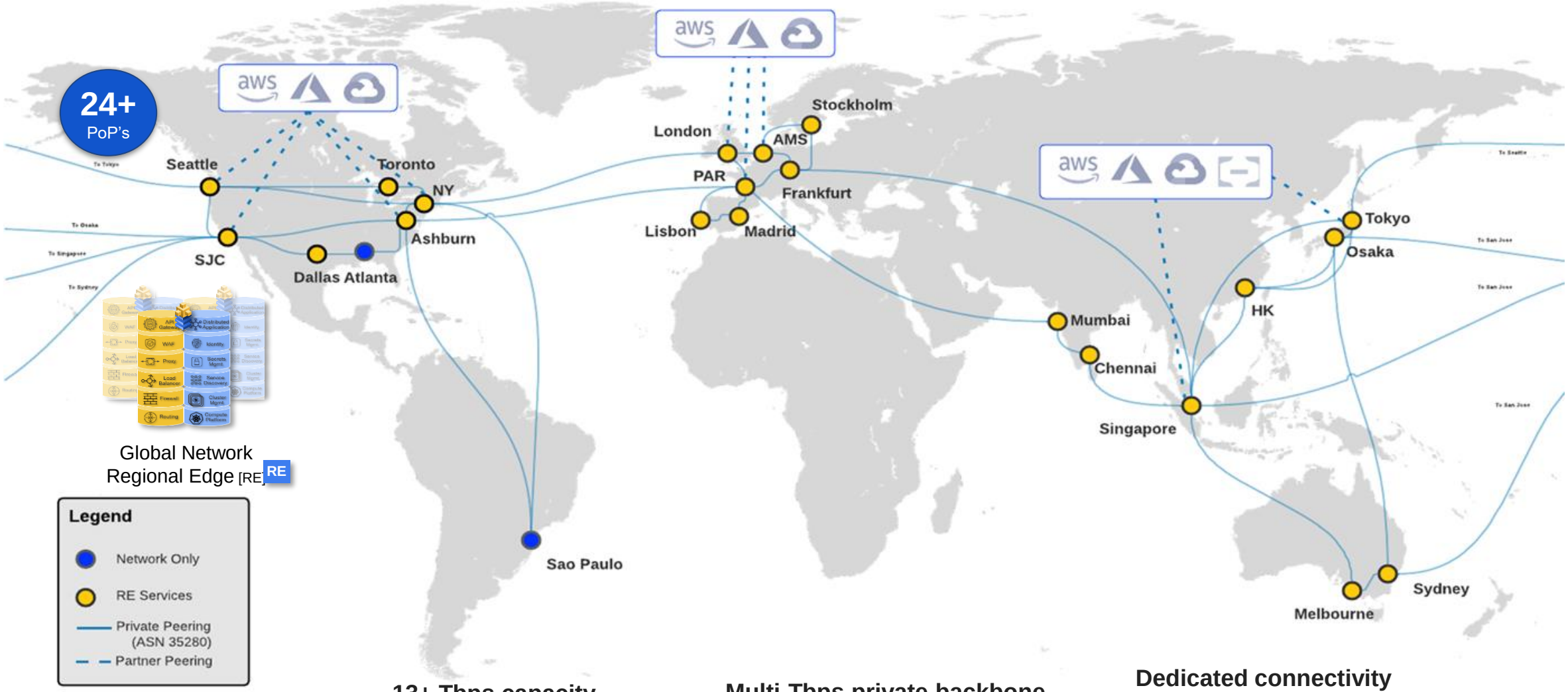
- Global backbone connecting F5 Distributed Cloud regions, customer edges (CEs), clouds, and internet
- Allows private peering
- Top 10 peered networks (ASN 35280) in the world

Site-Reliability Engineers (SREs)

- Global team of highly talented dev/operations engineers.
- Constant monitoring and maintaining of platform
- Perform upgrades of platform every 4-6 weeks.

Delivered across a private global network

Application Delivery Network (ADN)

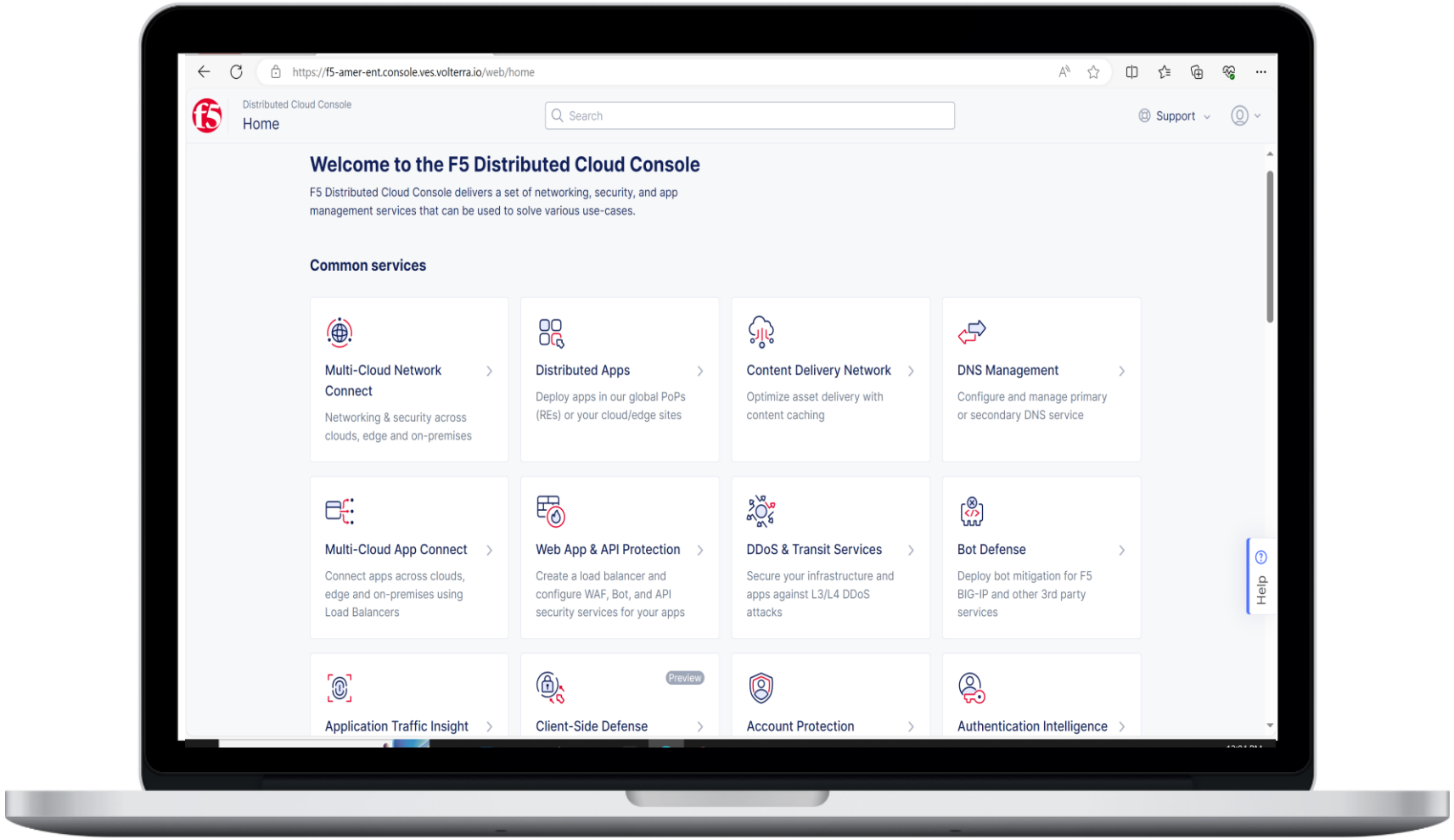


13+ Tbps capacity
(Tier-1 Carriers: NTT, Telia, Level3)

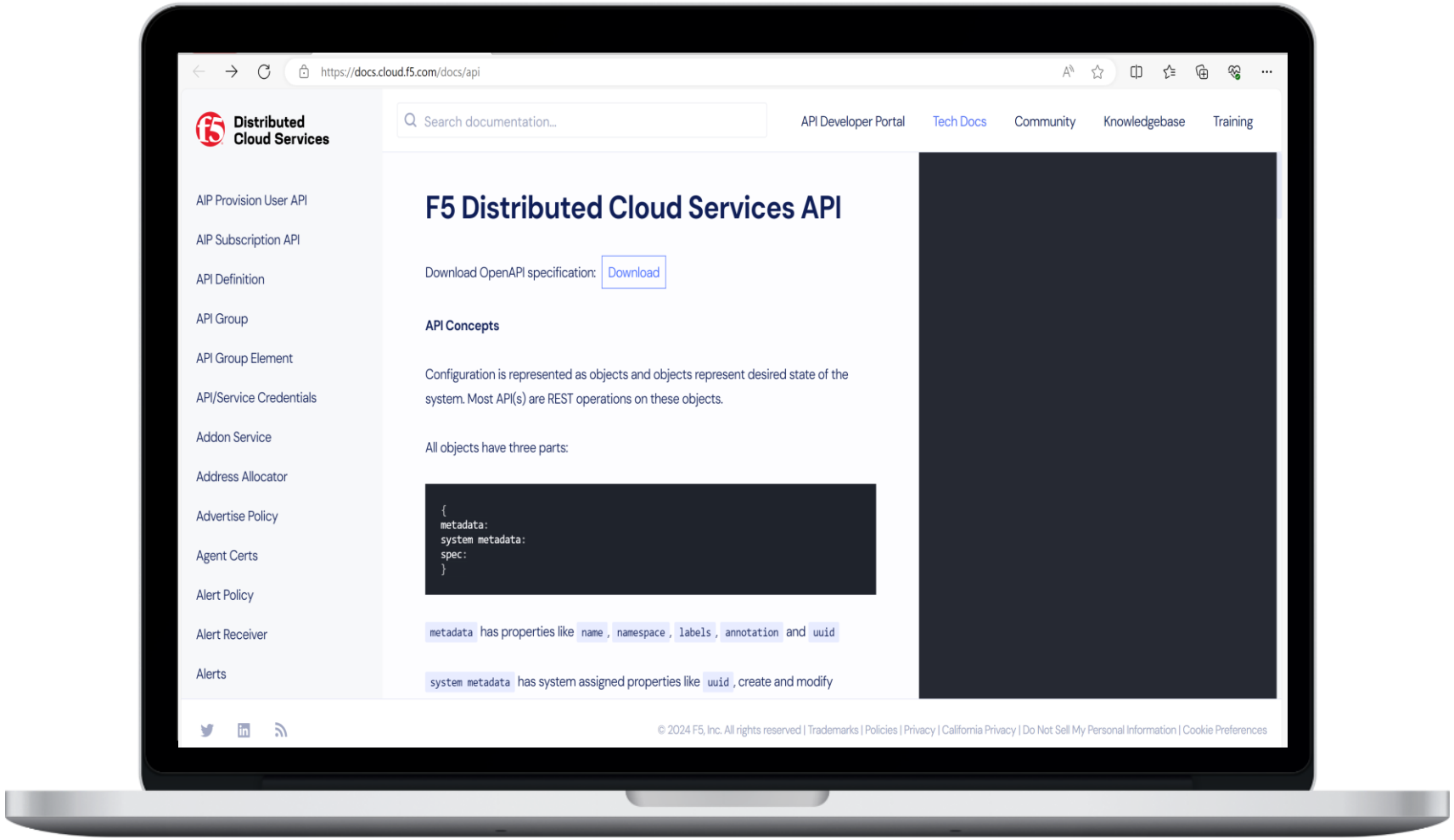
Multi-Tbps private backbone
(Zayo, Telia, CenturyLink)

Dedicated connectivity
(Cloud providers, SaaS providers)

Global Controller—F5 Distributed Cloud Console



Global Controller—API



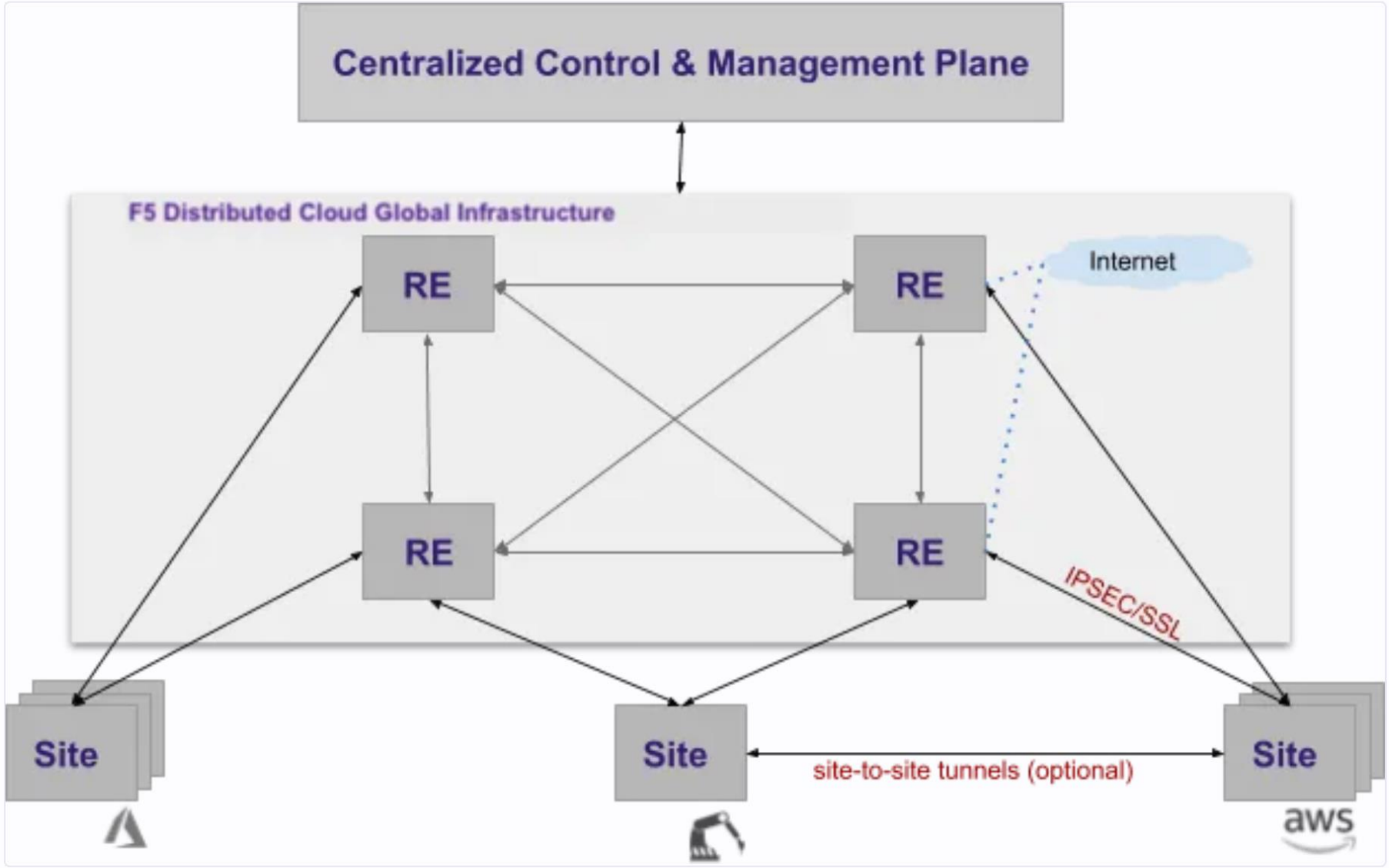


Figure: Components of F5 Distributed Cloud Services System

Regional edge—SaaS data plane

ADN – Application Delivery Network
Global app-to-app Network


24+ Global POPs


Public Clouds
Private Peering

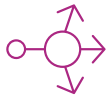

Multiple Tbps Capacity

Networking

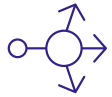

Router

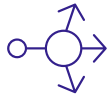

Firewall


DDoS Mitigation (Layer 3-4)

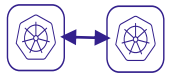

Multicloud Networking

Application Delivery


Load Balancing


L7 Routing


Service Discovery


Multi-Cluster Networking

Application Security


DDoS Mitigation (Layer 7)


WAF


Bot Defense


API Security

Distributed Networking and Security Services

Distributed Applications


K8s Compute Platform


K8s Cluster Management


Service Discovery


Identity

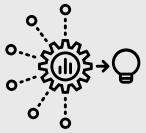

Secrets Management

Kubernetes Platform Services for Distributed Applications

Distributed Cloud Console
SaaS-based centralized console managing application lifecycle and visibility


Visibility and Analytics


Centralized Operations


Artificial Intelligence/ Advanced Insights

Customer edge—customer-owned data plane

Connects to RE—Application Delivery Network

Customer to XC Global Network

Networking

- Router
- Firewall
- Multicloud Networking

Application Delivery

- Load Balancing
- L7 Routing
- Service Discovery
- Multi-Cluster Networking

Application Security

- DDoS Mitigation (Layer 7)
- WAF
- Bot Defense
- API Security

Distributed Networking and Security Services

Distributed Applications

- K8s Compute Platform
- K8s Cluster Management
- Service Discovery
- Identity
- Secrets Management

Kubernetes Platform Services for Distributed Applications

Distributed Cloud Console

SaaS-based centralized console managing application lifecycle and visibility

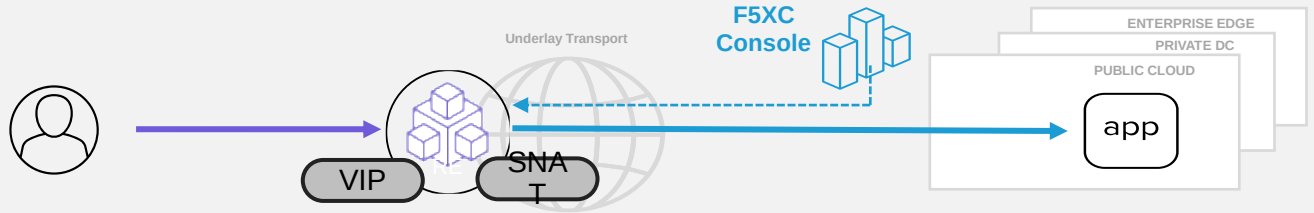
- Visibility and Analytics
- Centralized Operations
- Artificial Intelligence/ Advanced Insights

Distributed Cloud Platform

F5 Distributed Cloud—Topology Types

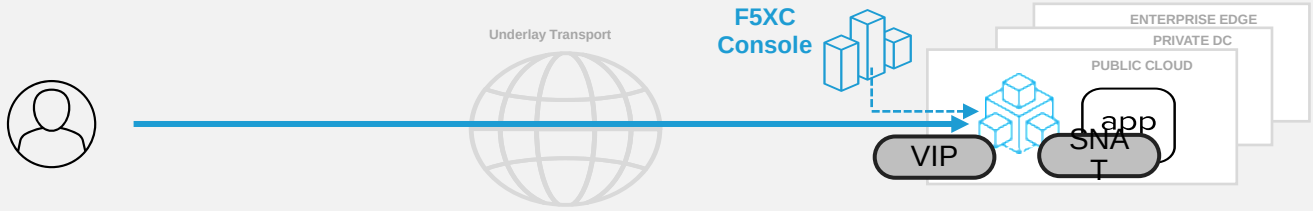
Regional Edge (RE)

Hosted in F5 Global Network
Shared Node (many customers)

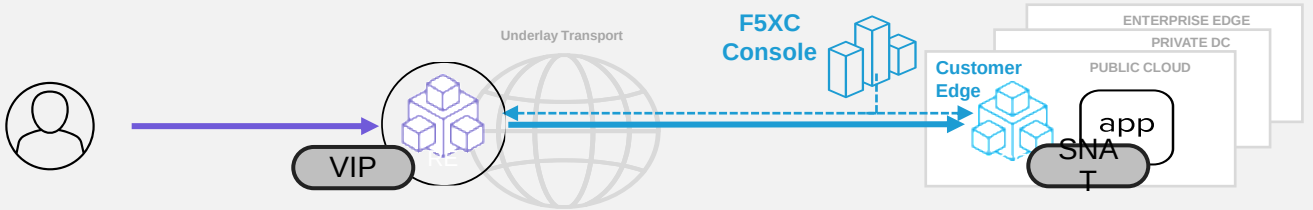


Customer Edge (CE)

Hosted in customer premise/public cloud
Dedicated Node (single customer)

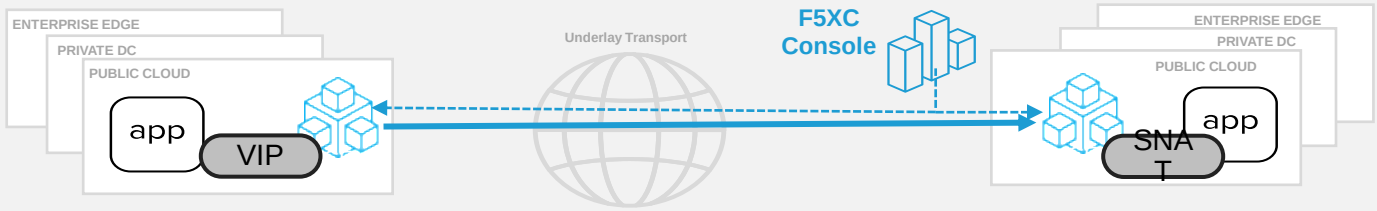


Hybrid (RE+CE)



Customer Edge (CE) MCN

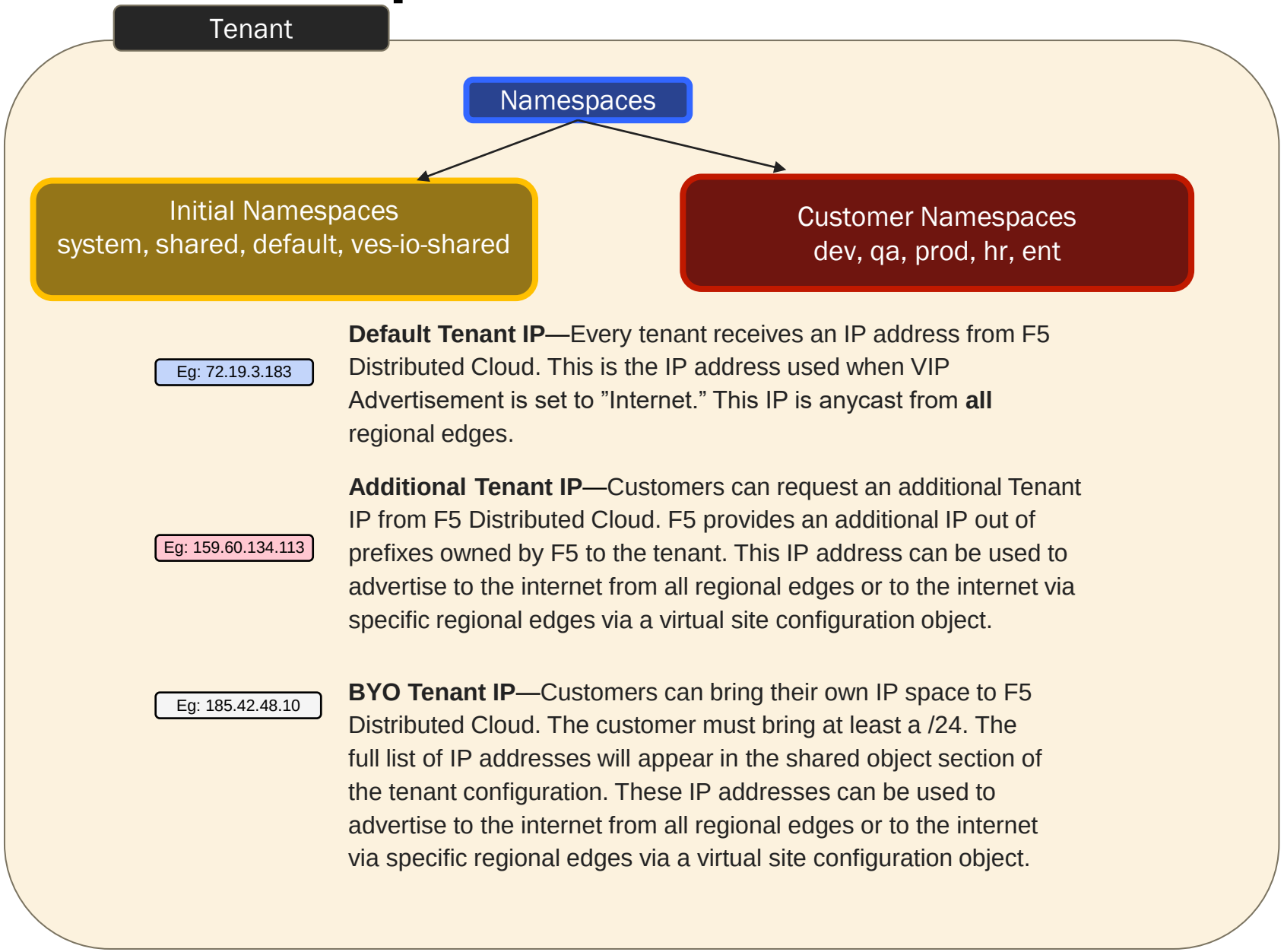
Hosted in customer premise/public cloud
Dedicated Node (single customer)



Topology types can be combined depending on the Enterprise Application Delivery requirements

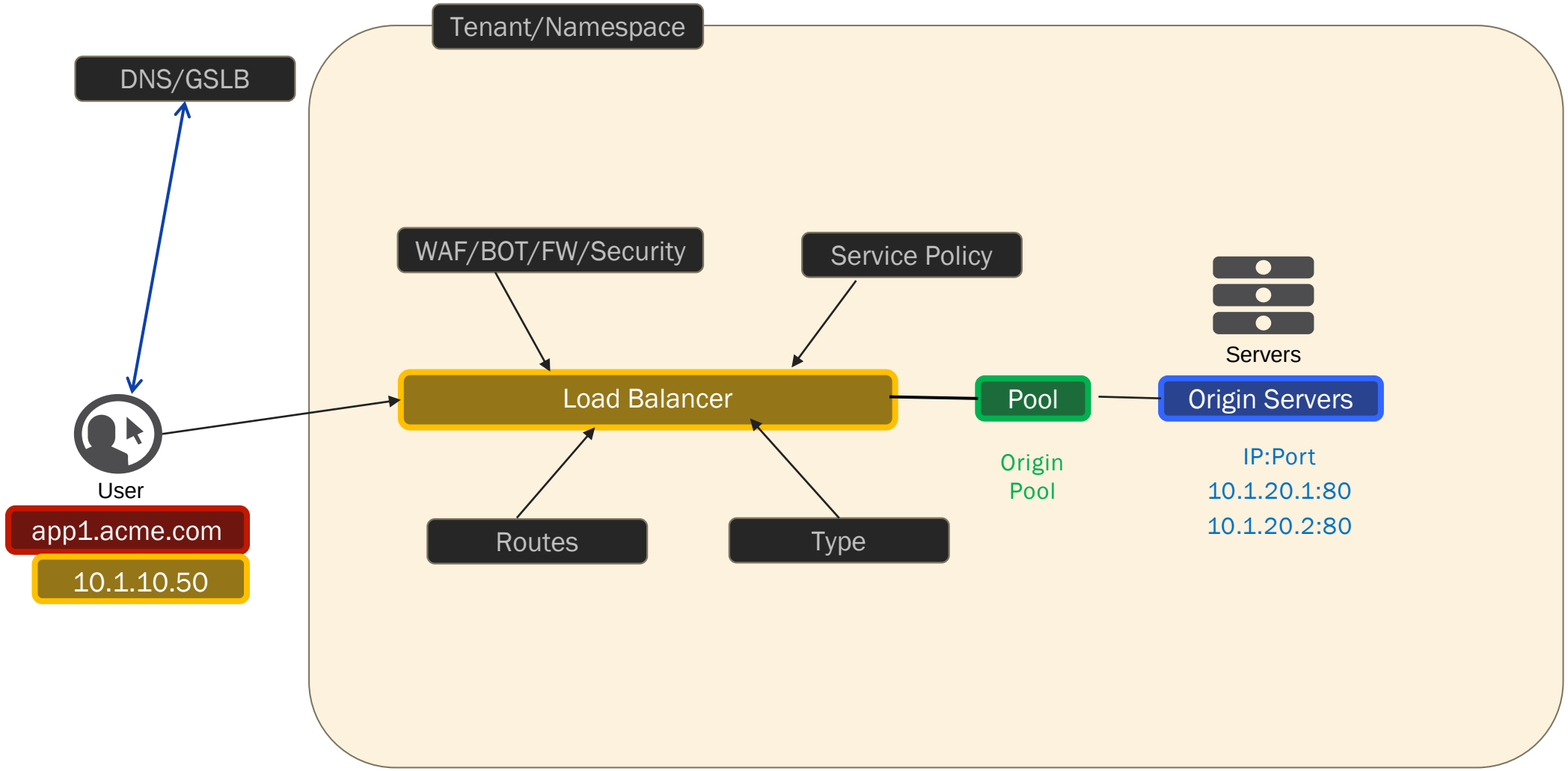
Distributed Cloud core concepts

Tenant and Namespaces



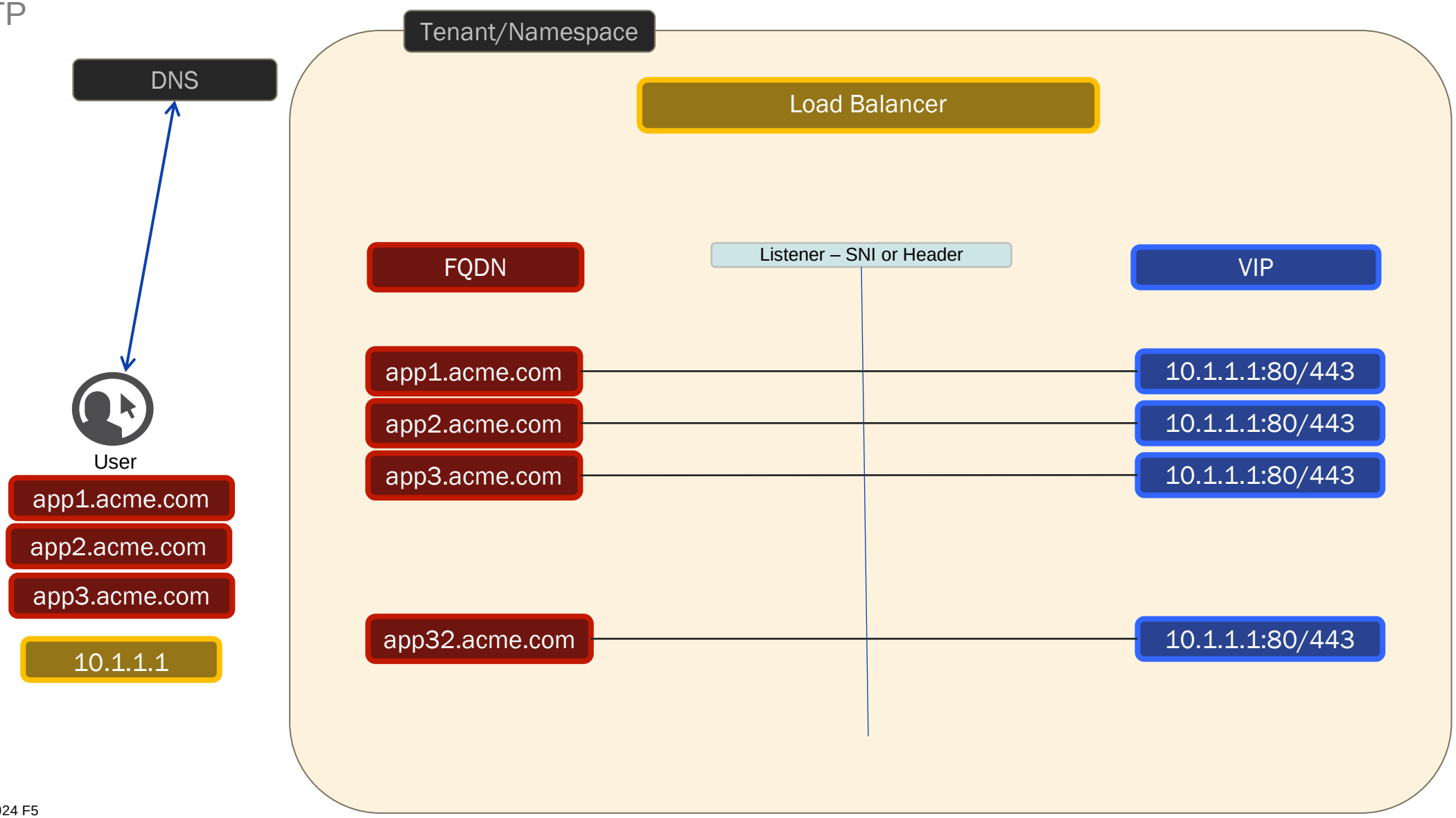
The XC load balancer—create

HTTP and TCP



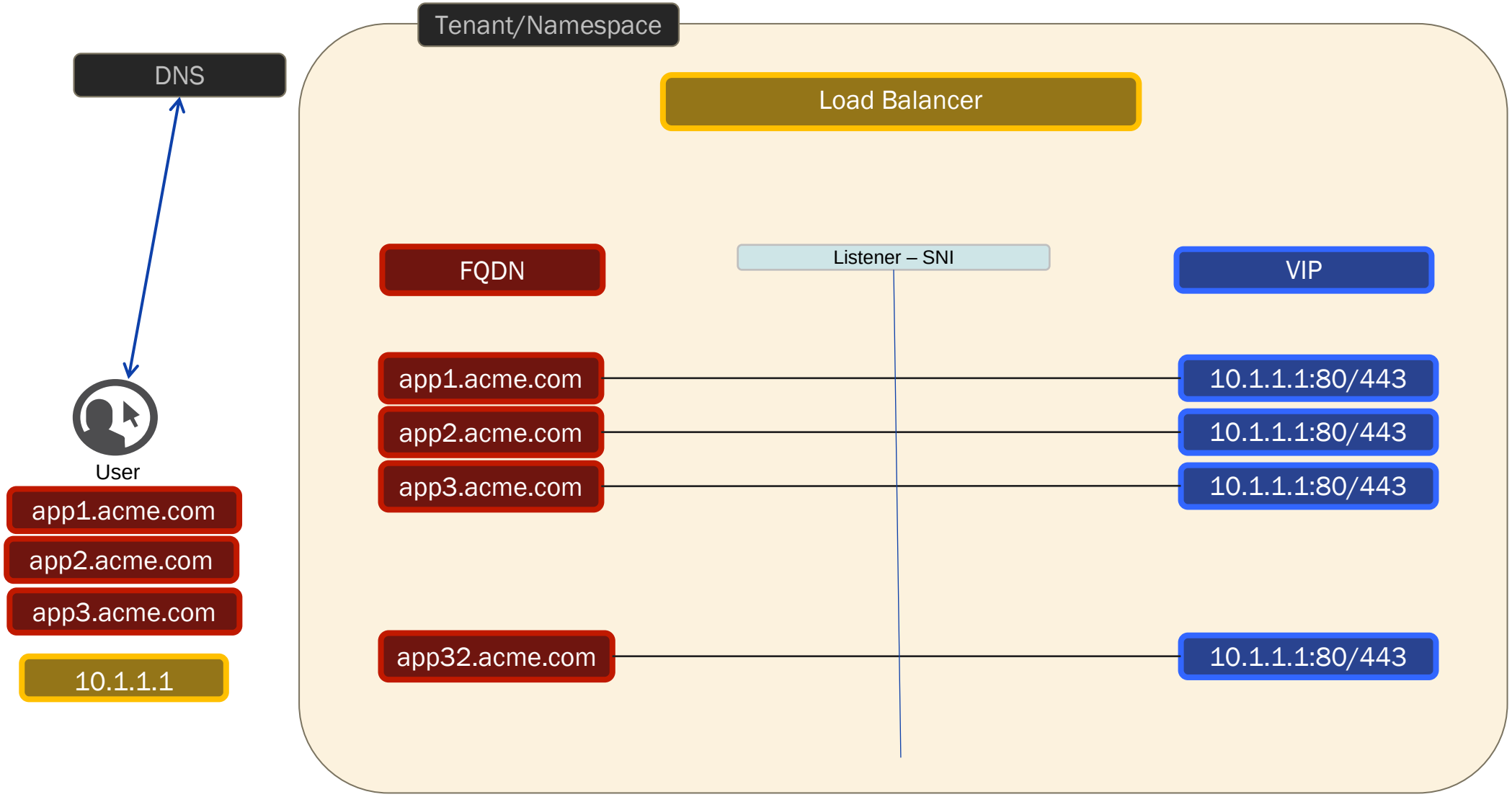
The XC load balancer—32 FQDN

HTTP

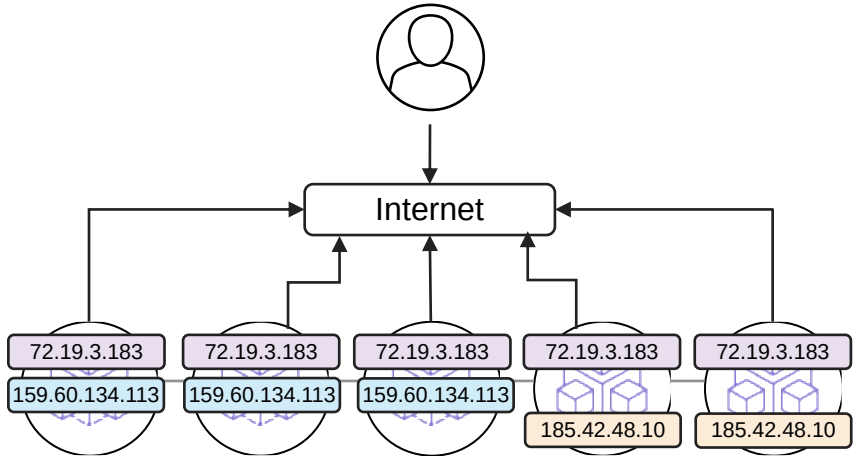


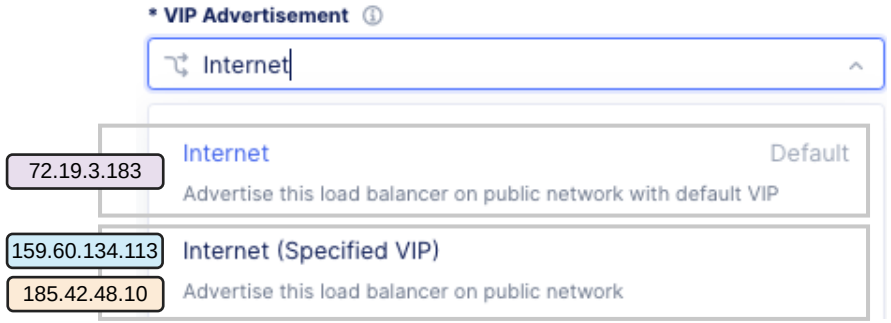
The XC load balancer—32 FQDN

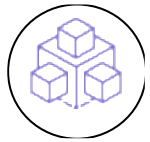
TCP



The XC load balancer—advertise (RE)

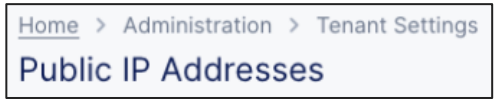






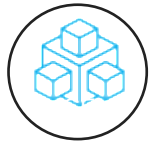
Advertise Policy

Specific IP	Specific Port
• Tenant IP • Add. Tenant IP • BYO Tenant IP	• Any



- Example of a customer bringing a /24 to F5 Distributed Cloud.
- 256 IPs are available to the customer to be used for different LBs.
- The customer can choose how these IPs are used, if they have LBs that share the same IP, or each LB gets its own IP

The XC load balancer—advertise (CE)



Advertise Policy

Specific IP	Specific Port
• Interface IP • Custom IP	• Any – Minus Restricted Ports

If picking up traffic on an interface IP of a site, choose which interfaces should listen.

Set which site should receive this listener and set the advertise policy.

If setting a custom IP, enter it here. Then update the site network interface that this custom IP should be advertised.

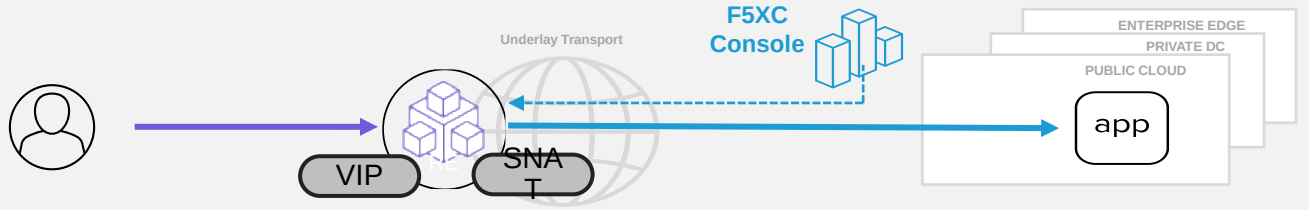
If you're defining multiple sites, you might choose to update the listening port for this specific site listener.

Distributed Cloud Platform

F5 Distributed Cloud—Topology Types

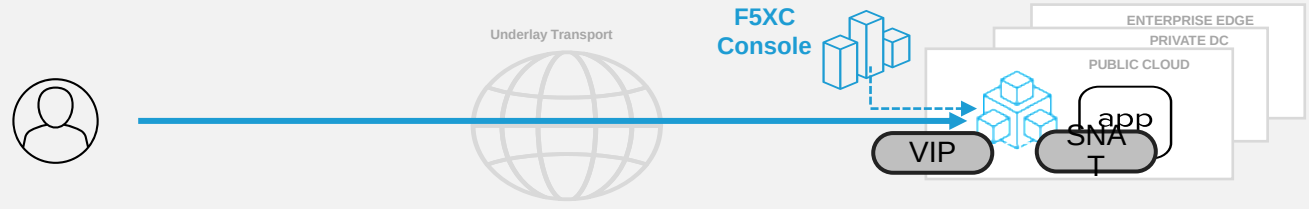
Regional Edge (RE)

Hosted in F5 Global Network
Shared Node (many customers)

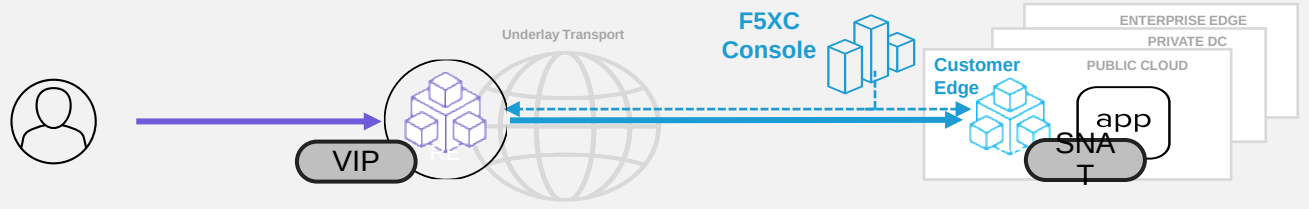


Customer Edge (CE)

Hosted in customer premise/public cloud
Dedicated Node (single customer)

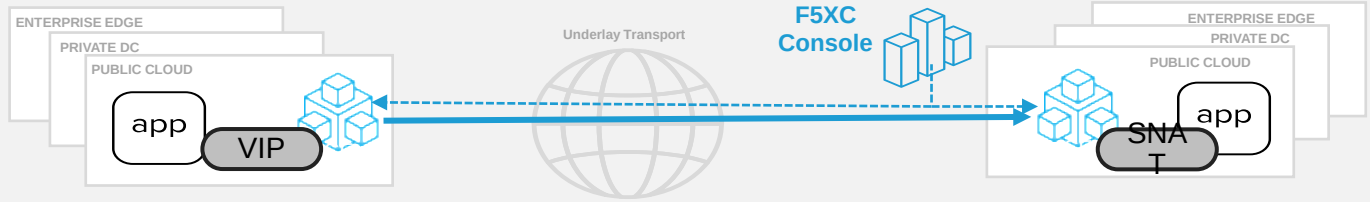


Hybrid (RE+CE)



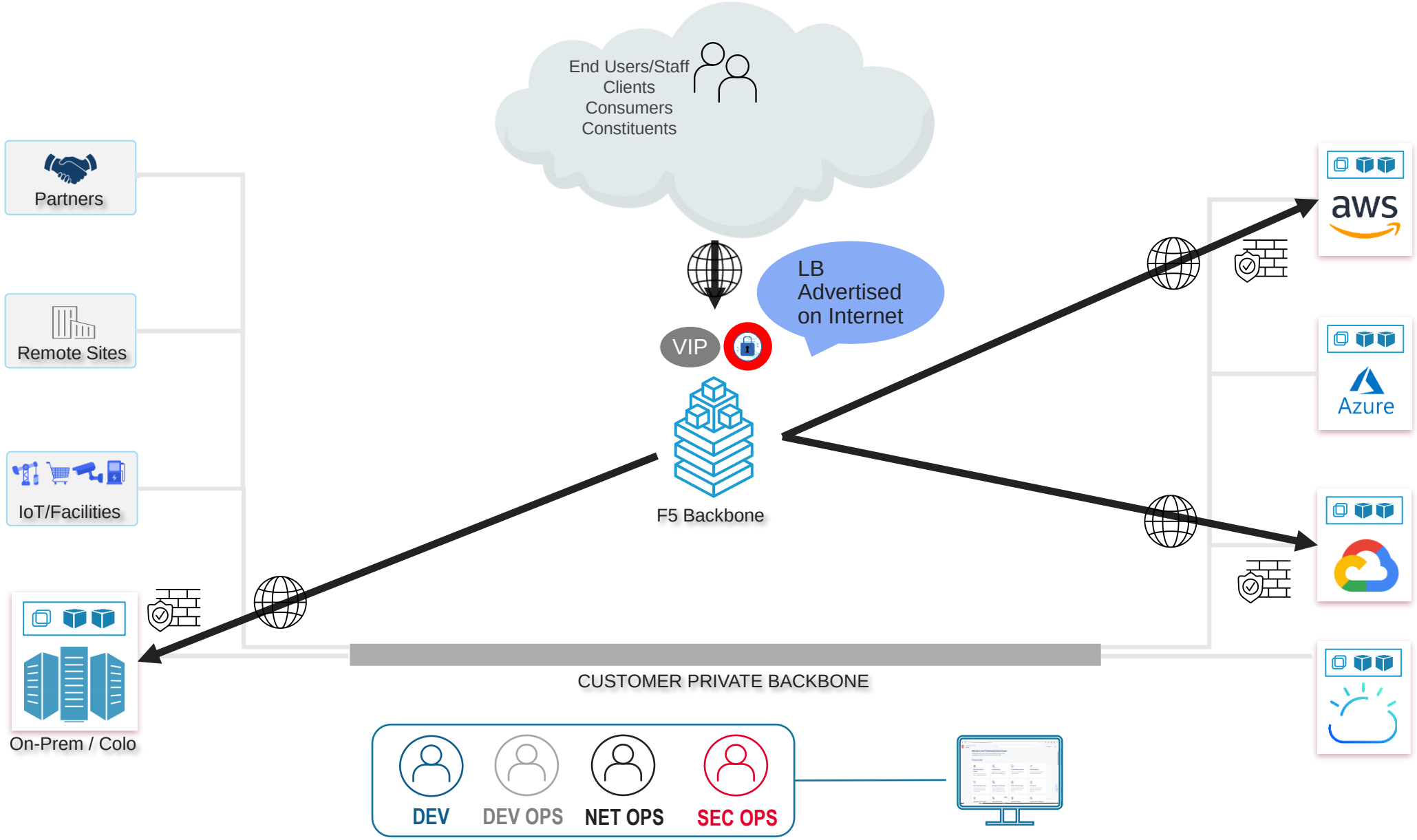
Customer Edge (CE) MCN

Hosted in customer premise/public cloud
Dedicated Node (single customer)

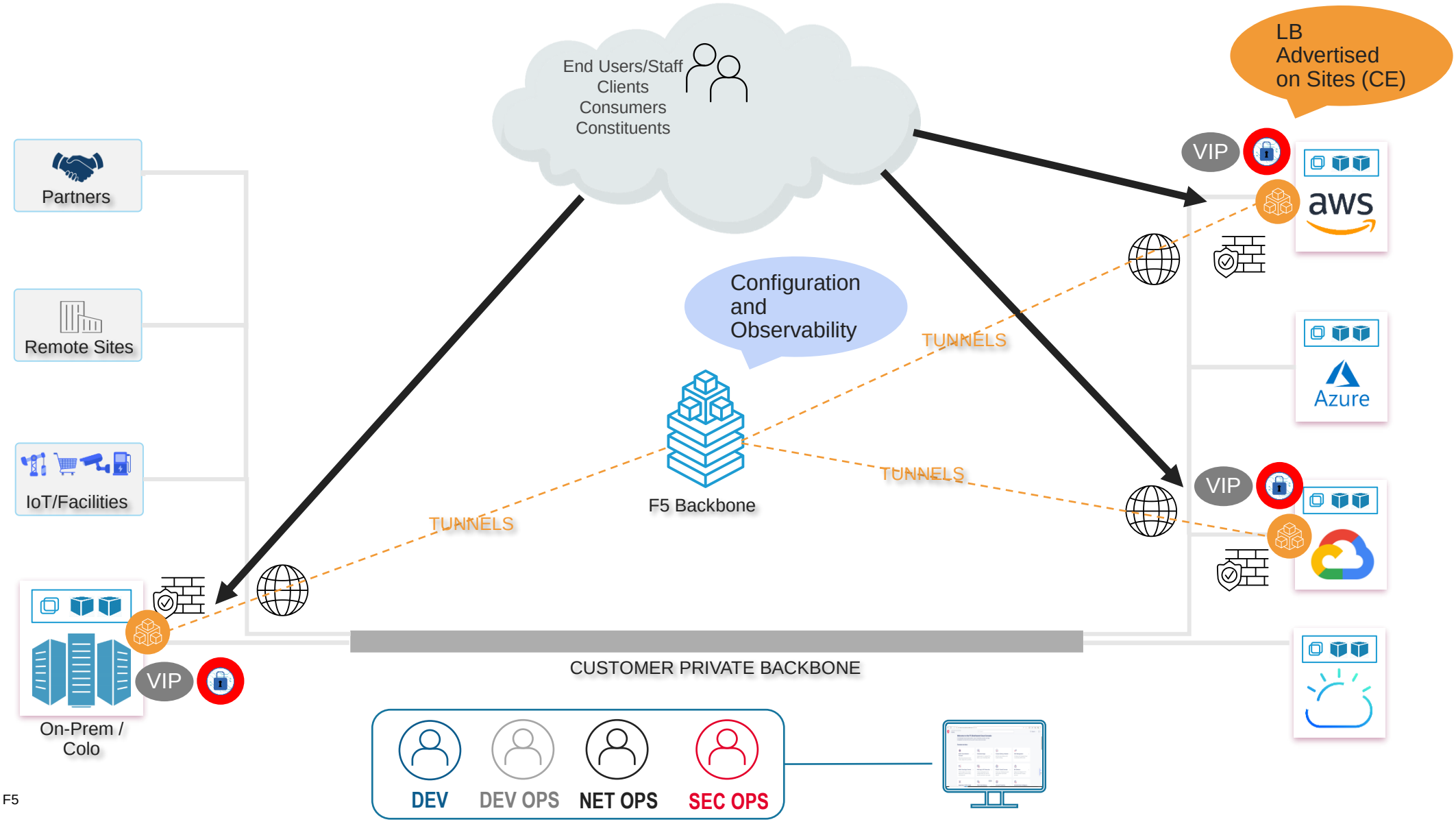


Topology types can be combined depending on the Enterprise Application Delivery requirements

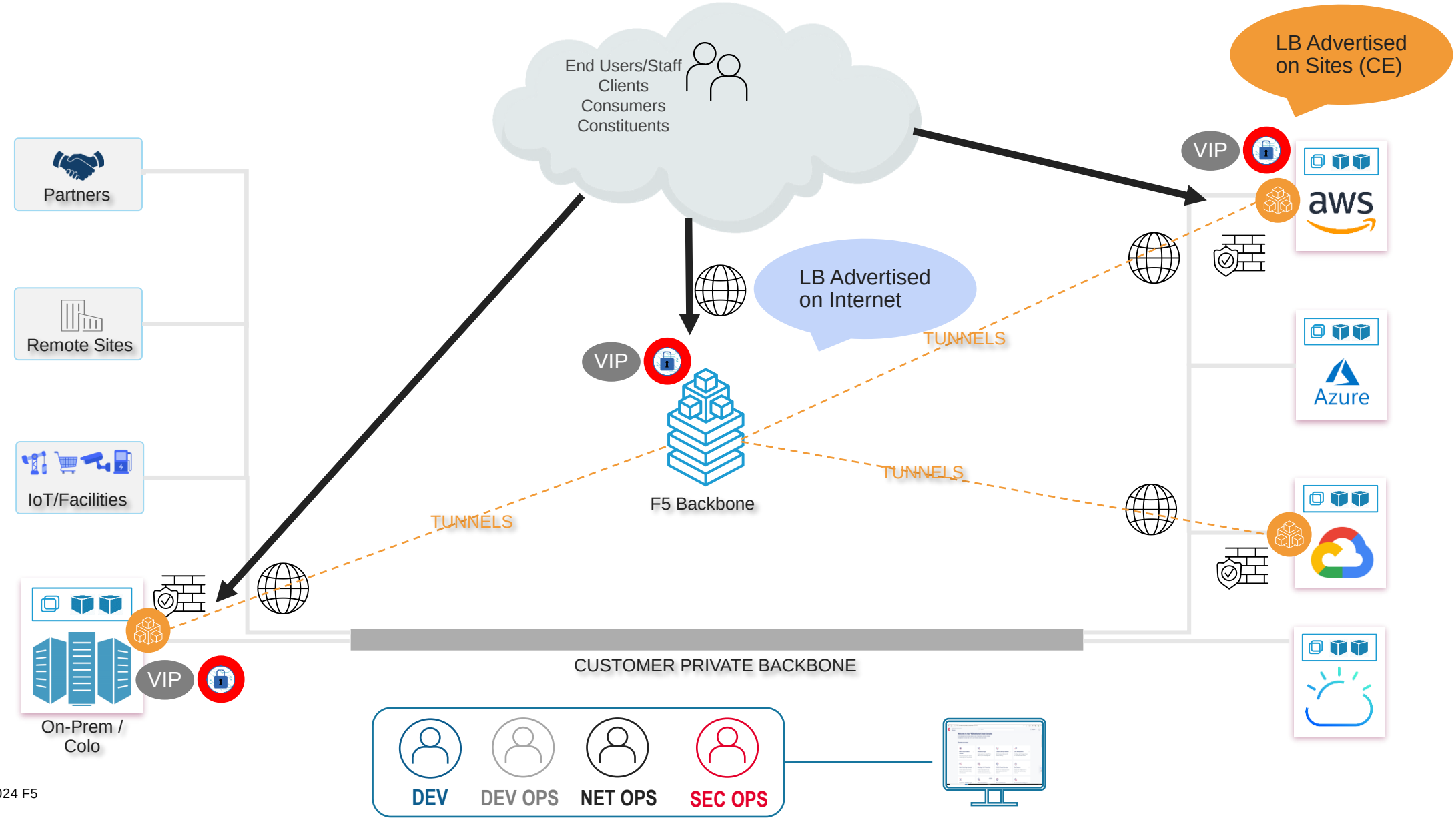
Internet-facing applications (RE only)



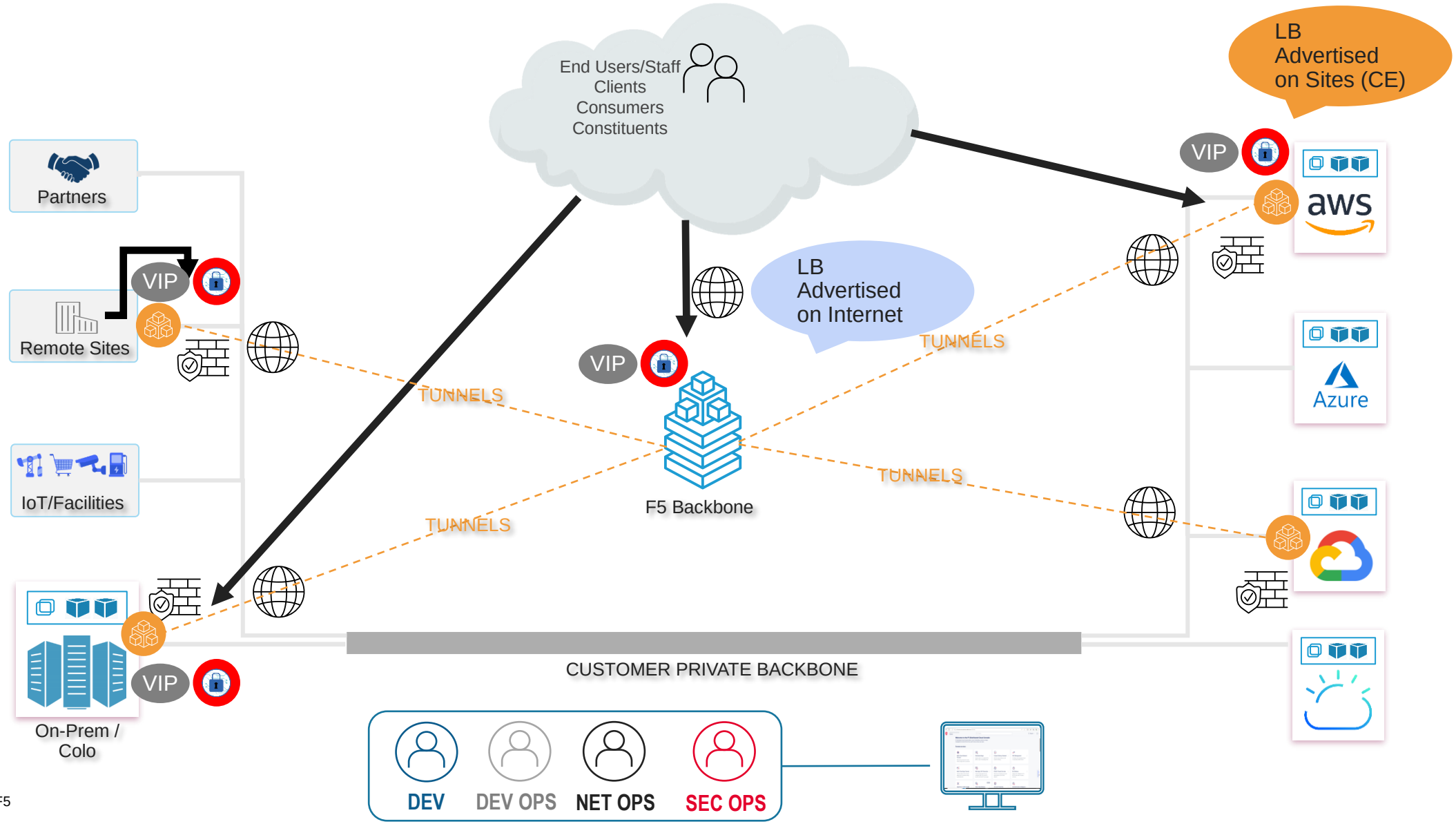
Internet-facing applications (CE Only)



Internet-facing applications (RE+CE)



Internet + internal applications (RE+CE)



Demo/walkthrough

My Function

```
function foo() {
    return bar;
}
```


Q & A