August 2020

BIG-IP LTM Essentials

LTM Essentials Hands On Lab Syllabus

- Networking Concepts, Pools, Virtual Servers, Load Balancing Methods
- SNAT, Profiles, Monitors
- Monitors cont’d, SSL termination
- iApps, F5 (Application Services Templates – FAST)
- High Availability

Assumptions

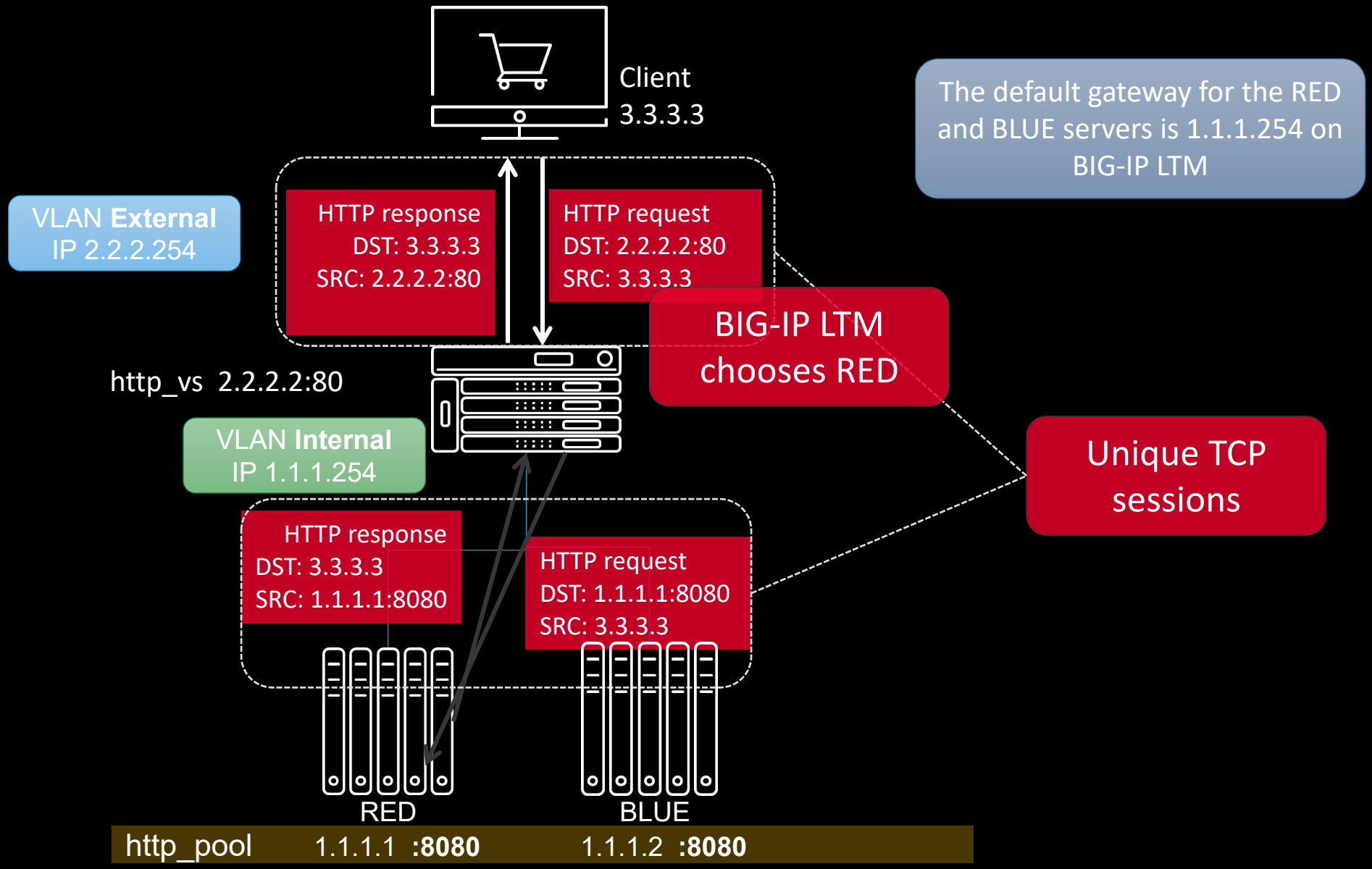
- Familiarity with licensing a BIG-IP
- Familiarity with initial BIG-IP Management Interface configuration
- Familiarity with provisioning BIG-IP Resources

Network Configuration

Overview of Networking

- TMOS is a full proxy architecture
  - Traffic must pass through BIG-IP to gain the benefits of TMOS
- Routed mode (recommended)
  - Real servers are on an internal network behind the BIG-IP
  - The BIG-IP is default gateway for the servers
  - The virtual servers reside on the external network
  - Accessible by the clients
- nPath/Direct Server Return Mode
  - Also know as, ***One-Armed mode***
  - Allows a BIG-IP to be inserted into existing networks without changing IP address structure
  - Not used frequently, but it is possible

Routed Mode

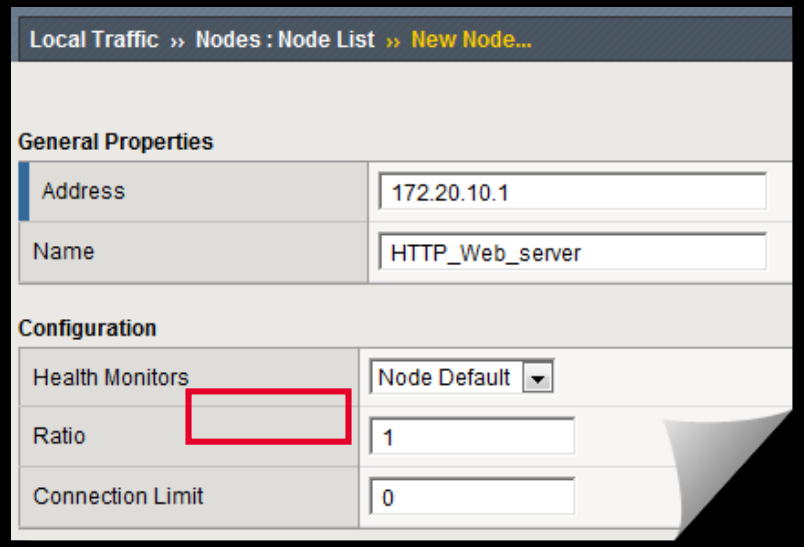

Client
3.3.3.3
The default gateway for the RED and BLUE servers is 1.1.1.254 on BIG-IP LTM
VLAN External
IP 2.2.2.254
HTTP response
DST: 3.3.3.3
SRC: 2.2.2.2:80
HTTP request
DST: 2.2.2.2:80
SRC: 3.3.3.3
BIG-IP LTM chooses RED
http_vs 2.2.2.2:80
VLAN Internal
IP 1.1.1.254
Unique TCP sessions
HTTP response
DST: 3.3.3.3
SRC: 1.1.1.1:8080
HTTP request
DST: 1.1.1.1:8080
SRC: 3.3.3.3
RED
BLUE
http_pool 1.1.1.1 :8080 1.1.1.2 :8080

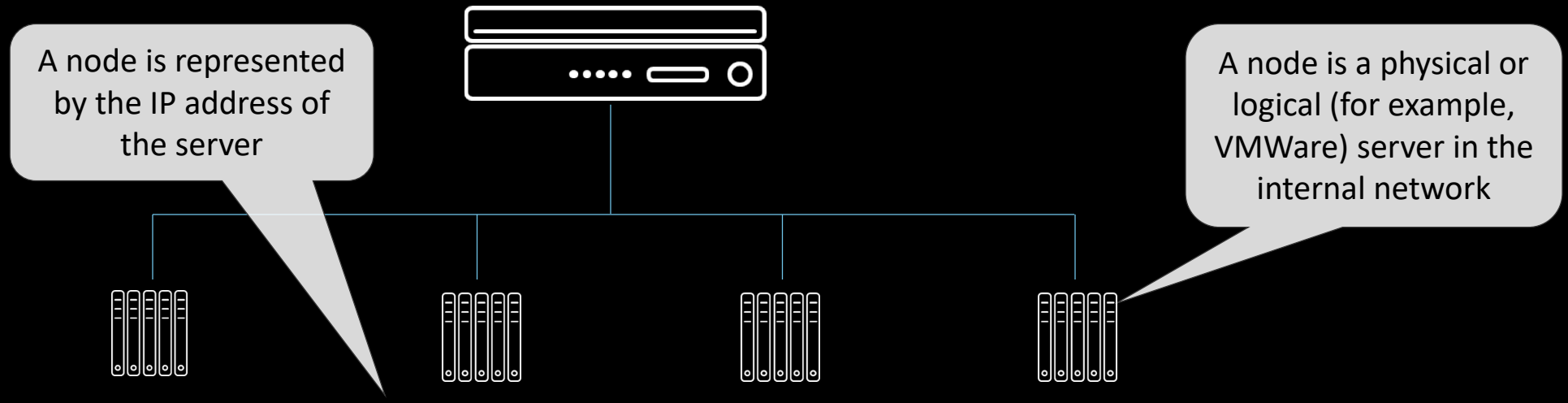
nPath/DSR (Direct Server Return)

- Similar to Single Arm Method of deployment
- Virtual Server IP should reside within the same subnet as physical servers (Nodes)
- Load Balanced Server default gateway is not the BIG-IP, but ofen is a Router or Firewall
- Network Traffic routes around the BIG-IP
- Asymmetric Routing
- Client IP address is retained
- Potentially exposes internal load balanced servers to security risk

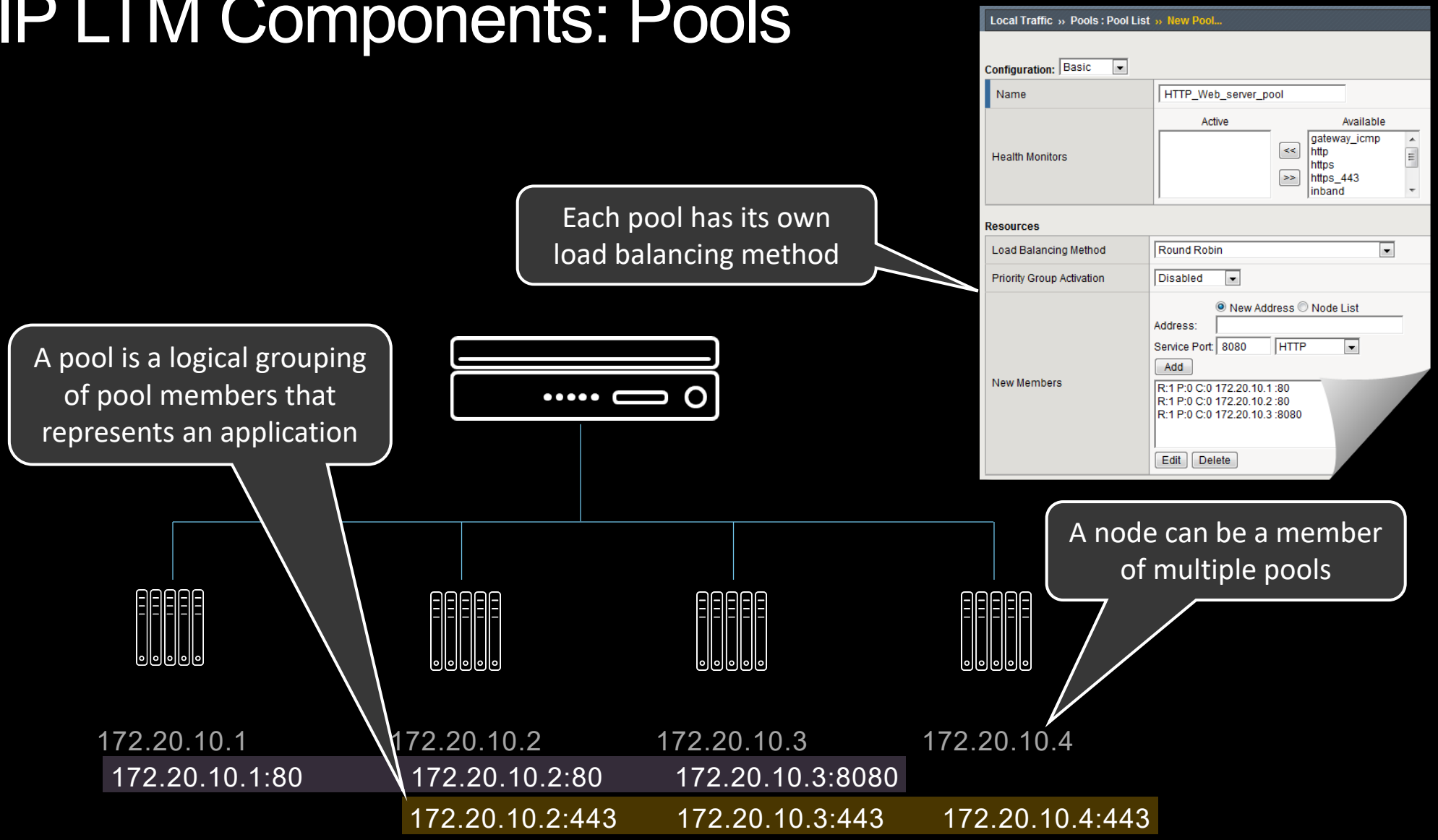
LTM COMPONENTS

BIG-IP LTM Components: Nodes

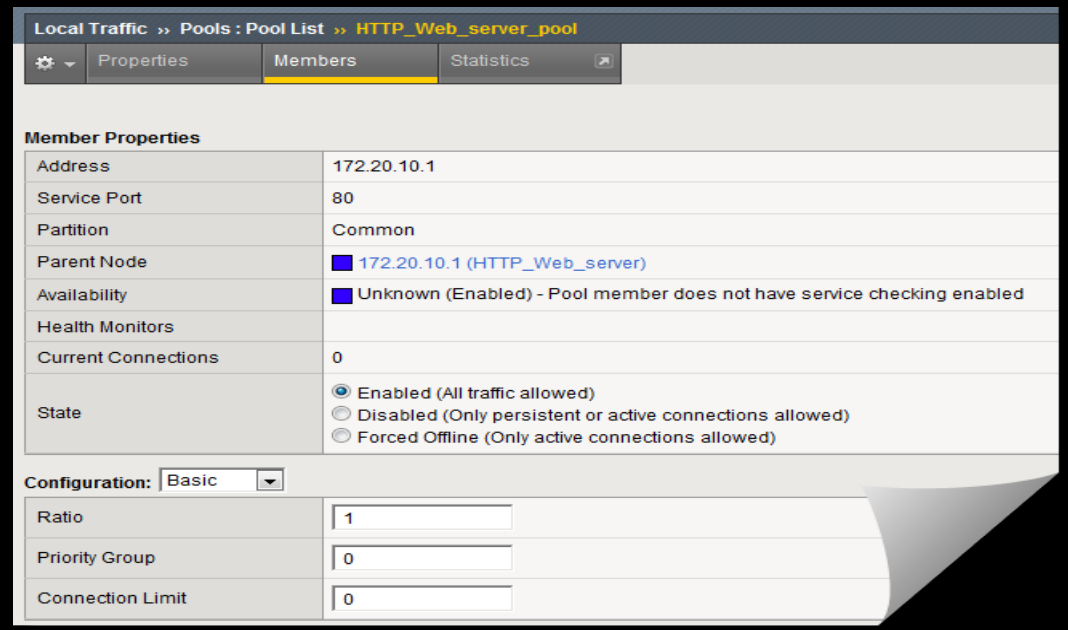




BIG-IP LTM Components: Pools



BIG-IP LTM Components: Pool Members



A pool member is a service running on a node, represented by the IP address of the node and service (port) number

A node can host multiple pool members

172.20.10.1
172.20.10.1:80

172.20.10.2
172.20.10.2:80
172.20.10.2:443

172.20.10.3
172.20.10.3:80
172.20.10.3:443

172.20.10.4
172.20.10.4:443

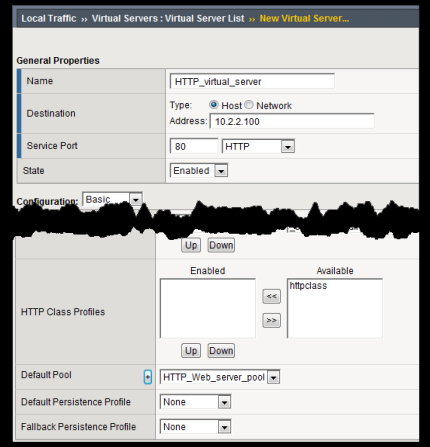
VIRTUAL SERVERS
(AND OTHER BIG-IP LISTENERS)

BIG-IP LTM Components: Virtual Servers

BIG-IP LTM is a default deny device; the virtual server is the most common way allow client requests to pass through

A virtual server is an IP address and service (port) combination that listens

Each virtual server will uniquely process client request that match its IP address and



10.2.2.100:80

10.2.2.100:443

10.2.2.225:8080

Each virtual server then directs the traffic, usually to an application pool

The virtual server translates the destination IP address and port to the selected pool member

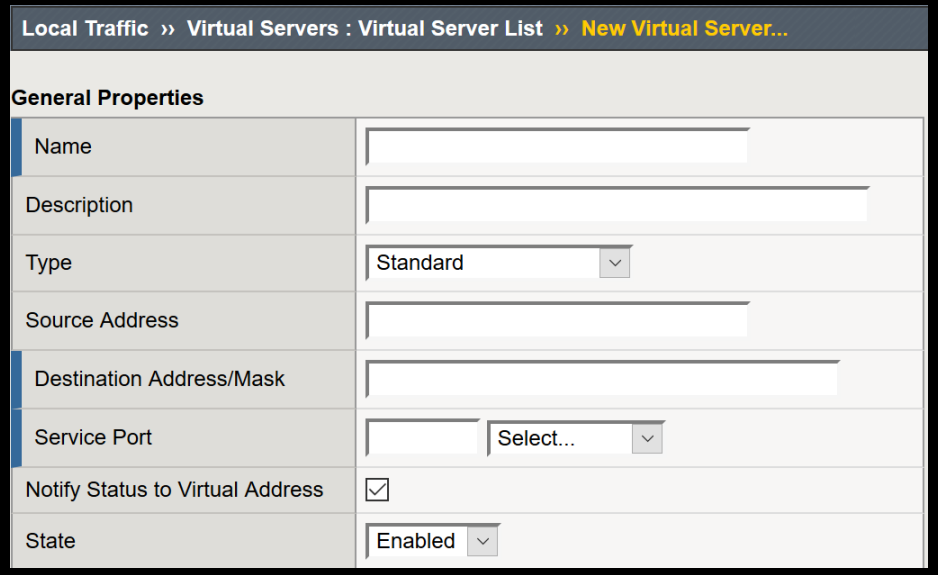
172.20.10.1 172.20.10.2 172.20.10.3 172.20.10.4

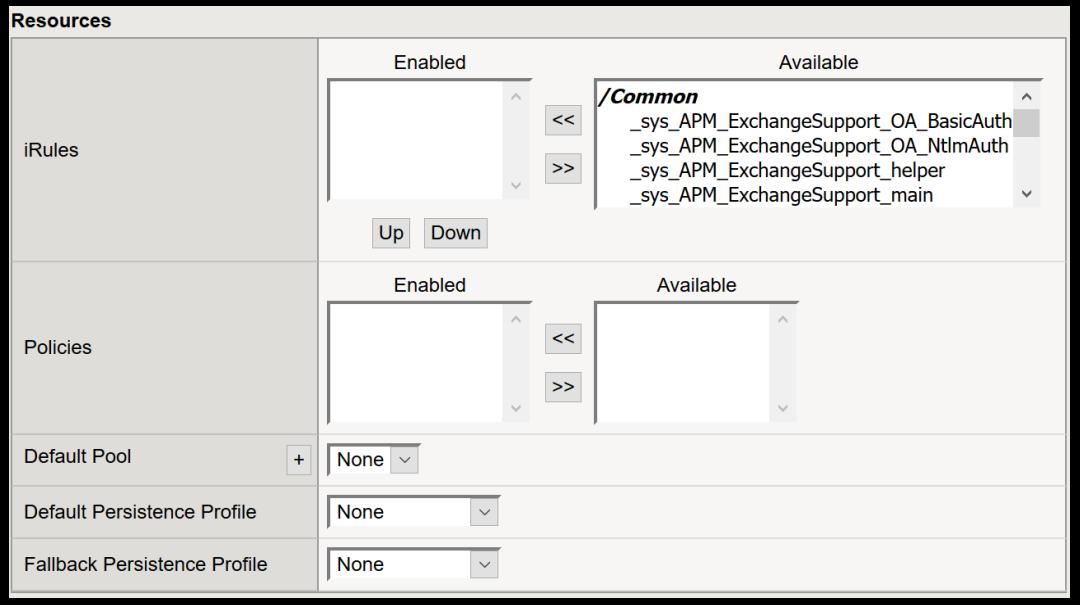
172.20.10.1:80 172.20.10.2:80 172.20.10.3:8080

172.20.10.2:443 172.20.10.3:443 172.20.10.4:443

Virtual Servers

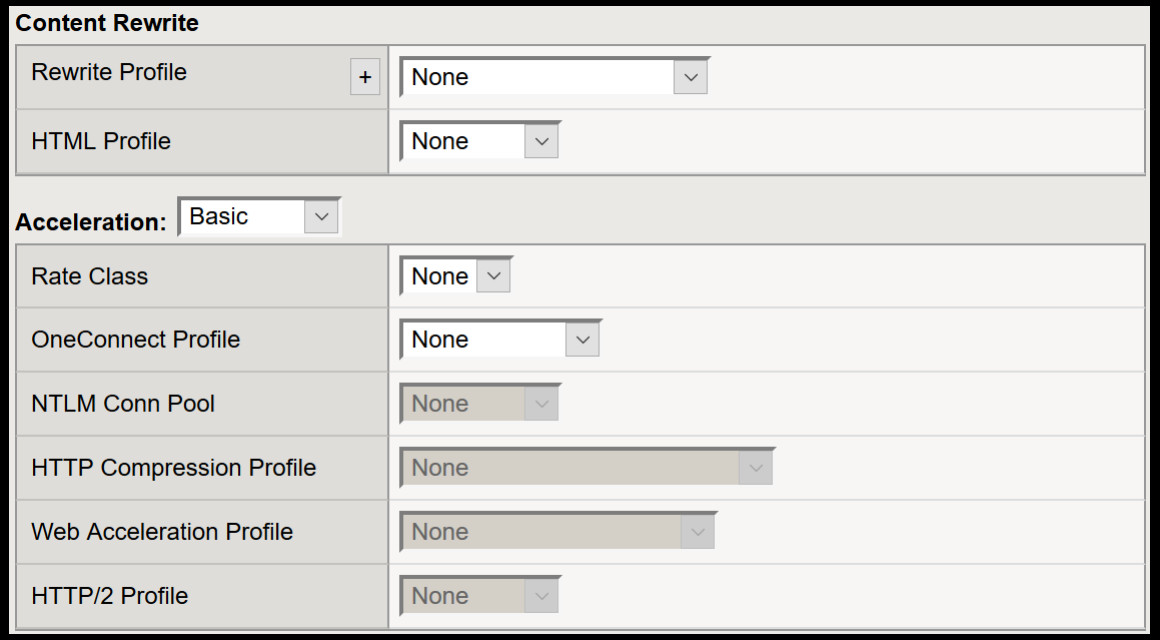
- One of the most important configuration components
- Determines what traffic is to pass
- Where the traffic goes
- How it is viewed/manipulated/validated (mostly via profiles)
- So in the last slides we saw virtual server basics (in and out) …..

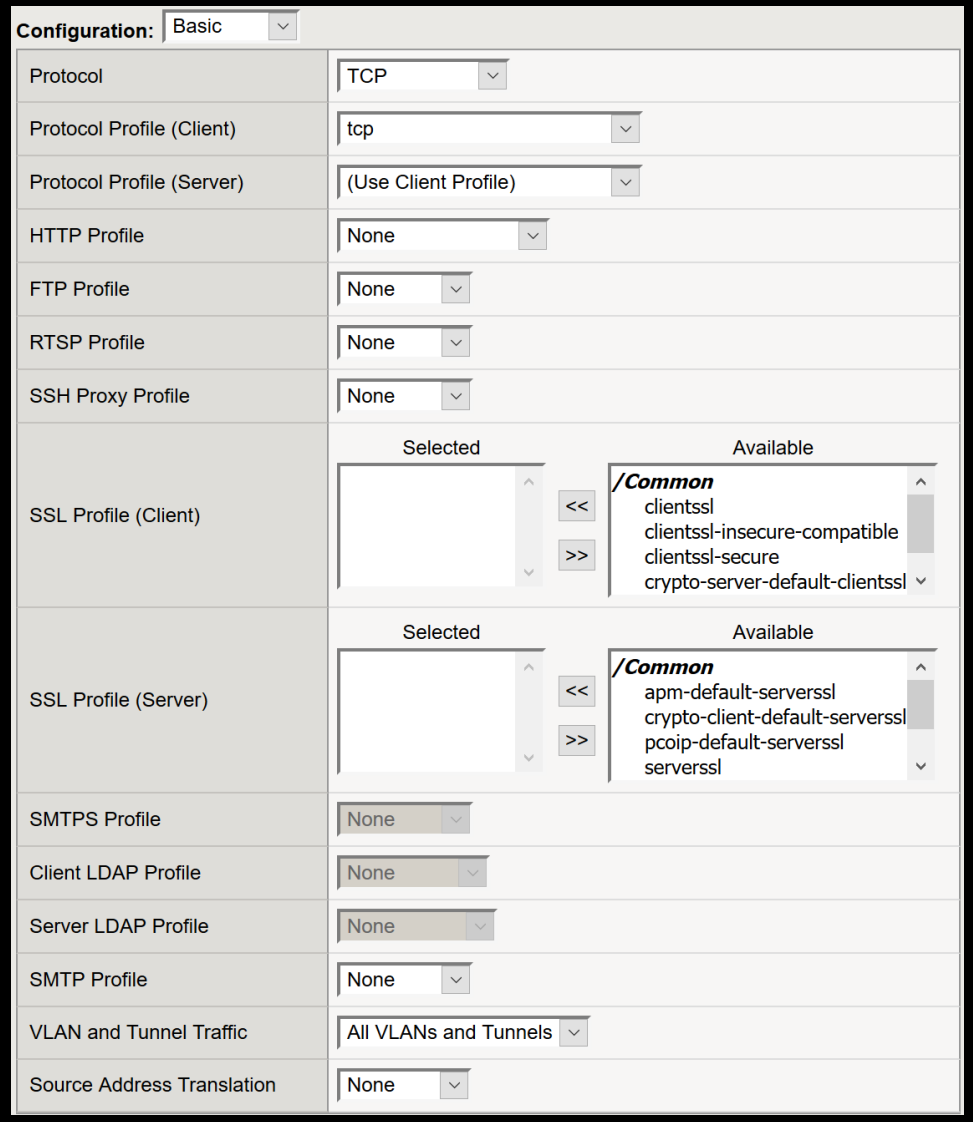




But there is so much more….

- And this is just the basic menu…
  - Layer 4-7 profiles
  - Restrictions on traffic
  - Source Address Translation





How Does a BIG-IP Handle Inbound Traffic

- A Virtual Server isn't the only listener
- Listeners are
  - Self IPs (Port Lockdown: None)
  - SNATs (Source initiated)
  - NATs (Two-way)
  - And of course Virtual Servers

Packet Processing Priority

1. Existing connection in connection table
2. Packet filter rule
3. Virtual server
4. SNAT
5. NAT
6. Self-IP
7. Drop

Load Balancing

A load balancing method is an algorithm or formula used to determine which pool member to send traffic

- Load balancing is connection based

Static load balancing methods distribute connections in a fixed manner

- Round Robin (RR)
- Ratio (Weighted Round Robin)
- Distributes in a RR fashion for members/nodes whose ratio has not been met

Dynamic load balancing methods consider one or more factors, such as the current connection count

It is important to experiment with different load balancing methods and select the one that offers the best performance in your environment

Dynamic Load Balancing Methods

Least Connections

- Fewest L4 connections when load balancing decision is being made
- Recommended when servers have similar capabilities
- Very commonly used

Fastest

- Balances based upon the number of outstanding L7 requests and then L4 connections
- Requires a L7 profile on the virtual server, else its just Least Connection
- Recommended when servers have similar capabilities

Observed

- Calculates a ratio each second based on the number of L4 connections
- Not recommended for large pools

Dynamic Load Balancing Methods

- Predictive
  - Calculates ratio base on the change between the previous connection counts and the current connection counts
  - Not recommended for large pools
- Weighted Least Connections
  - Based on how close the number of connections are to meeting the connection limit for a pool member or node
  - Requires connection limits be set on pool member or node
  - Recommended when servers have different capabilities
- Dynamic Ratio
  - Dynamically weights servers based on the results of SNMP/WMI queries
  - Requires SNMP_DCA , SNMP_Base, or WMI pool monitoring
  - Recommended when custom calculations are needed

Introduction to Monitors

A monitor is a test;

- Of a specific application. For an expected response. Within a given time

Monitors have common attributes

- Interval - time between each check
- Timeout - time required for a successful check to be received before BIG-IP marks the node as unavailable

BIG-IP LTM can use composite monitors, so it can apply multiple checks

- It can use all or some of the monitors to determine member status

Monitors can also use reverse logic

Monitors are served from the Self IP addresses

Profiles

A profile defines how a virtual server processes packets it receives

- Based on which profiles are assigned to the virtual server
- Based upon the profile's configured parameters
- The same profile can be associated with one or more virtual servers

Different profile types, different traffic processing capabilities

- Protocol profiles, such as, TCP and UDP
- SSL profiles, for client-side and server-side certificates and keys
- Service (L7) profiles, such as, HTTP, FTP, DNS
- And many more…….

Profiles have a parent/child relationship

- Changes to a parent profile are passed down to the child profile(s)

SSL Offload

- Terminates the SSL connection at BIG-IP
  - BIG-IP has full visibility into the application
  - Enables the use of iRules, Profiles, et al
  - Can decrypt/encrypt for 3rd party security devices (ie. IPS/IDS)
  - Can free up valuable server resources
  - Consolidated certificate and key management
  - Support for FIPS hardware-based key security
- Selectively insert/retrieve SSL client certificate information to be used in traffic management decisions

7	APPLICATION
6	PRESENTATION
5	SESSION
4	TRANSPORT
3	NETWORK
2	DATA LINK
1	PHYSICAL

LAB TIME

PLEASE WORK ON LAB 1, 2, AND 3

IAPPS AND FAST

iApps Overview

iApps provide F5 administrators a template-based solution for application deployment

Customizable framework

iApps consolidate the creation and management of virtual servers, profiles, monitors, policies, profiles, and iRules required to deploy and run an application.

Commonly used iApps are Office365, ADFS, Sharepoint, Citrix, Vmware View

iApps have been around for several years which is why we are going to talk about a new technology

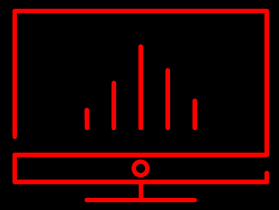
iApp Templates consist of five sections

- Attributes
- Presentation
- Implementation
- Macro
- Help

In Lab #4 you will have an opportunity to deploy a relatively simple iApp

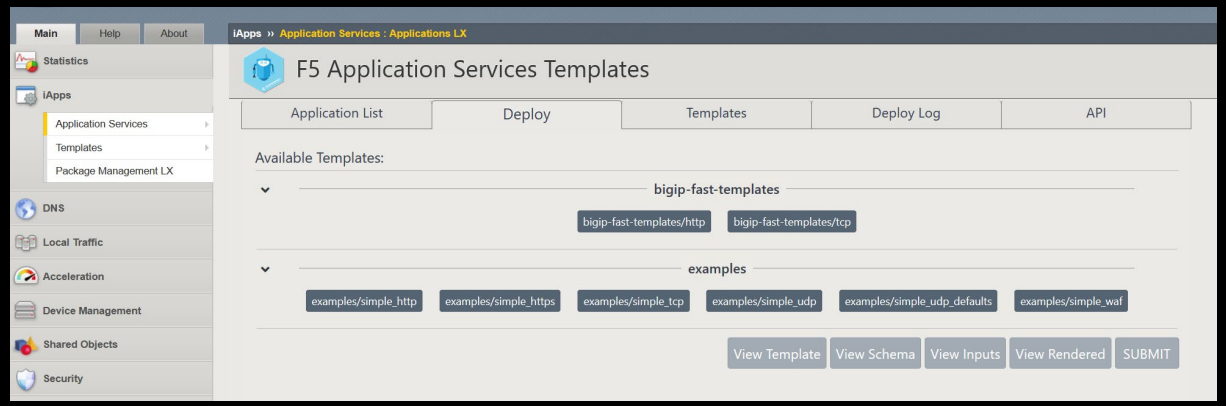
F5 Application Services Templates (FAST)

The next generation of Templating at F5

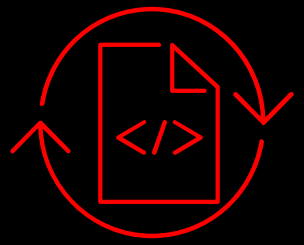


GUI

- New front end templating system for BIG-IP (initial target)
- Generated with cross-platform templating framework inputs
- Consistent UI/UX for creating, provisioning, and managing F5 application services and policies



Why Should I Care?



Cross-platform templating framework

- Declarative framework for working with current and future F5 solutions
- Unifies and simplifies customer experience for working with the F5 solutions portfolio

seamless integration with automation tools like Postman, CI/CD pipelines, and (multi) cloud instances.

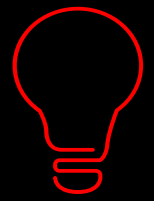
API driven integration

The lab exercise will leverage Postman and connect to a BIG-IP via API calls

FAST Benefits

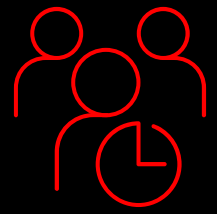
FAST makes working with f5 technologies easier and more streamlined

- **Creates a “one stop” app services shop**
- Unifies templating across the F5 portfolio via API
- Enables better integration with third-party solutions
- Extends popular “single API” approach



Aligns to “modern” app development approaches

- Leverages modern languages
- Integrates with automation tools, CI/CD pipelines, and cloud
- Gives AppDev and DevOps more freedom
- Increases deployment flexibility



Extends life of your F5 investment

- Integrates with current and future F5 solutions
- Offers flexibility and composability
- Democratizes template creation
- Enables specialized support model

Where Can I Learn More?

FAST LINKS

- FAST Download (GitHub)
- FAST Documentation
- FAST FAQ
- Questions? *solutionsfeedback@f5.com
- Bugs & RFEs: Please submit GitHub issues

DEVICE SERVICE CLUSTERS (DSC)

HIGH-AVAILABILITY

Device Service Cluster (DSC)

DSC is a series BIG-IPs supporting each other

- May also be referred to as Centralized Management Infrastructure (CMI)

Each BIG-IP has a Device Object for itself containing;

- Unique device information
- A Certificate for building trusts
- Device HA and failover settings for the local device

BIG-IPs are then placed in Device Trust Groups

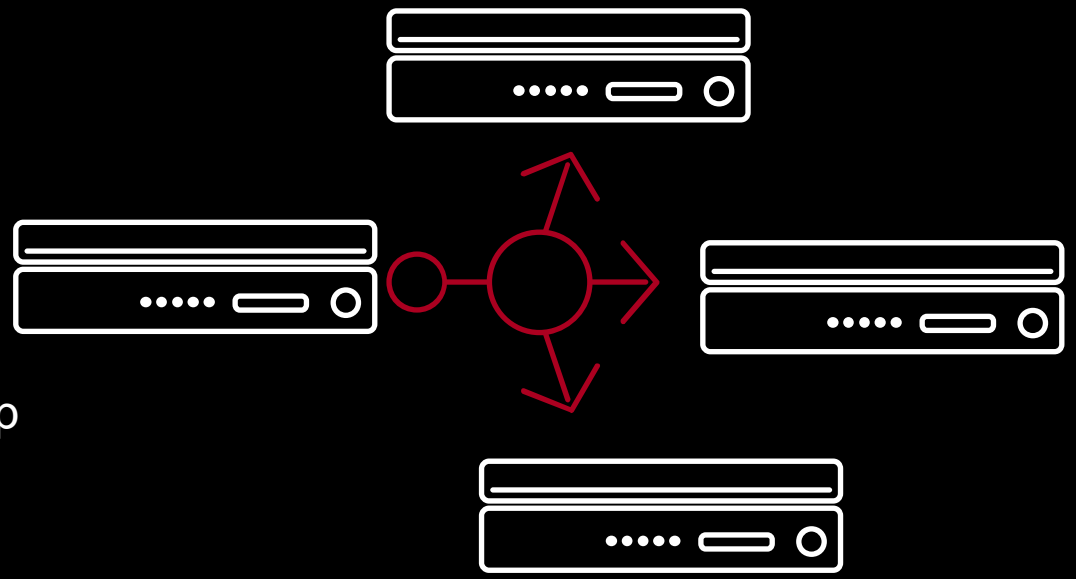
- Exchange certificates for secure communications
- Exchange HA settings

BIG-IPs in a Trust Group are combined into Device Groups

- A device group may support config sync and failover
- Or synchronization of selected configuration items only

Sync-Failover Device Groups

- Logical grouping of HA devices
  - F5 provides N+M redundancy
    - N Active units + M standby units
  - Mirroring requires only two devices be a part of the group
- A device can only be part of one sync-failover group



Sync Only Device Groups

Allows flexible membership

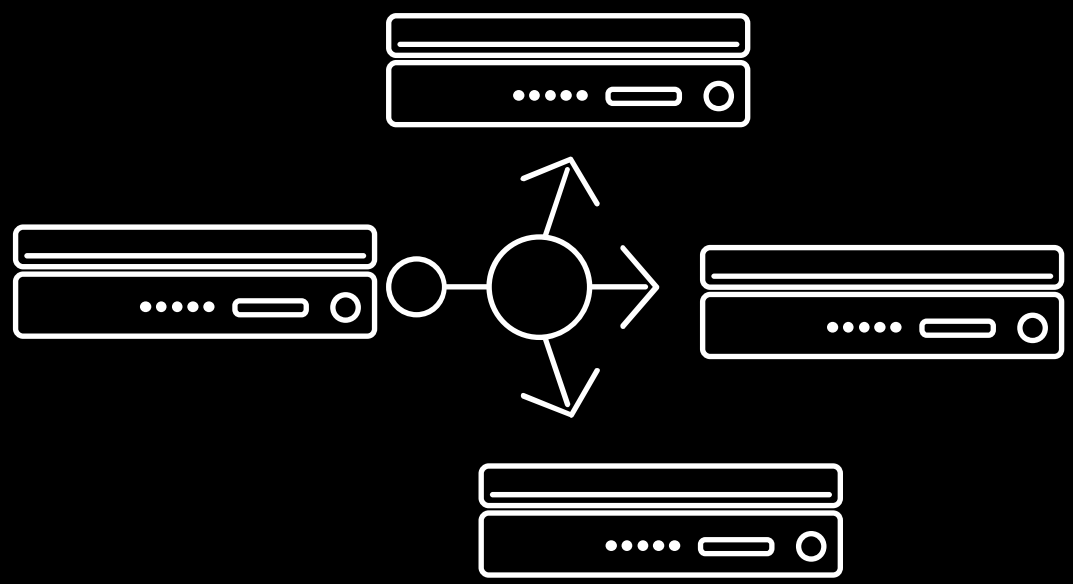
- Different hardware platforms
- Different license/modules

- Can be configured to auto-sync objects

- Max of 32 Sync-Only groups are supported

Device trust uses built-in sync-only group “device_trust_group”

- Auto-sync enabled
- Adding devices to trust-domain auto-adds to device_trust_group



- Certificates
- CRL
- Data groups
- External monitors
- iApps
- iRules
- Policies
- Profiles

LAB TIME

PLEASE WORK ON LAB 4 AND 5