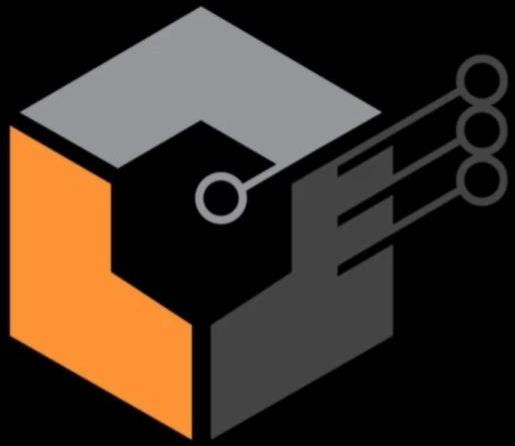
F5 101 Exam Preparation

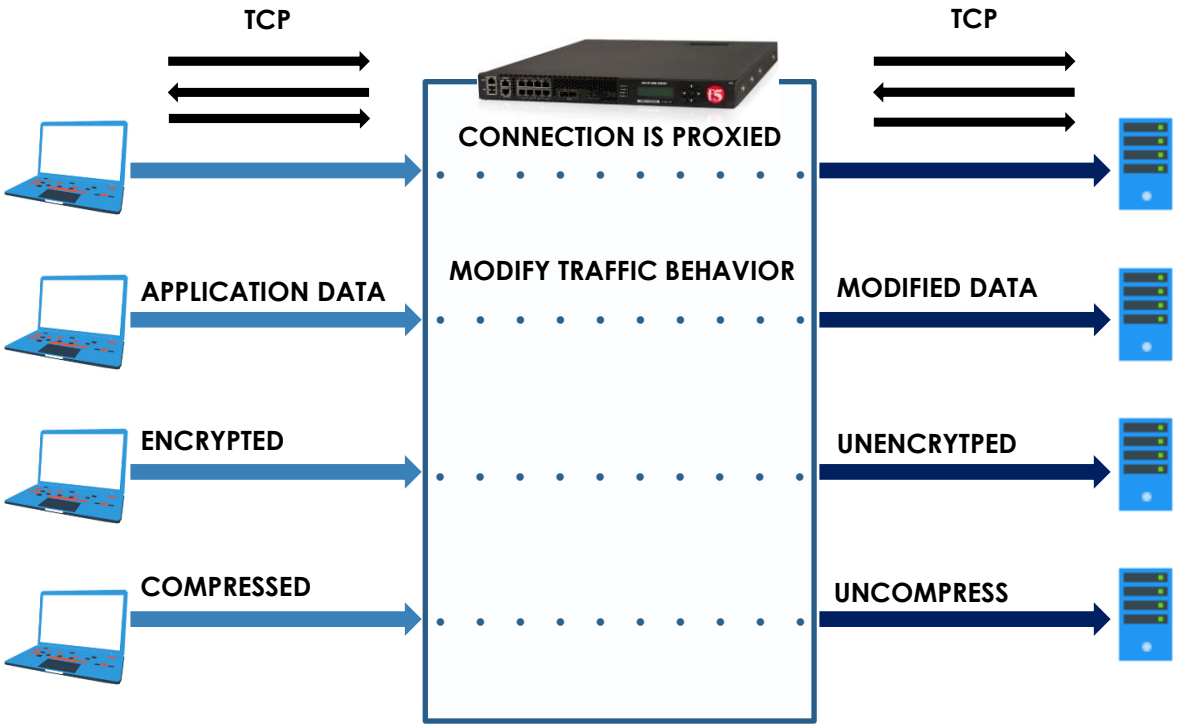
Application Delivery Controller Overview



ZURIEN

www.zurien.com

Introduction to Proxy Servers



Full Proxies

- Maintains two separate connections
- Completely understands applications
- It can examine both application request and response

Introduction to Proxy Servers

Proxy Servers / Proxies / Web Proxy / HTTP Proxy

- Often configured and used for web purposes
- Sits between the client and the server
- Clients communicate to proxy while proxy communicates the destination web server

Types of Proxies

- Forward Proxies
- Reverse Proxies
- Half Proxies
- Full Proxies

ADC Overview

Application Delivery Controller (ADC)

- Is a computer network device in a data center
- Remove load from the web servers as it helps applications direct user traffic from and to servers
- Includes many OSI layer 3-7 services which happen to include load-balancing
- Offer more advanced features such as content redirection and server health monitoring

Other features

- IP Traffic Optimization
- Traffic Chaining/Steering
- SSL Offload
- Web Application Firewall
- Carrier Grade NAT
- The list goes on

ADC Overview

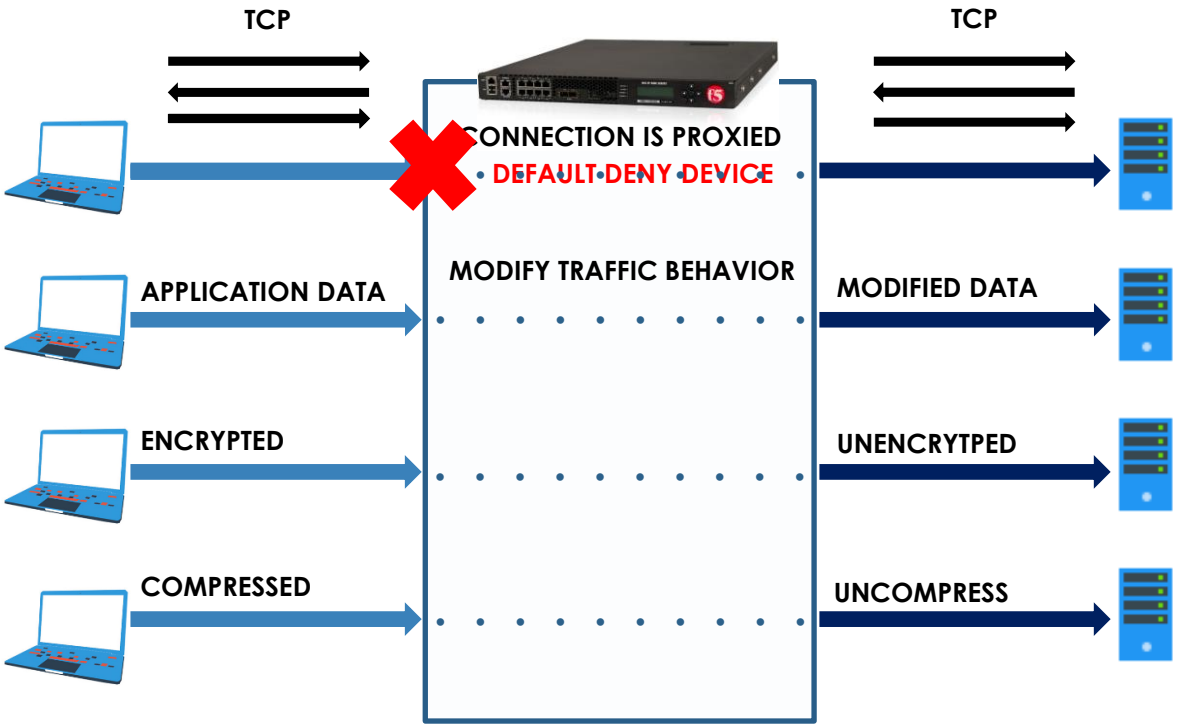
F5 BIG-IP

- Application Delivery Controller High performance appliance
- Comes in Hardware, Chassis/Blade and Virtual Appliance
- Programmability feature
- Modularized Software

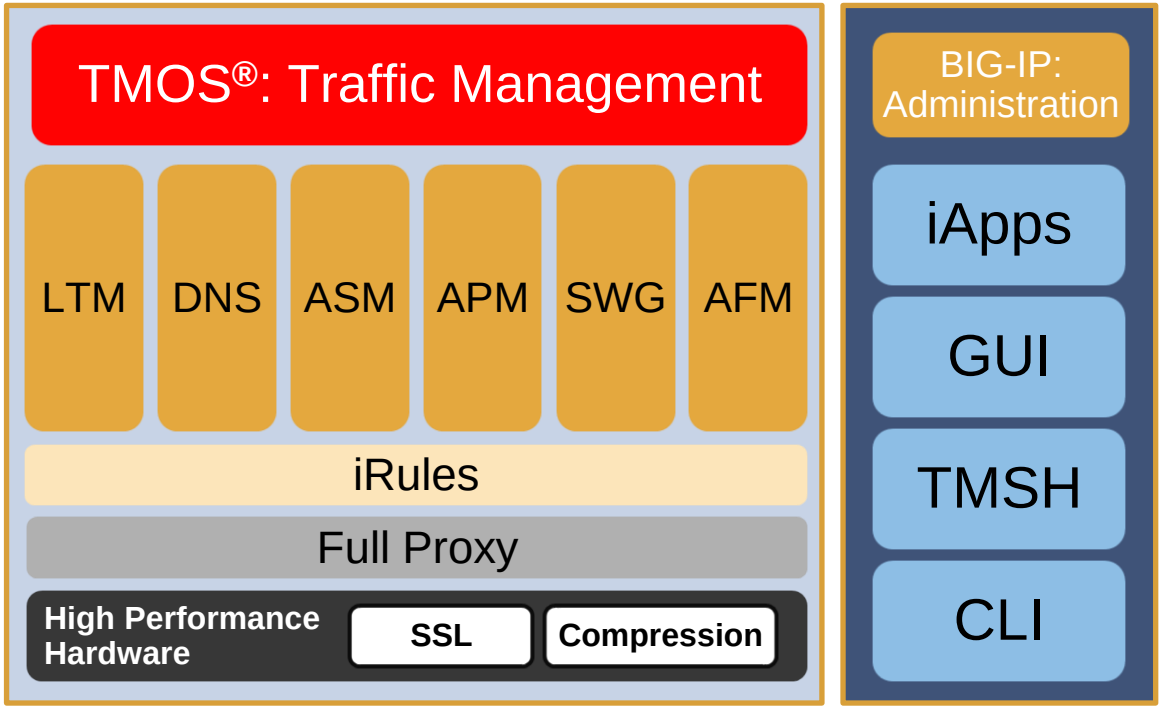
Modules can be added:

- Local Traffic Manager (LTM)
- BIG-IP DNS (Formerly called GTM)
- Application Security (ASM)
- Access Policy Manager (APM)
- Advanced Firewall Manager (AFM)

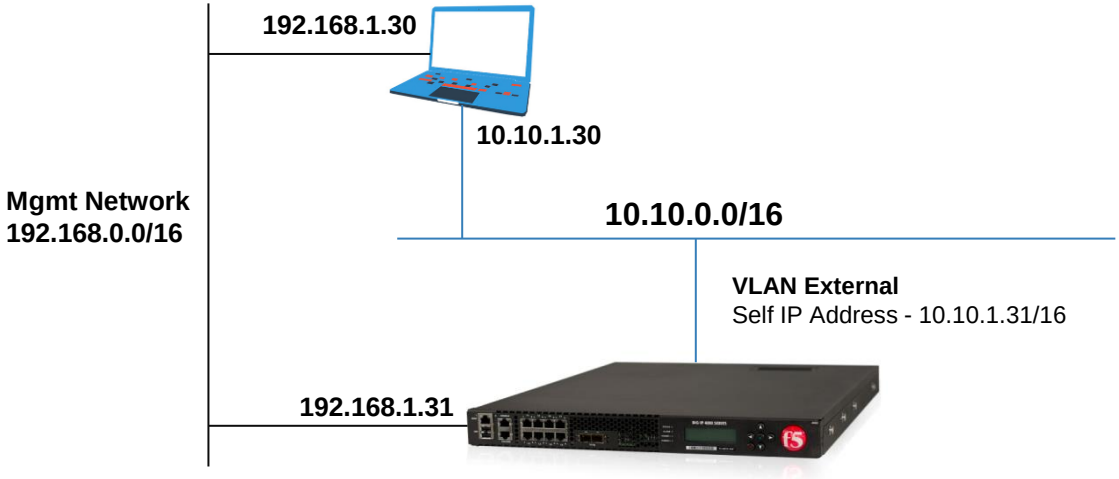
ADC Overview



ADC Overview



ADC Overview



Management Access

- Default IP 192.168.1.245 for Hardware
- DHCP Client for Virtual Edition
- Only via SSH and HTTPS
- Default SSH credentials – root/default
- Default HTTPS credentials – admin/admin

Port Lockdown

- Filtering options
- Allows BIG-IP management access thru External and Internal VLANs
- External VLAN by default is set to none

ADC Overview

Local Traffic Manager (LTM)

- Load Balancing and Monitoring
- Application Visibility and Reporting (AVR)
- L7 Intelligent Traffic Management
- Core Protocol optimization (HTTP, TCP, SPDY, SSL)
- SSL proxy and services
- Application Acceleration – caching, compression, bandwidth controller
- SYN flood protection

ADC Overview

BIGIP DNS (formerly known as GTM)

- Global Server Load Balancing
- DNS Services
- Global application High-Availability
- Geolocation
- Real-time DNSSEC
- DNS DDoS Attack protection

ADC Overview

Application Security Manager (ASM)

- PCI Compliant Web Application Firewall
- Compressive attack protection such as Cross-site Scripting, SQL Injection, Session Hijacking, Sensitive Data Exposure etc.
- Web scraping prevention
- Brute Force Mitigation
- Layer 7 DDoS protection
- Rapid Deployment
- Manual and Automated Policy Building

ADC Overview

Application Policy Manager (APM)

- SSL VPN Remote Access solution
- Identity and Access Management
- Scales up to 2 Million concurrent access sessions
- AAA Integration – Active Directory, LDAP, RADIUS, RSA SecureID
- BYOD enablement
- Single sign-on enhancements (Identity Federation with SAML 2.0)

ADC Overview

Advanced Firewall Manager (AFM)

- Data Center Firewall Operates in Layer 2 – 4
- Network Firewall – Policies & Rules
- DoS/DDoS Protection – Attack Vectors
- Port Misuse
- Intrusion Protection System (IPS)
- Logs and Reporting

ADC Overview

Resource Provisioning

- You can manage the provisioning of licensed modules on the BIG-IP® system along with system memory, disk space, and CPU usage

Four Available Resources Allocation Settings for Modules:

- None/Disabled - Specifies that a module is not provisioned. A module that is not provisioned does not run.
- Dedicated - Specifies that the system allocates all CPU, memory, and disk resources to one module. When you select this option, the system sets all other modules to None (Disabled).
- Nominal - Specifies that, when first enabled, a module gets the least amount of resources required. Then, after all modules are enabled, the module gets additional resources from the portion of remaining resources.
- Minimum - Specifies that when the module is enabled, it gets the least amount of resources required. No additional resources are ever allocated to the module.

ADC Overview

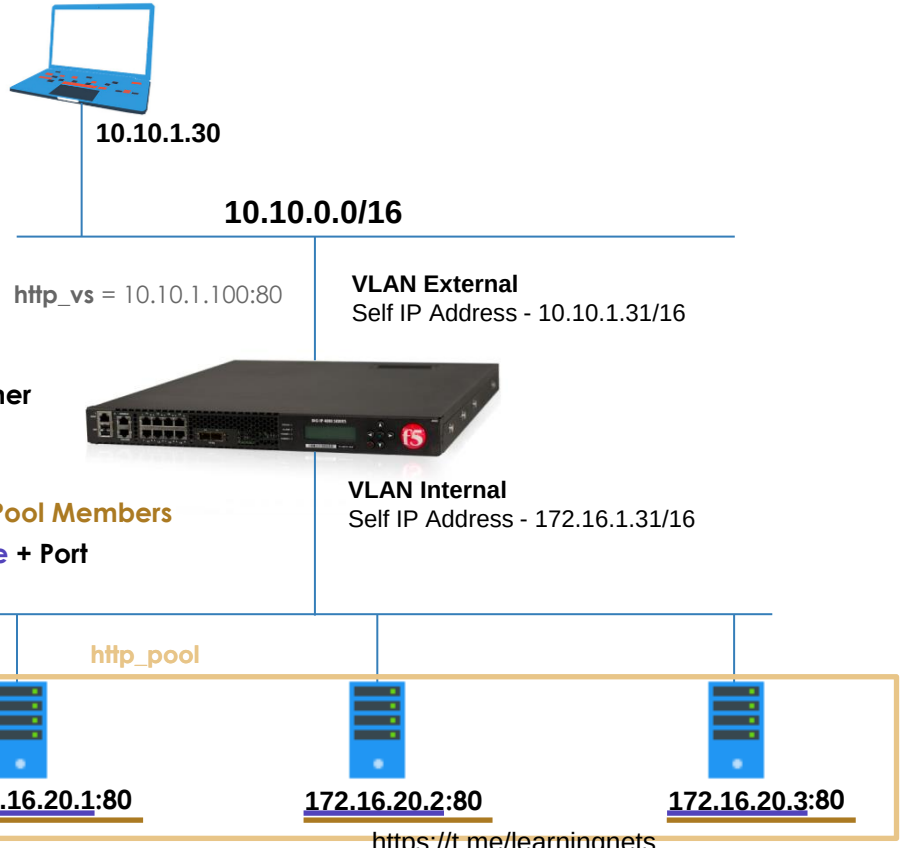
Other Features

- iRule – scripting tool use to extend BIG-IP capabilities
- iControl – API allows F5 BIG-IP device to integrate with 3rd party systems
- iApps – user-customizable framework for deploying applications
- iHealth – System Diagnostic Tool

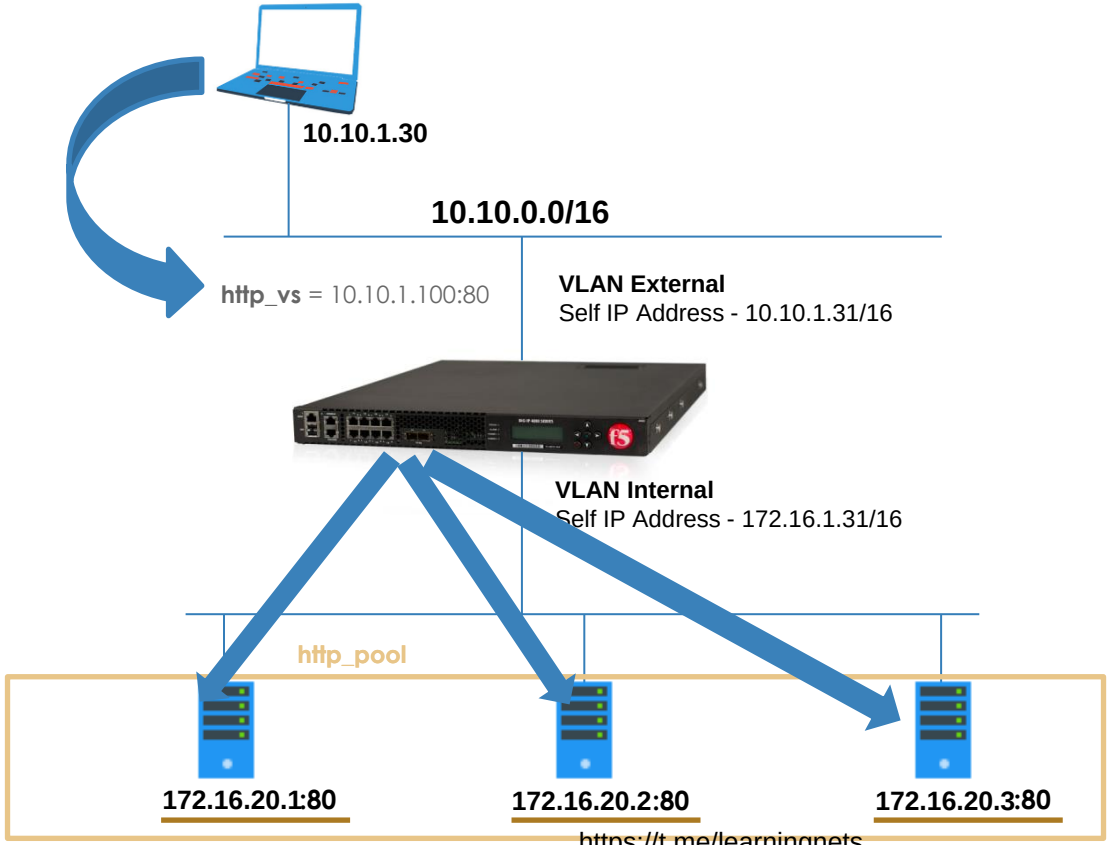
BIG-IQ

- Central point of control for F5 physical and virtual devices
- Inventory up to 200 BIG-IP devices
- Upgrade devices
- Monitor SSL certificates
- iHealth Integration

Load Balancing Concepts



Load Balancing Concepts



Load Balancing Concepts

Static Load Balancing

- Round Robin (default)
- Ratio

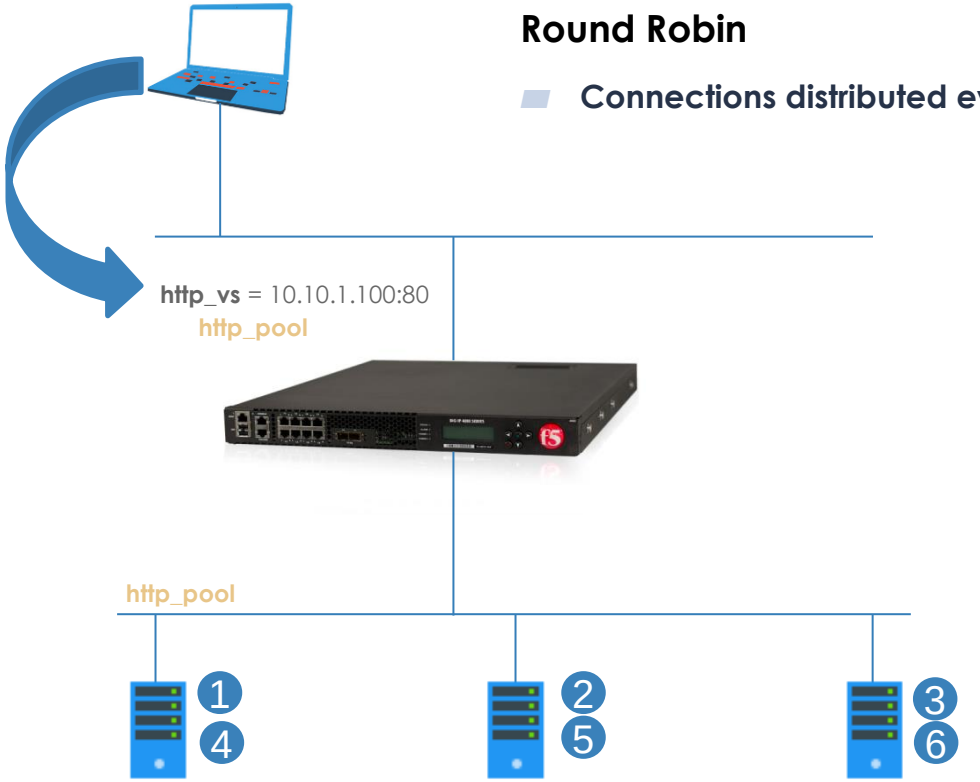
Dynamic Load Balancing

- Least Connections
- Fastest
- Weighted Least Connections
- Least Session
- Observed
- Predictive

Failure Mechanism

- Priority Group Activation
- Failback Host

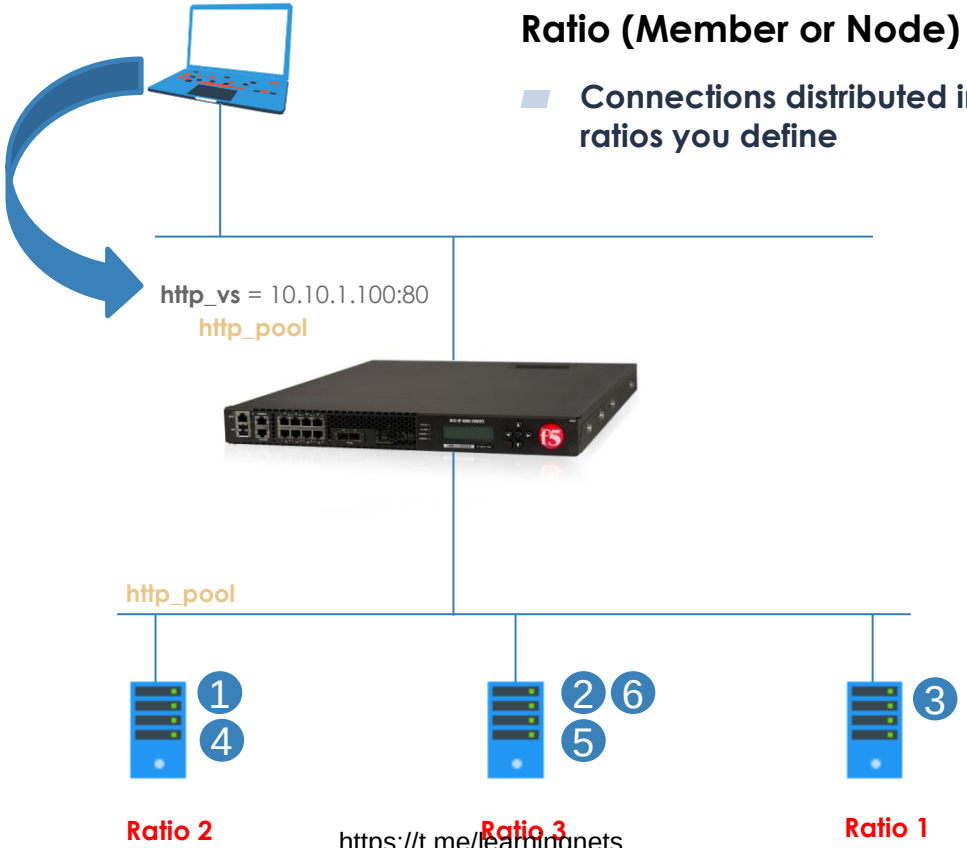
Load Balancing Concepts



Round Robin

- Connections distributed evenly across all available members

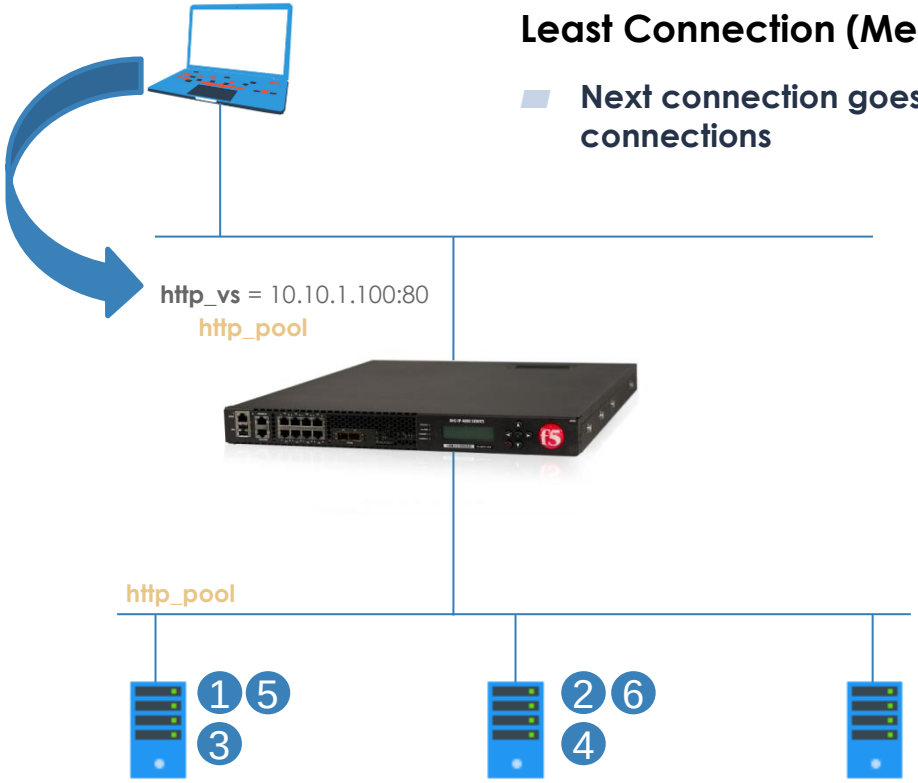
Load Balancing Concepts



Ratio (Member or Node)

- Connections distributed in weighted round robin pattern using ratios you define

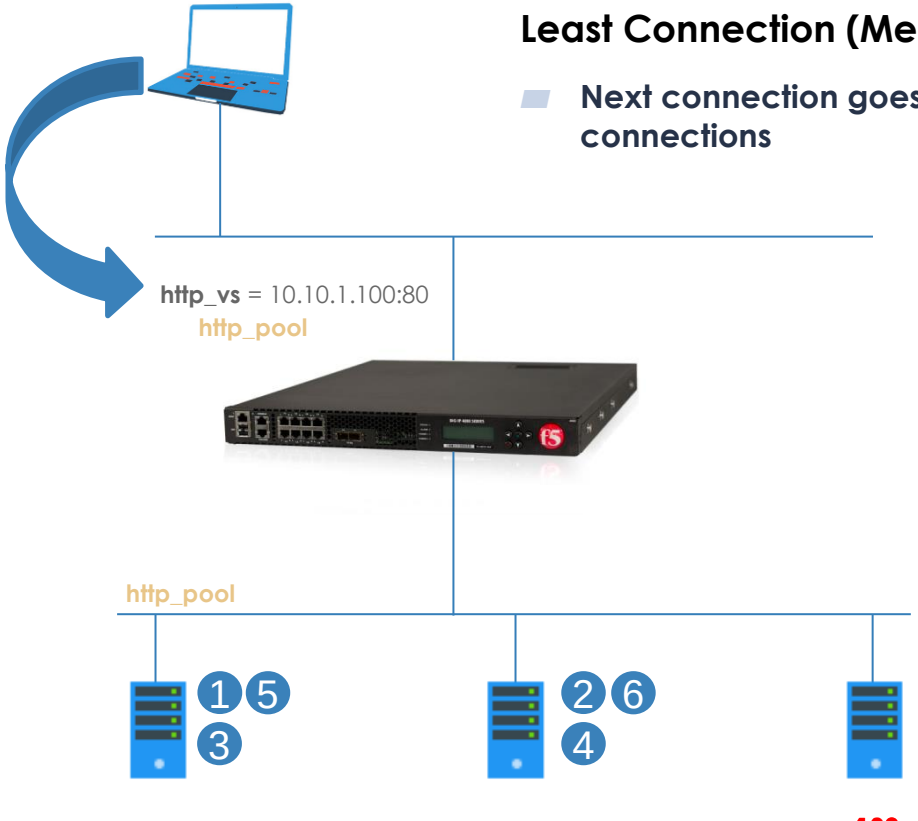
Load Balancing Concepts



Least Connection (Member or Node)

- Next connection goes to member or node with fewest open connections

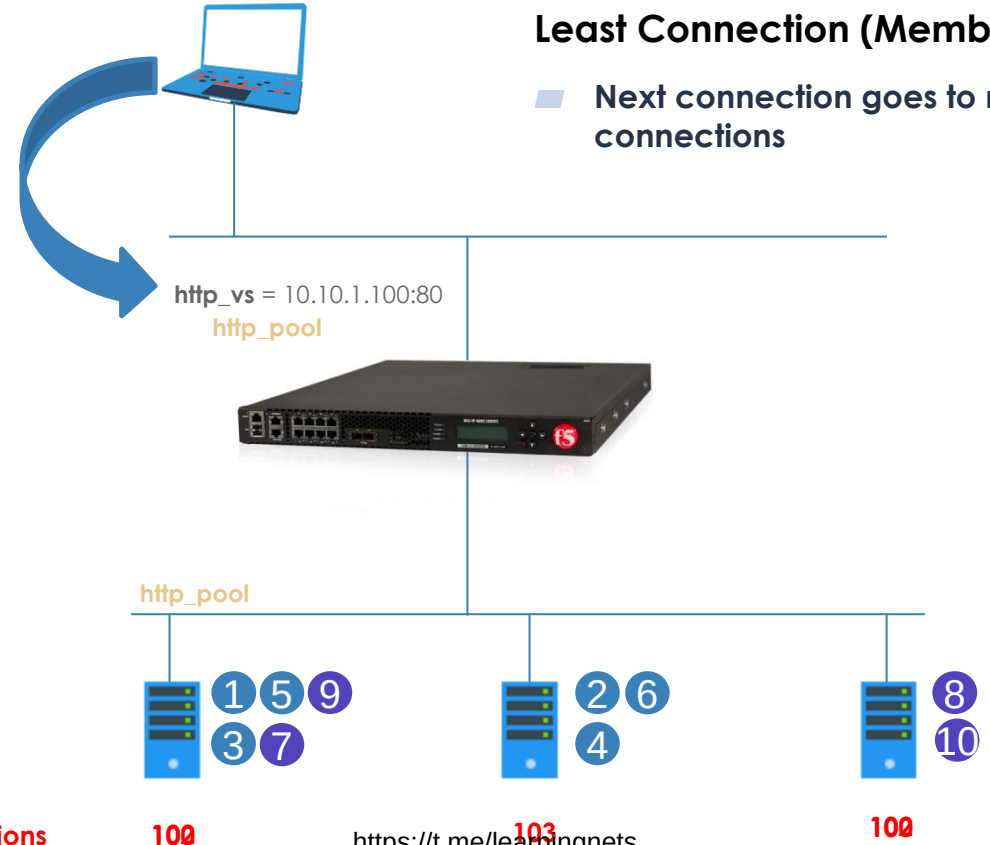
Load Balancing Concepts



Least Connection (Member or Node)

- Next connection goes to member or node with fewest open connections

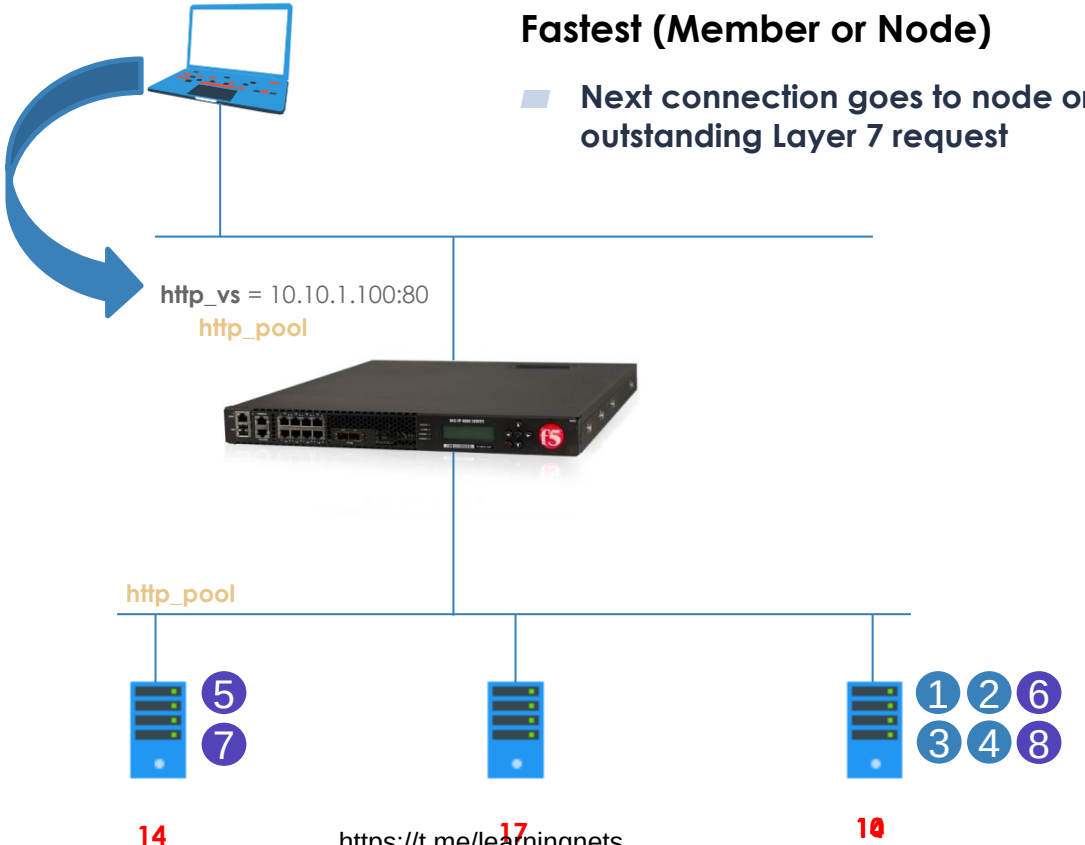
Load Balancing Concepts



Least Connection (Member or Node)

- Next connection goes to member or node with fewest open connections

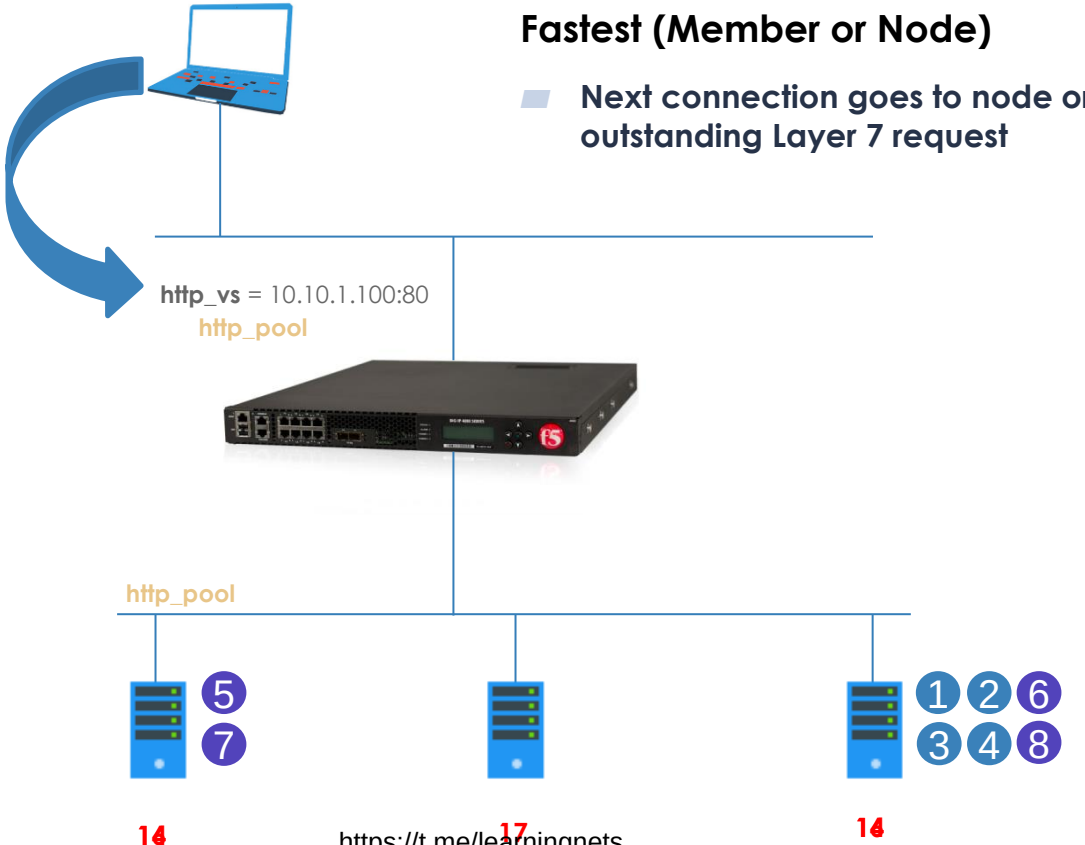
Load Balancing Concepts



Fastest (Member or Node)

- Next connection goes to node or member with fewest outstanding Layer 7 request

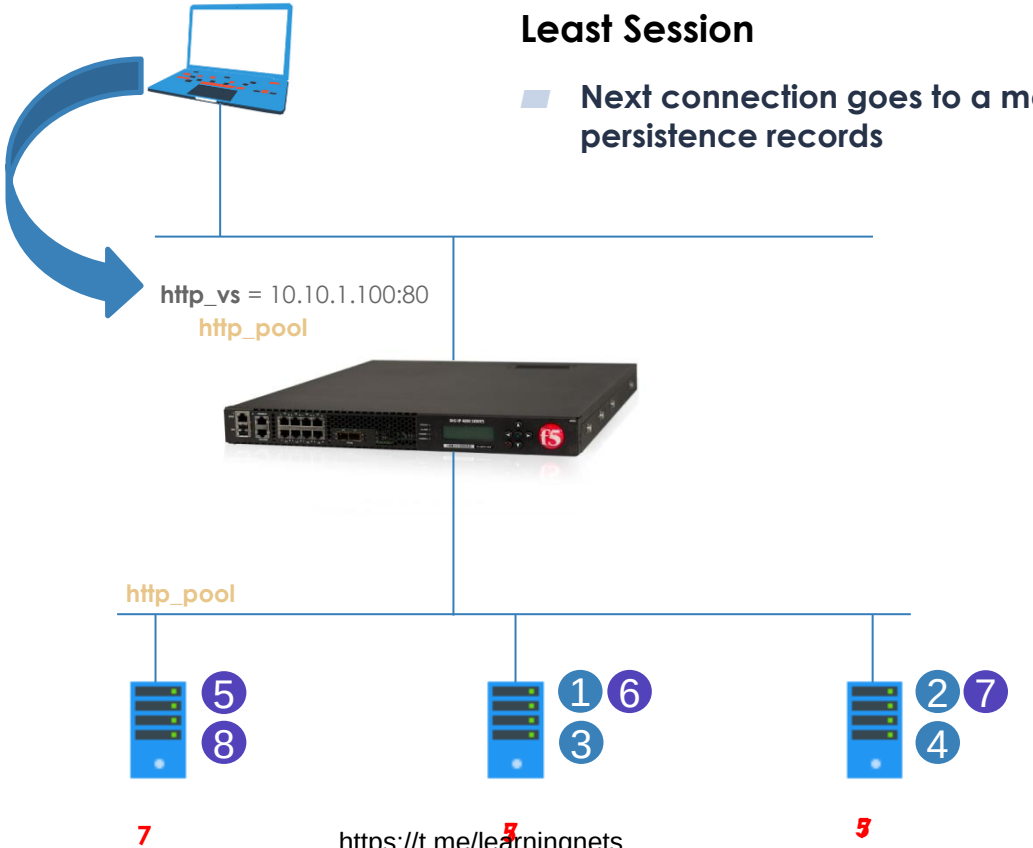
Load Balancing Concepts



Fastest (Member or Node)

- Next connection goes to node or member with fewest outstanding Layer 7 request

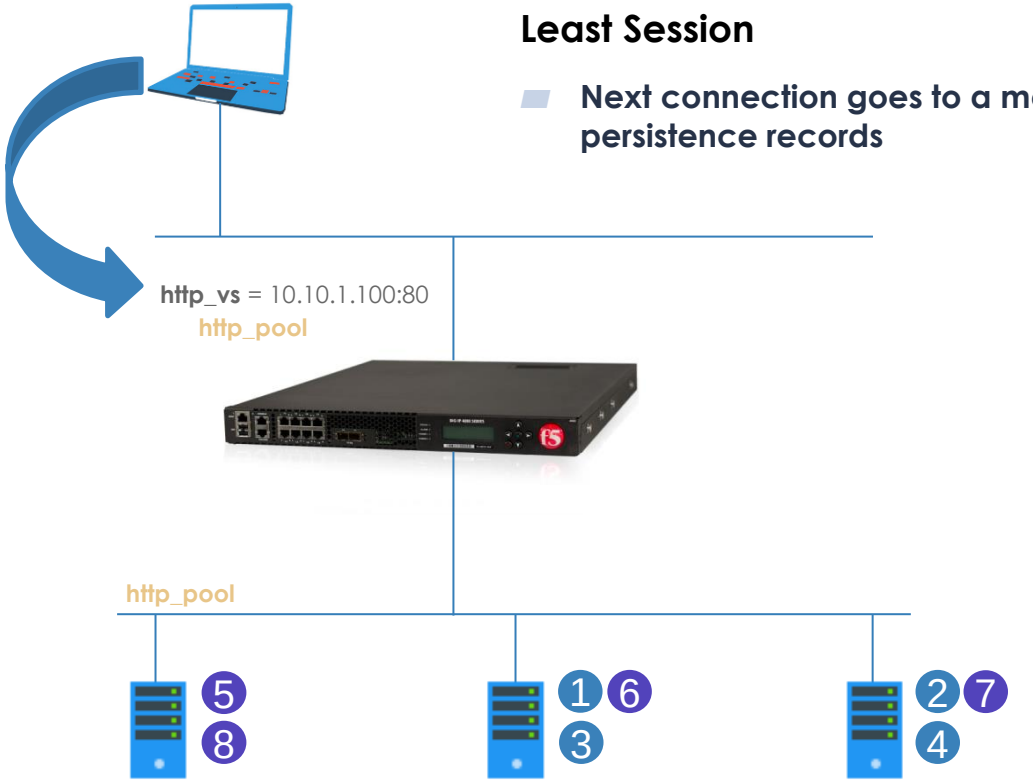
Load Balancing Concepts



Least Session

- Next connection goes to a member with fewest existing persistence records

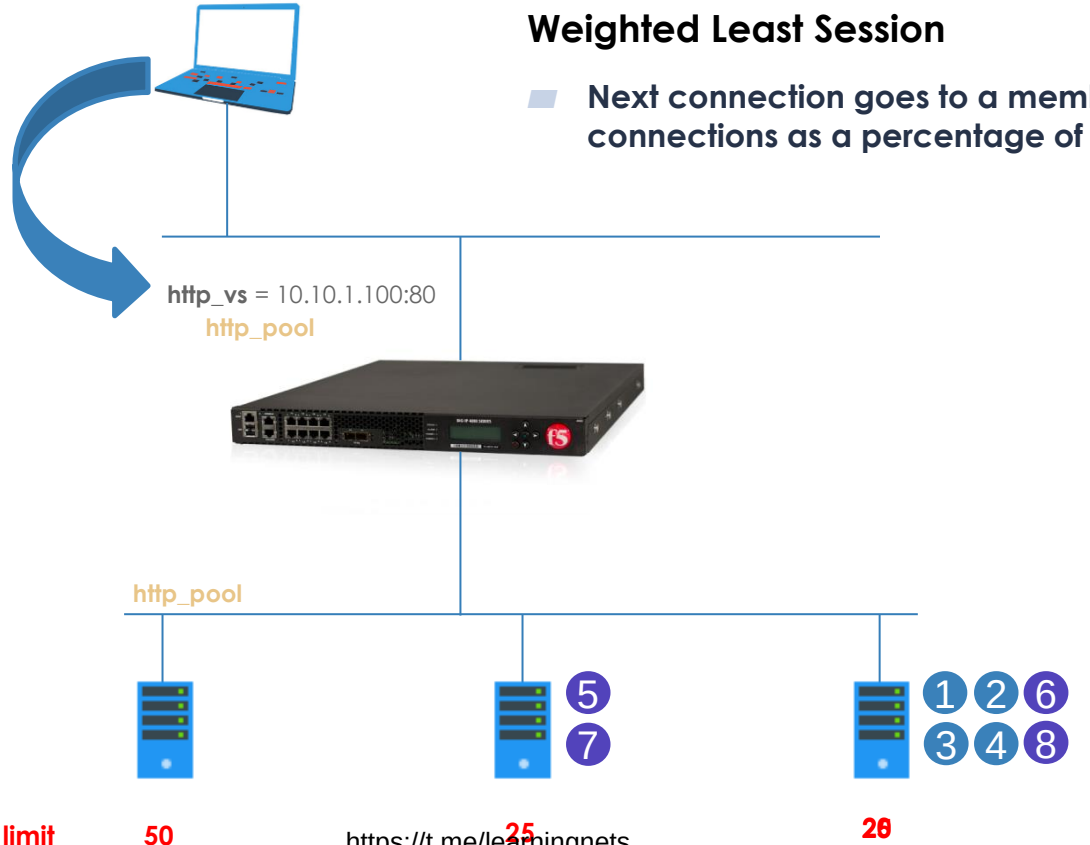
Load Balancing Concepts



Least Session

- Next connection goes to a member with fewest existing persistence records

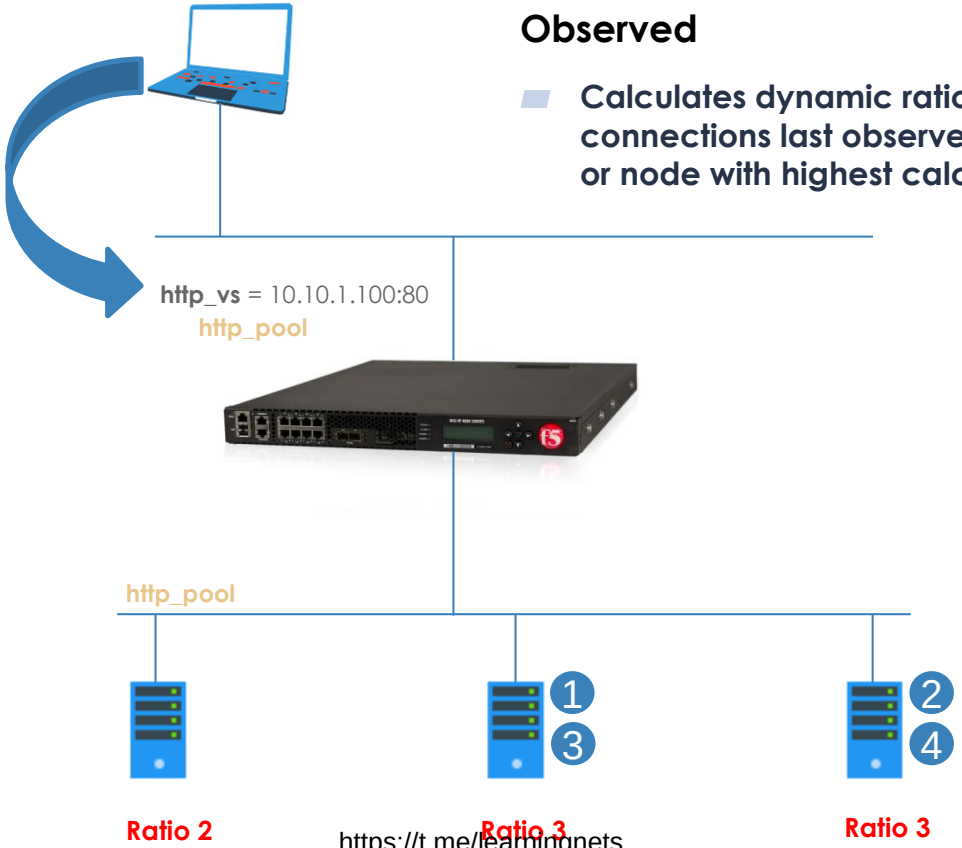
Load Balancing Concepts



Weighted Least Session

- Next connection goes to a member or node with fewest connections as a percentage of its connection limit.

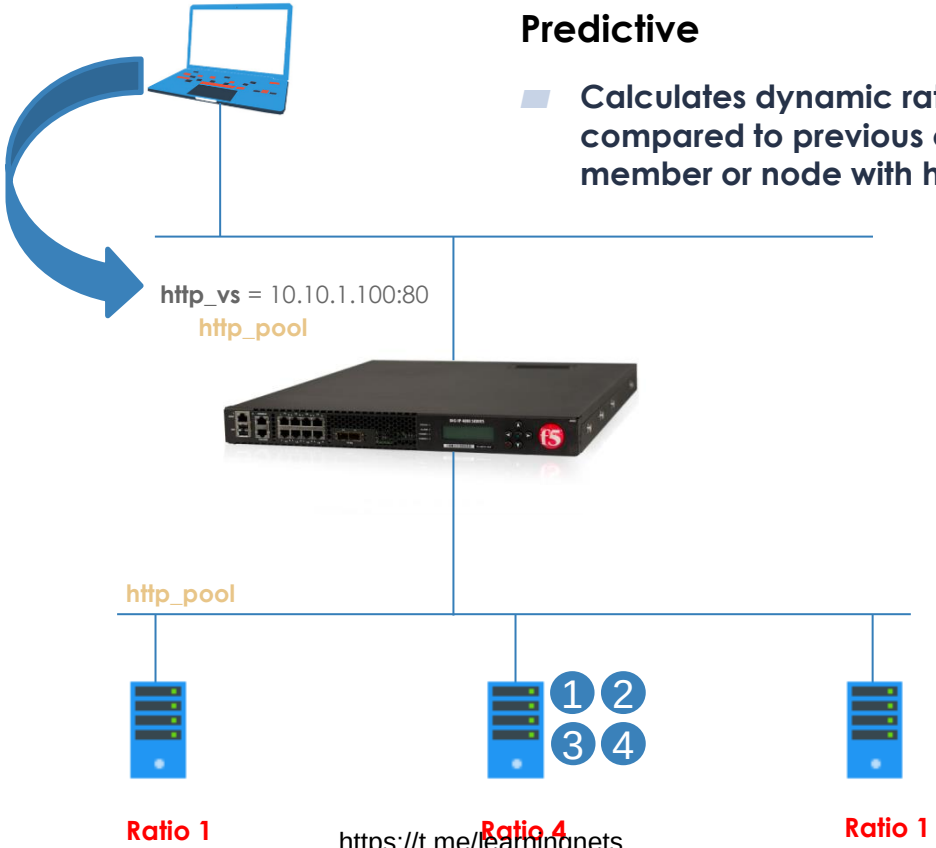
Load Balancing Concepts



Observed

- Calculates dynamic ratio value based on number of L4 connections last observed. Next connection goes to member or node with highest calculated ratio.

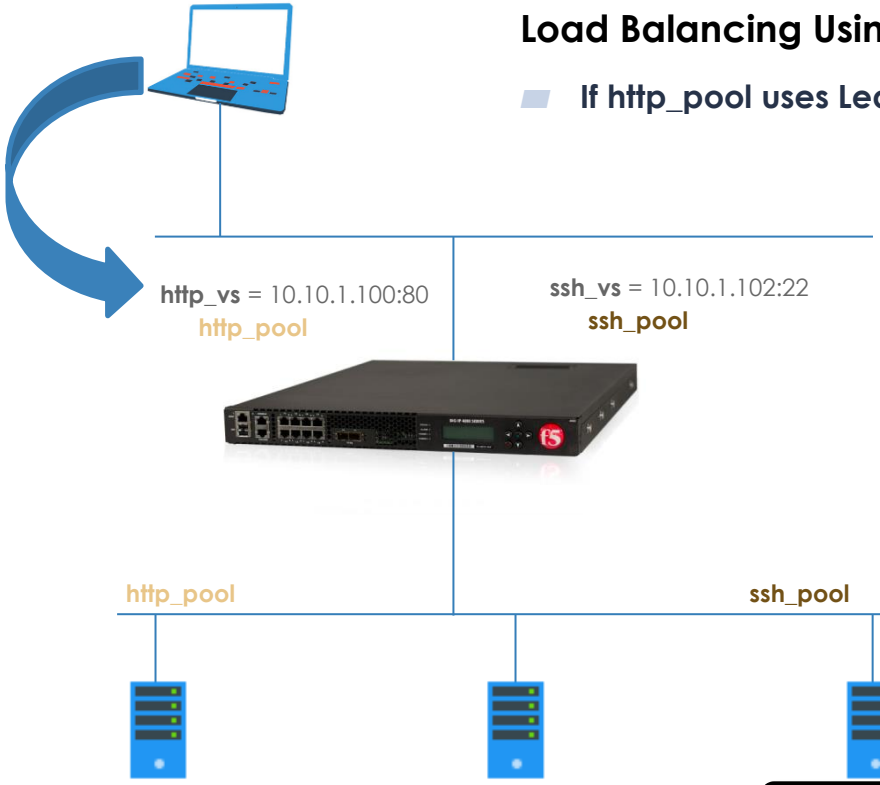
Load Balancing Concepts



Predictive

- Calculates dynamic ratio value based on current connections compared to previous connections. Next connection to member or node with highest ratio.

Load Balancing Concepts



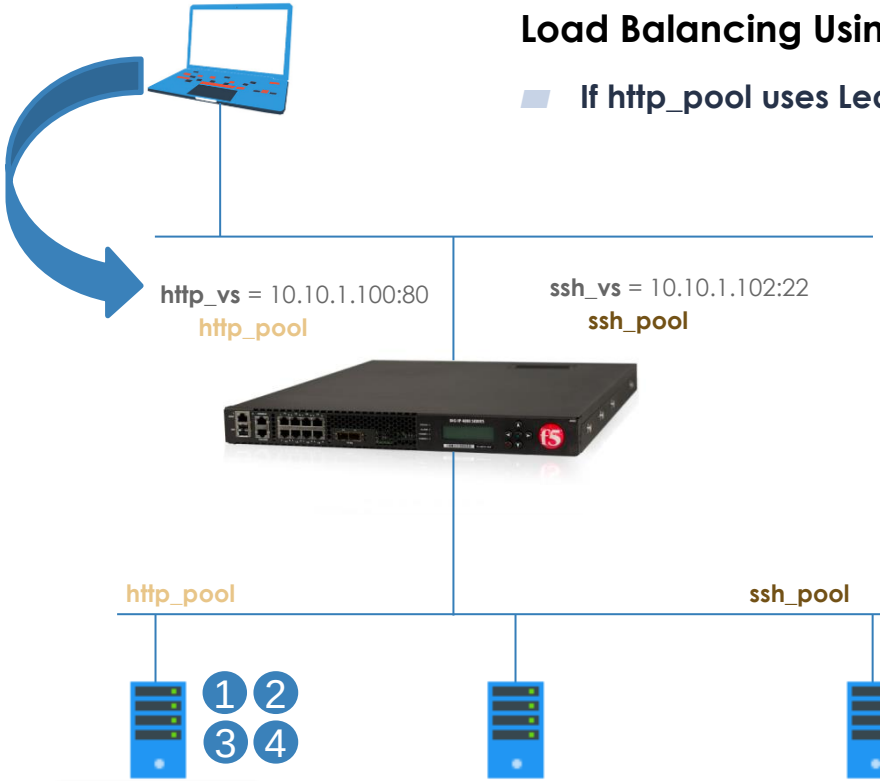
Load Balancing Using Member

- If http_pool uses Least Connections (member) then..

…next connection request to member with fewest connections

http_pool	107	108	99
ssh_pool	2	3	25

Load Balancing Concepts



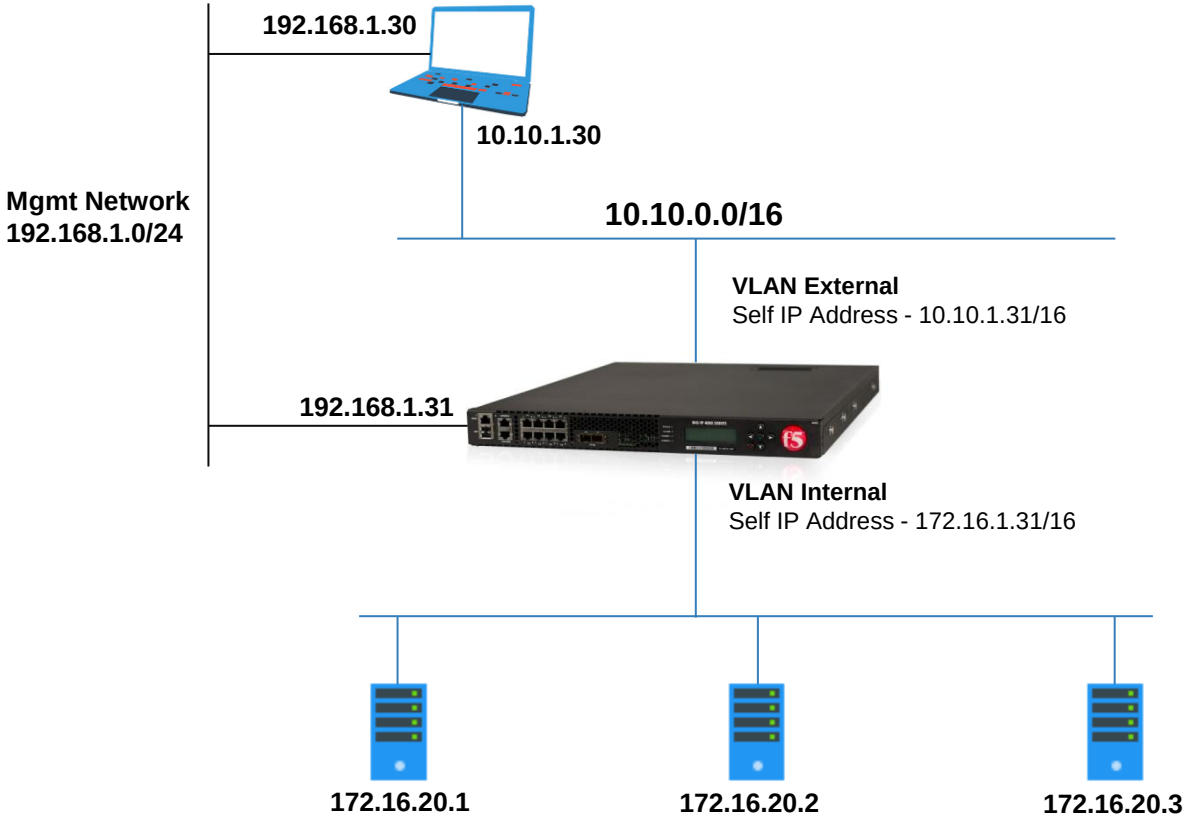
Load Balancing Using Node

- If http_pool uses Least Connections (node) then..

…next connection request to node with fewest connections

http_pool	107	108	99
ssh_pool	2	3	25

Configuring Load Balancing in ADC



Configuring Load Balancing in ADC

Static Load Balancing

- Round Robin (default)
- Ratio

Dynamic Load Balancing

- Least Connections
- Fastest
- Weighted Least Connections
- Observed
- Predictive

Failure Mechanism

- Priority Group Activation
- Failback Host

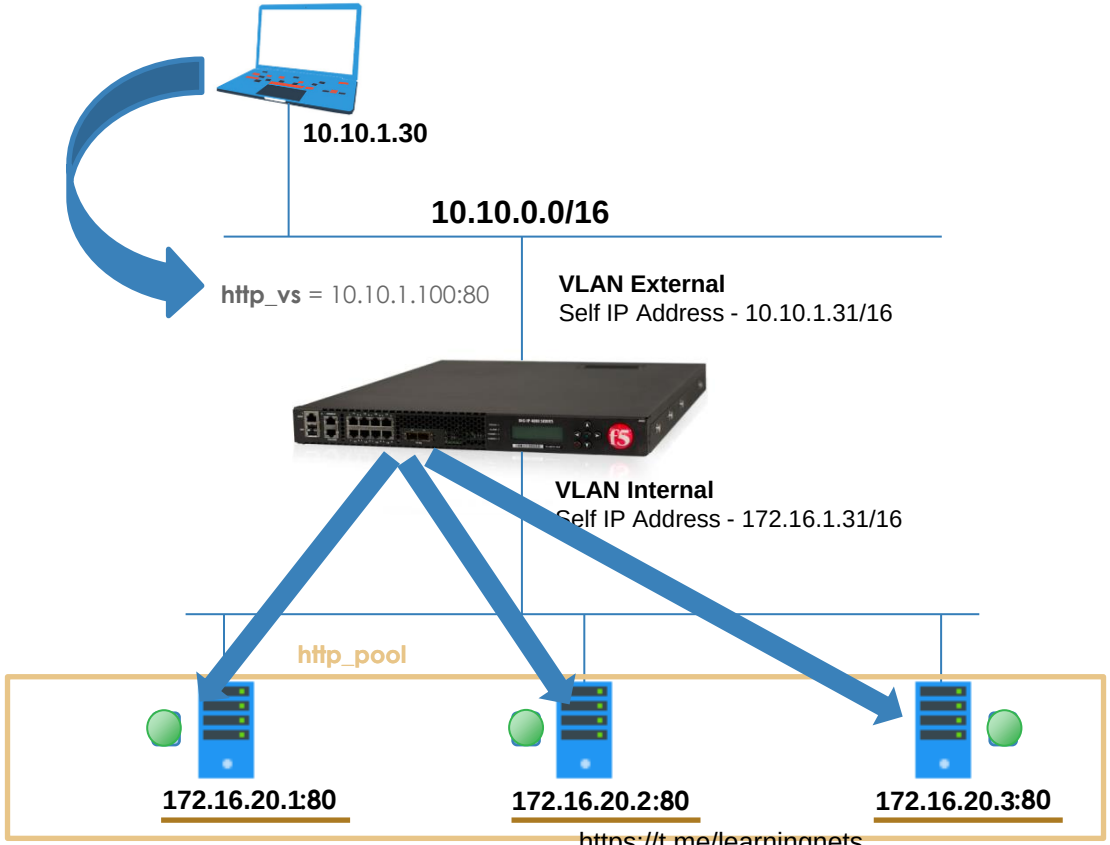
Comparing Member and Node Load Balancing

- Member = IP + Port
- Node = IP only

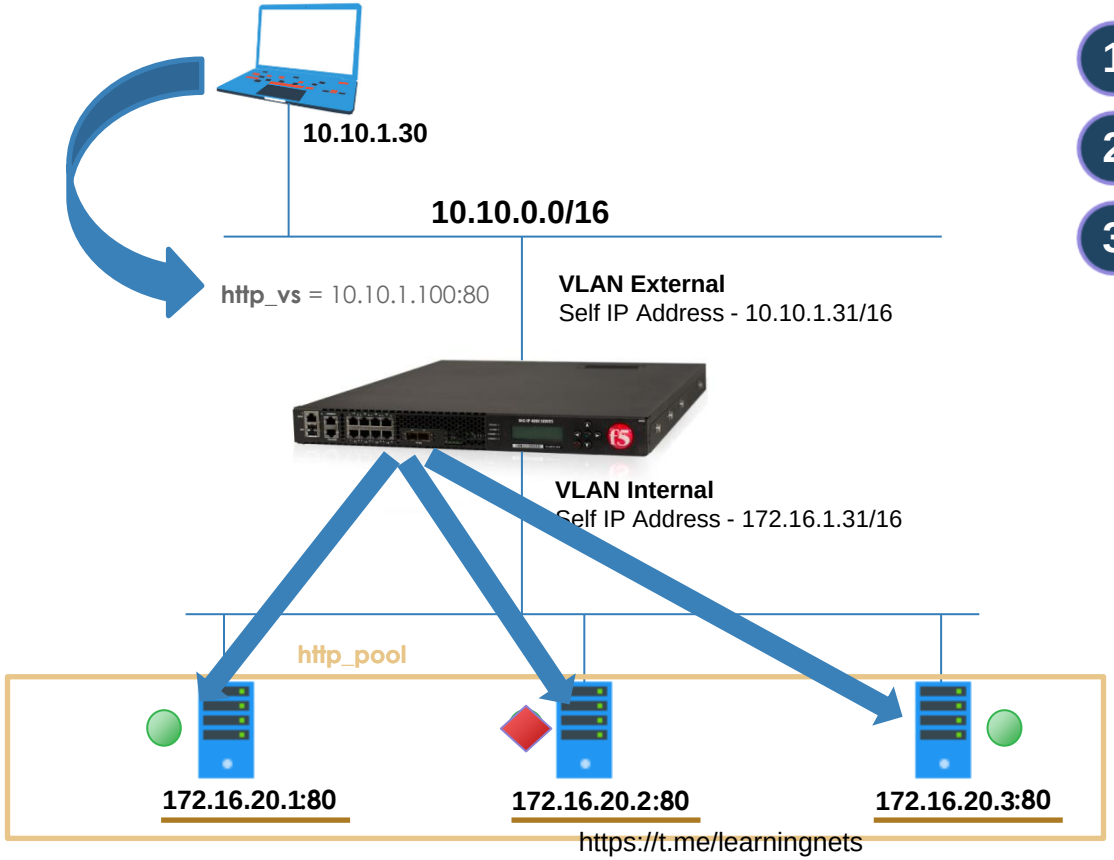
Demo

- Configuration

Health Monitors Overview

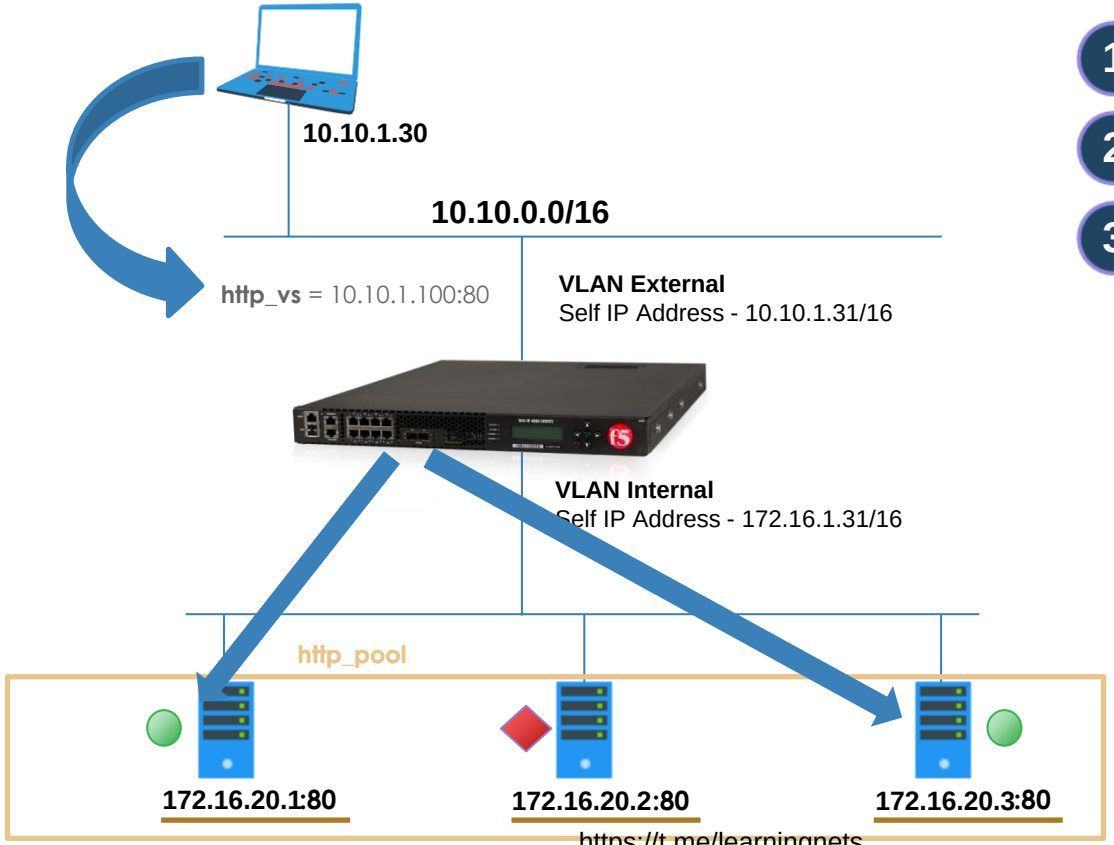


Health Monitors Overview



1. a specific resource for...
2. an expected response within...
3. a predefined time interval.

Health Monitors Overview



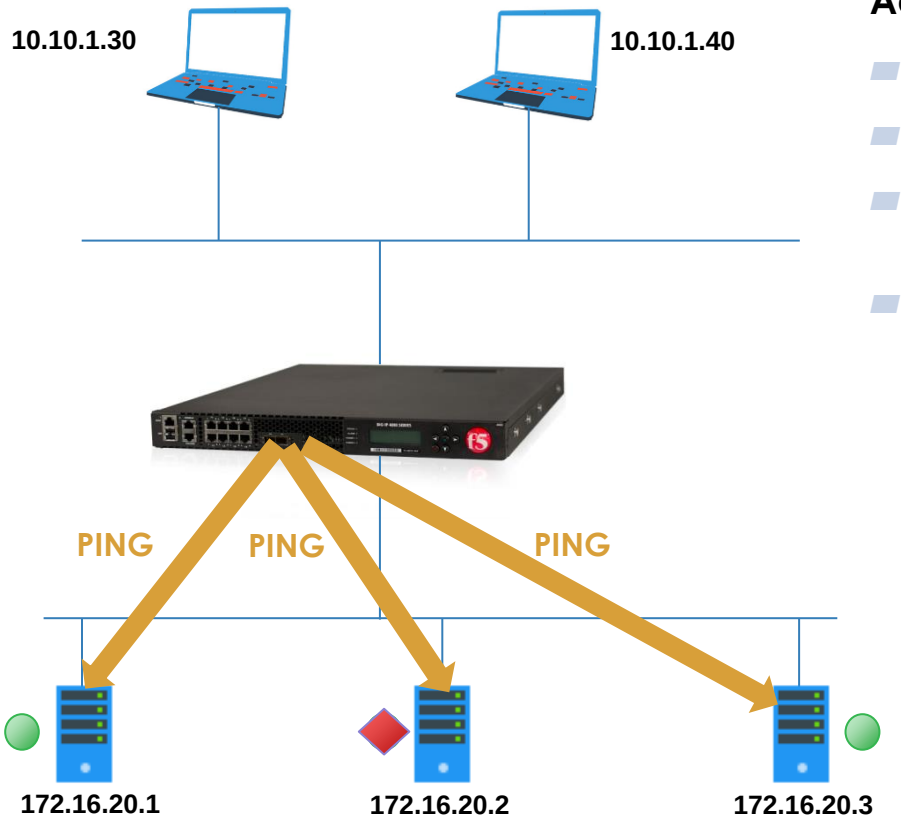
1. a specific resource for...
2. an expected response within...
3. a predefined time interval.

Health Monitors Overview

Types of Resources

- Nodes
- Pools
- Pool Members
- Links (BIG-IP DNS and Link Controller only)

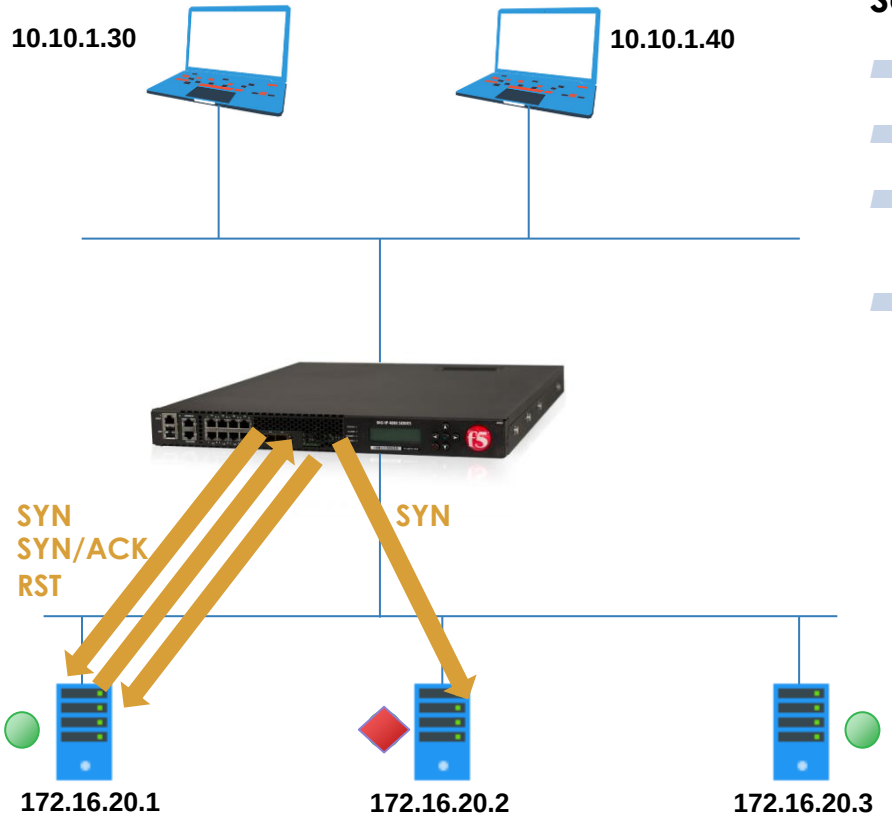
Health Monitors Overview



Address Check Monitor

- Ping an IP Address as a Health Test
- Determines Availability of a device
- Marks node/member offline if no response within timeout
- Example: ICMP

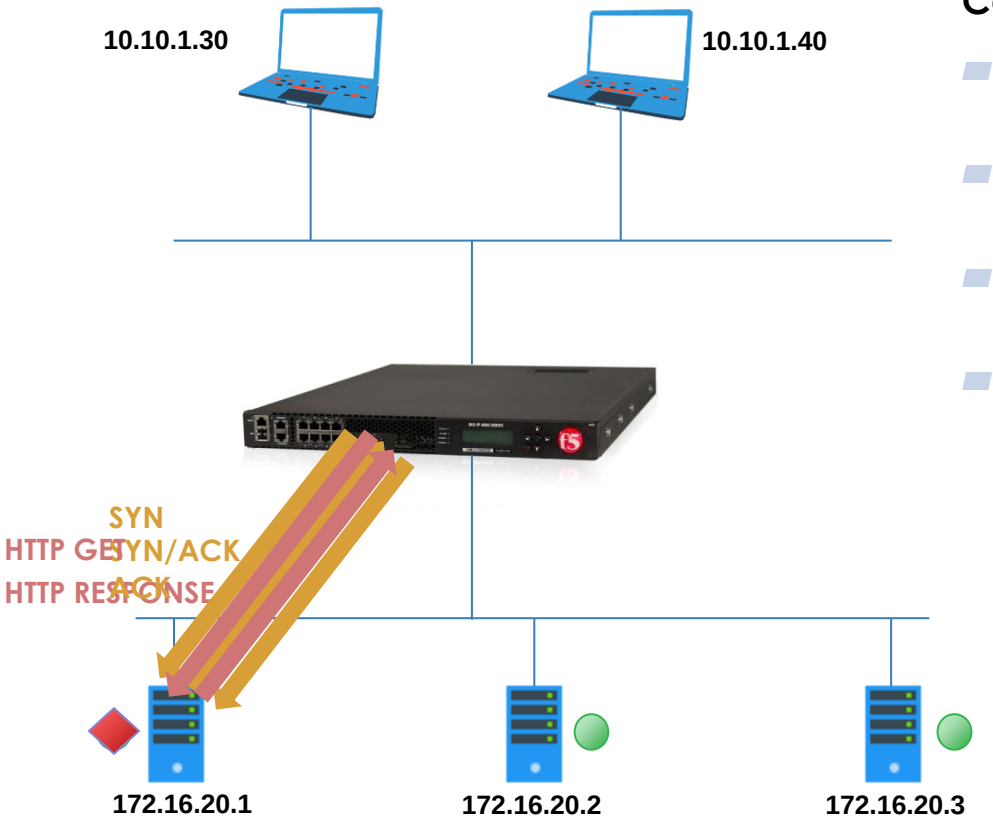
Health Monitors Overview



Service Check Monitor

- Opens a connection to pool members (service)
- Determines Availability of a service
- Marks pool member offline if no response within timeout
- Example: TCP

Health Monitors Overview



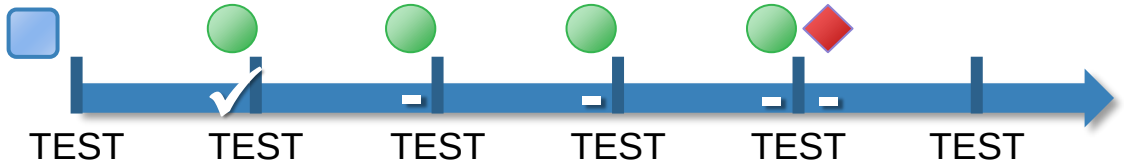
Content Check Monitor

- Opens a connection, send command, examine response
- Determines Availability of a service and appropriate content
- Marks pool member offline if no successful response withing timeout
- Example: HTTP (custom)

Health Monitors Overview

Monitor Interval and Timeout Settings

- Interval – number of seconds between each test
  - how often the monitor tests (default is 5 seconds)
- Timeout – how long before the device is marked unavailable if there is no successful test
  - default is 16 seconds
- Recommended timeout = (3 x Interval) + 1



Health Monitors Overview

Types of Monitor

- Address Check
- Service Check
- Content Check

Monitor Interval and Timeout Settings

Custom HTTP Monitor

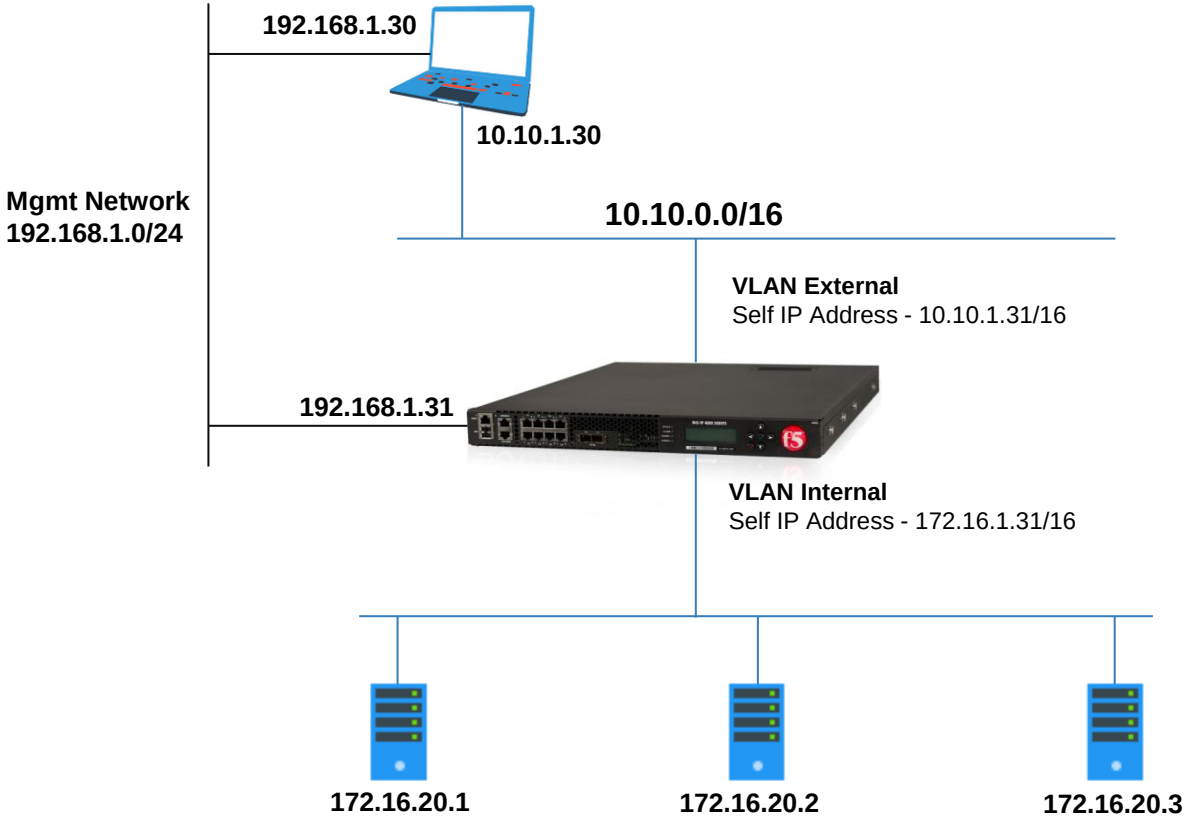
Testing Monitor

- Actual Application (HTTP)
- Monitor -> Test

Assigning Monitor

- Pool
- Pool Member Specific
- Default Node
- Node Specific

Configuring Health Monitors in ADC



Profiles

Profiles

- Used to affect the behavior of certain types of network traffic.
- Object that contains settings with values for controlling the behavior of network and applications:
- Profile Types:
  - Application Services – HTTP, DNS, FTP
  - L4 Protocols – TCP, UDP
  - Authentication – LDAP, Radius
  - Persistence – Source Address, Cookie
  - Optimization – Mobile, LAN, WAN
- All Profiles are associated to Virtual Server
- Profile Dependencies
  - Some profiles are dependent on others
  - Some profiles can’t be combined on one virtual server

Profiles

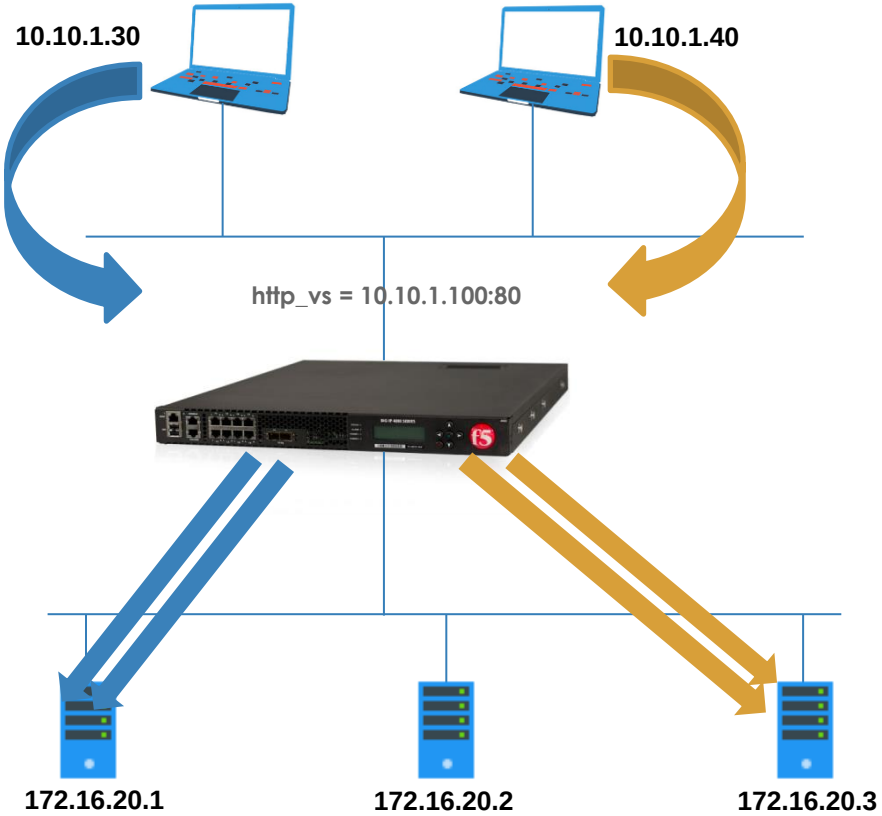
SSL Profiles

- BIG-IP accepts and terminates client requests that are sent using fully encapsulated protocol and provides a number of configurable settings for managing client-side SSL connections.
- Uses specialized hardware built for SSL Acceleration to remove processing bottlenecks and encrypt data without having to change application code.

SSL Termination Advantage

- BIG-IP performs SSL key exchange and bulk encryption
- Centralizes certificate management
- Offloads SSL traffic and Hardware acceleration from servers
- Allows iRule processing, cookie persistence, security policies and many others.

Persistence

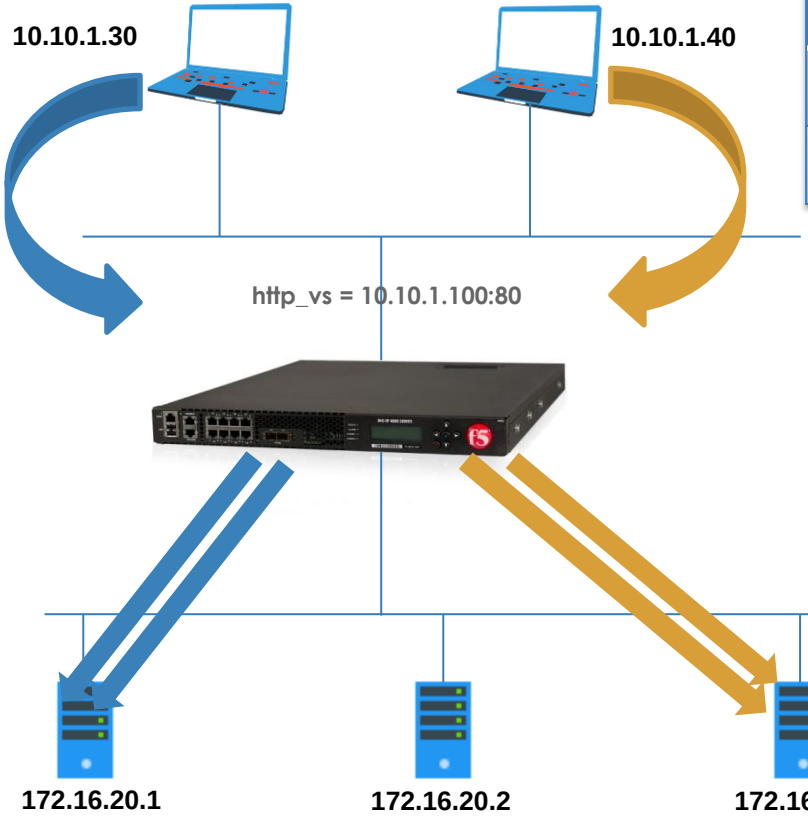


Persistence

Persistence Types on the BIG-IP System

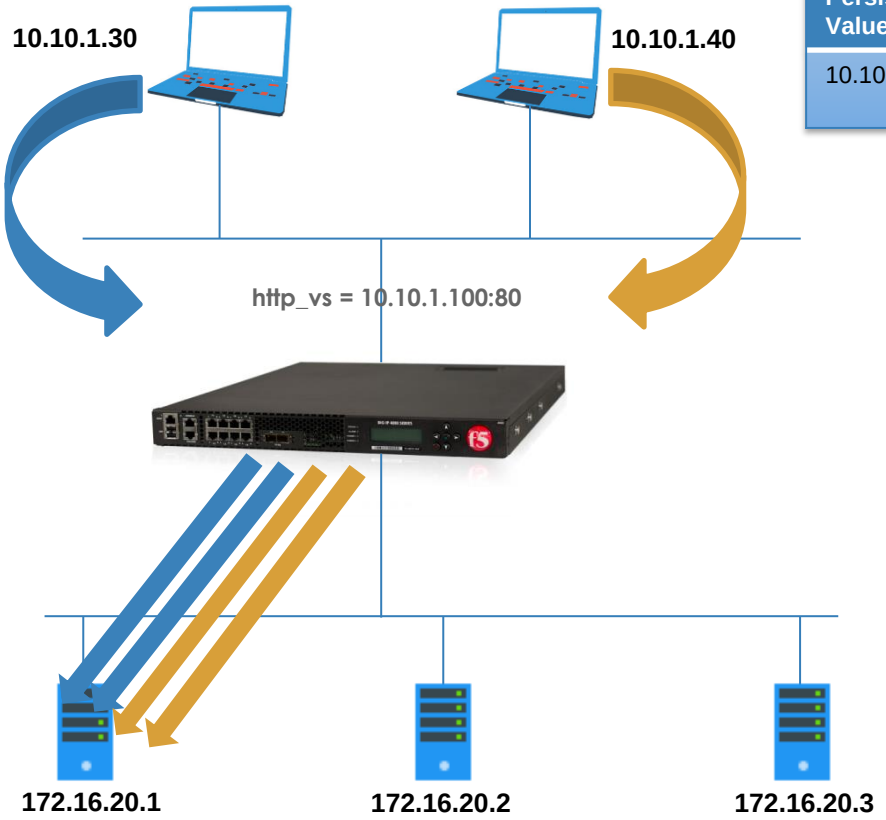
- Source Address Affinity – Based on source IP Address
- Cookie Persistence – Based on contents of browser cookie
- Destination Address Affinity – Based on destination IP address
- SSL – Based on SSL ID session ID
- Universal – Customize your own persistence criteria
- Hash – Create a persistence hash based on an existing iRule

Persistence



Persistence Value	Persistence Mode	Virtual Server	Pool	Pool Member	Age
10.10.1.30	Source Address	http_vs	http_pool	172.16.20.1:80	180 sec
10.10.1.40	Source Address	http_vs	http_pool	172.16.20.3:80	180 sec

Persistence



Persistence Value	Persistence Mode	Virtual Server	Pool	Pool Member	Age
10.10.1.0	Source Address	http_vs	http_pool	172.16.20.1:80	180 sec

Prefix Length

- 24

Persistence

Cookie Persistence

- Special cookie is inserted as the BIG-IP sends reply to the Client
- Special cookie contains selected Pool Member
- HTTP Profile is required
- Default cookie name is BIGipServer <pool_name>

Types of Cookie Persistence

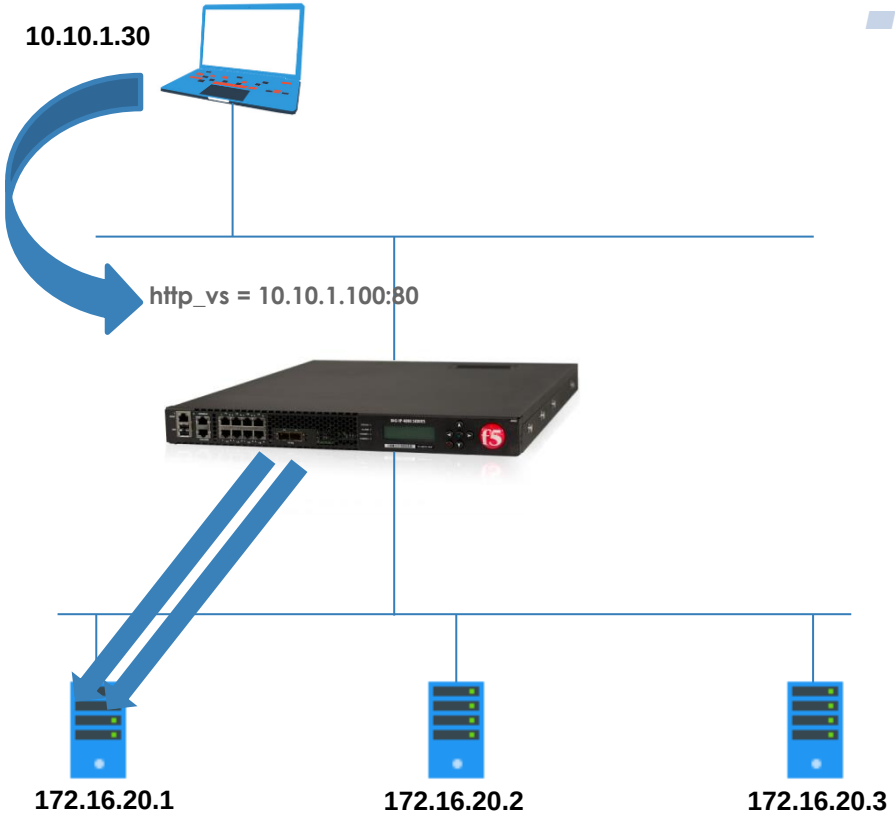
- HTTP Cookie Insert

  BIG-IP alone manages persistence cookie
- HTTP Cookie Rewrite

  BIG-IP rewrites cookie as the application sends it blank
- HTTP Cookie Passive

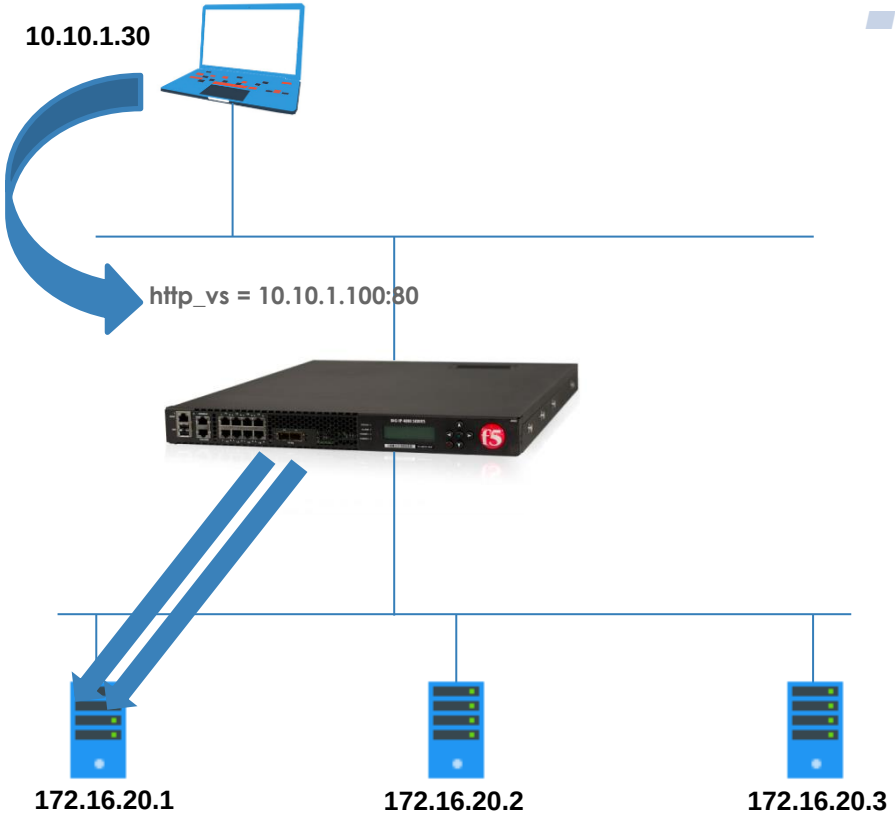
  Application alone manages persistence cookie

Persistence



- HTTP Cookie Insert
  - BIG-IP alone manages persistence cookie
  - Always Send Cookie (Disabled by default)

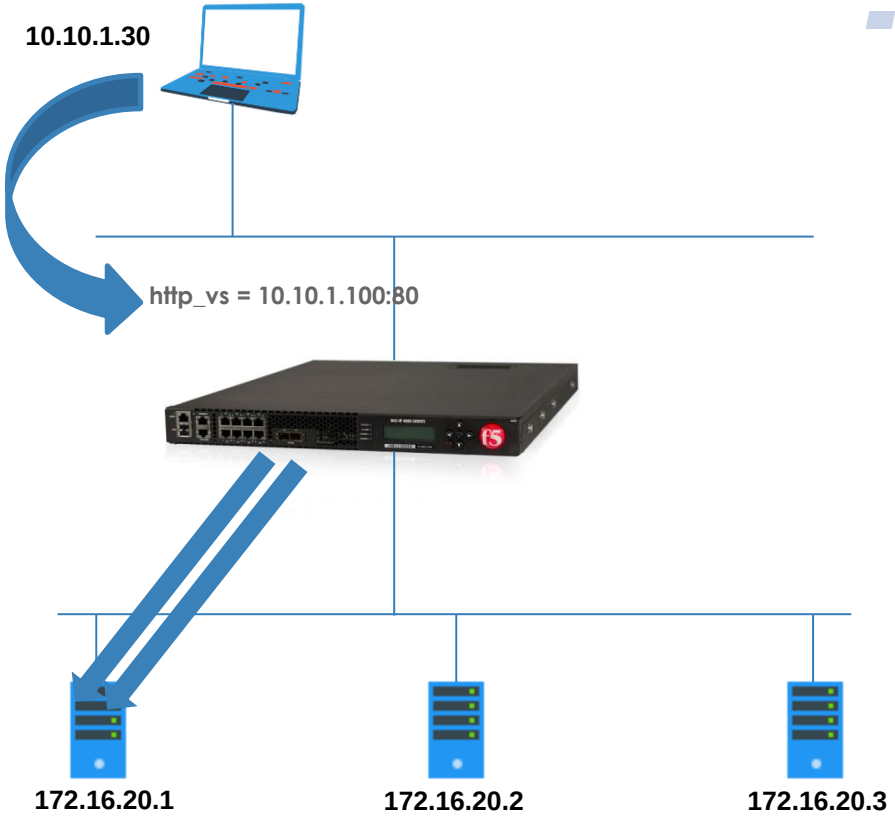
Persistence



- **HTTP Cookie Rewrite**

  BIG-IP rewrites cookie as the application sends it blank

Persistence



- **HTTP Cookie Passive**
  - **Application alone manages persistence cookie**
  - **BIG-IP lets cookie pass through**

iRule

BIG-IP iRule is when?

- If functionality is not available on CLI and GUI
- Custom Logging
- Custom Selection

BIG-IP iRule is commonly use for:

- Custom Pool and Server Selection
- HTTP to HTTPS Redirection
- Universal Persistence
- Intelligent SNAT

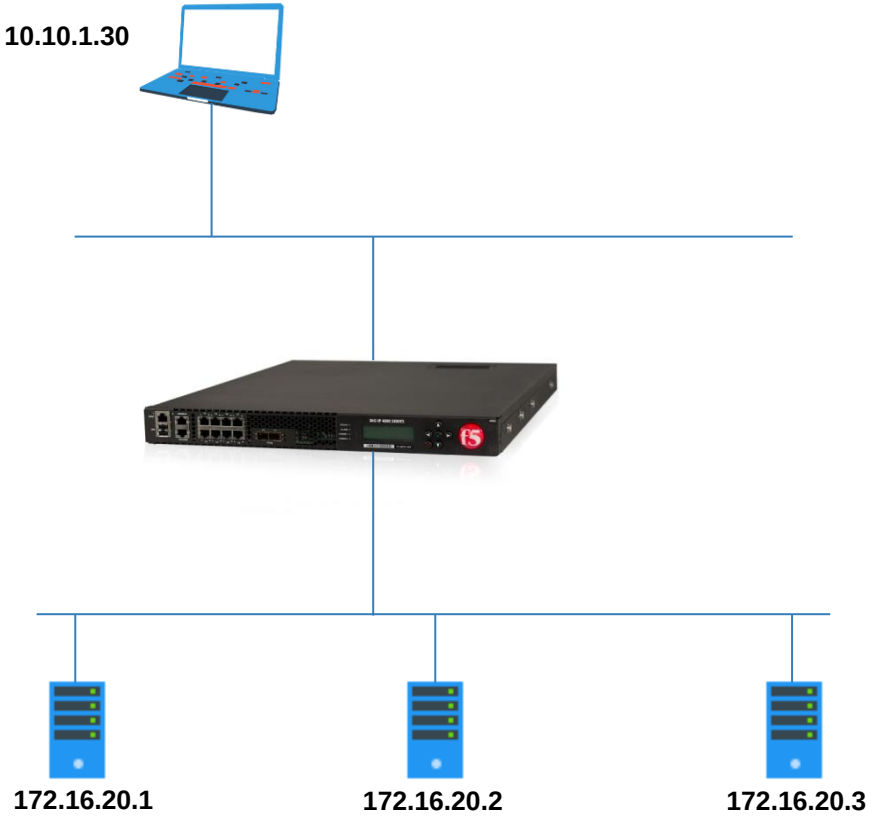
iRule

Components

- **An** event **defines the activity that triggers the iRule**
- **An** operator **is used in a conditional expression**
- **A** command **indicates the action to perform**

```
when EVENT {
    if { conditional expression } {
      action
    } elseif { condition expression } {
      action
    } else {
      action
    }
}
```

iRule



iRule Event

iRule

Operators

- equals (==)
- greater-than (>)
- less-than (<)
- starts_with
- contains
- ends_with

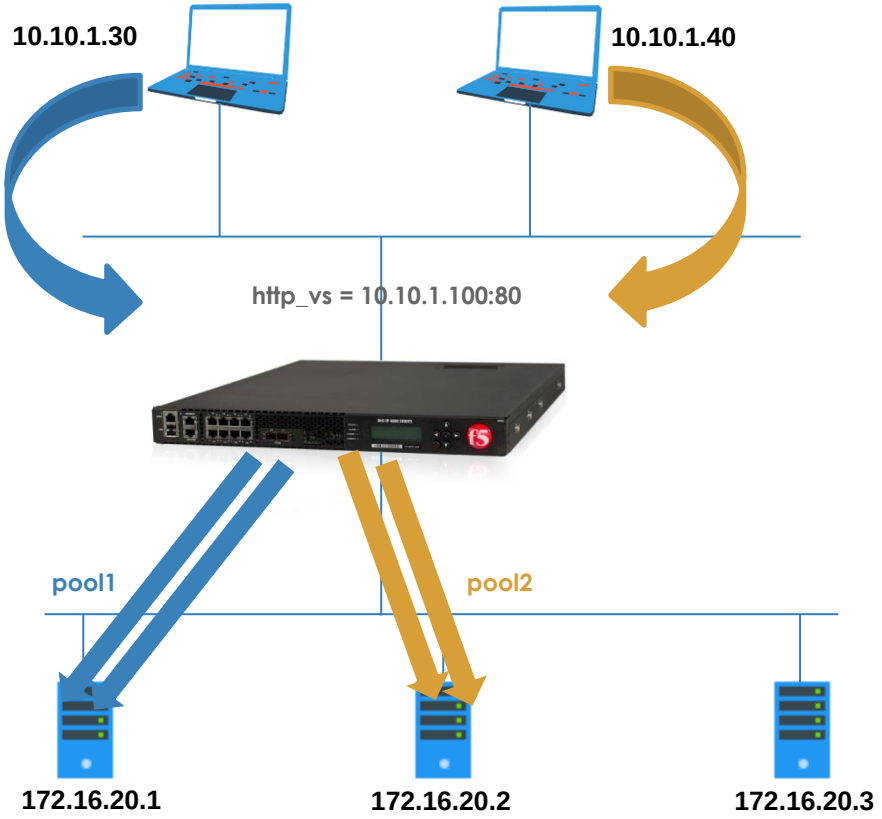
Statement

- if
- switch
- log
- pool

Commands

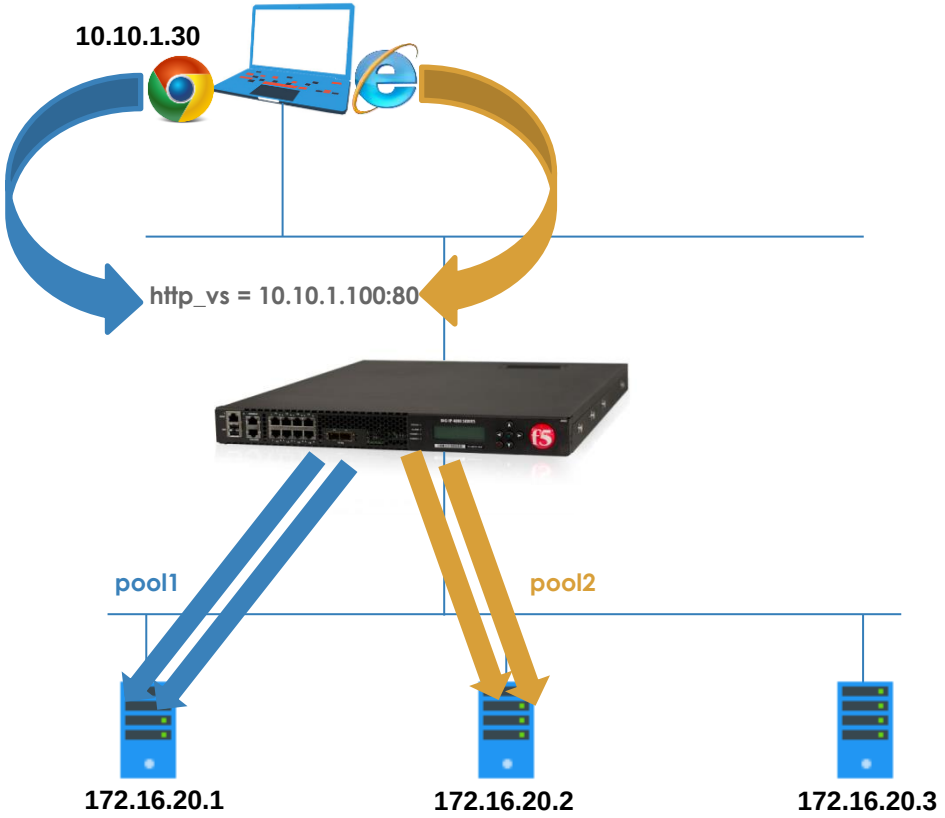
- TCP::payload
- IP::client_addr
- HTTP::header

iRule




```
when CLIENT_ACCEPTED {
    if { [IP::client_addr] equals "10.10.1.30" } {
      pool pool1
    } elseif { [IP::client_addr] equals "10.10.1.40" } {
      pool pool2
    }
}
```

iRule




```
when HTTP_REQUEST {
  if { [HTTP::header User-Agent] contains "Chrome" } {
    pool pool1
  } elseif { [HTTP::header User-Agent] contains "MSIE" } {
    pool pool2
  } else {
    pool pool3
  }
}
```

Chrome User Agent

- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36

Internet Explorer User Agent

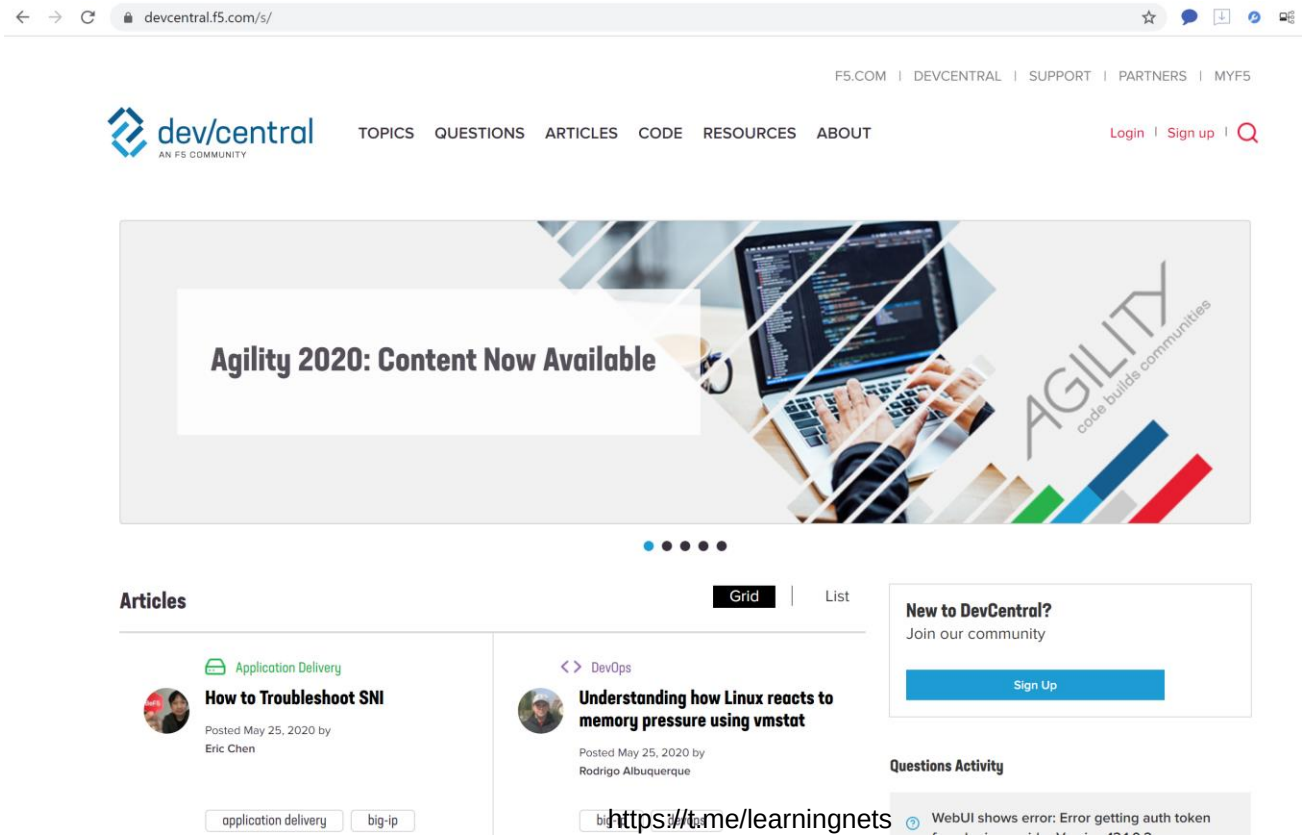
- Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko

Firefox User Agent

- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0

iRule

DevCentral



High Availability (HA)

F5 HA

- characteristic of a system which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.
- Refers to core system services being up and running on one (or both) of the two BIG-IP Systems

Active-Standby Pair

- Pair of devices – one is active processing traffic and the other ready to take over if failover occurs
- Two devices synchronize their configuration

Active-Active Pair

- Both Pair of devices are actively processing traffic and ready to take over one another if failover occurs.
- Two devices synchronize their configuration

High Availability (HA)

Device Service Clustering (DSC)

- is an underlying architecture within BIG-IP Traffic Management Operation System (TMOS)
- DSC provides synchronization and failover of BIG-IP configuration data
- Configure a BIG-IP device on a network to:
  - Synchronize some or all of its configuration data among several BIG-IP devices
  - Fail over to one of many available devices
  - Mirror connections to a peer device to prevent interruption in service during failover

High Availability (HA)

Deploying a New High Availability Configuration

- Prepare to Deploy DSC Configuration on BIG-IP devices

  Unique device names, configure VLANs, Self Ips, Synchronized clocks, UCS archives and passwords

- Configure DSC Communications

  Add internal self IP address for ConfigSync, Mirror Connection and Failover heartbeat

- Establish Device Trust

  Add peer using management IP address, admin username and password

- Establish a Sync-Failover Device Group

  Add which devices will participate in the Sync-Failover Cluster

- Synchronize Configuration Data

  Push Configuration from Primary device to Secondary device

High Availability (HA)

Failover Communications Method

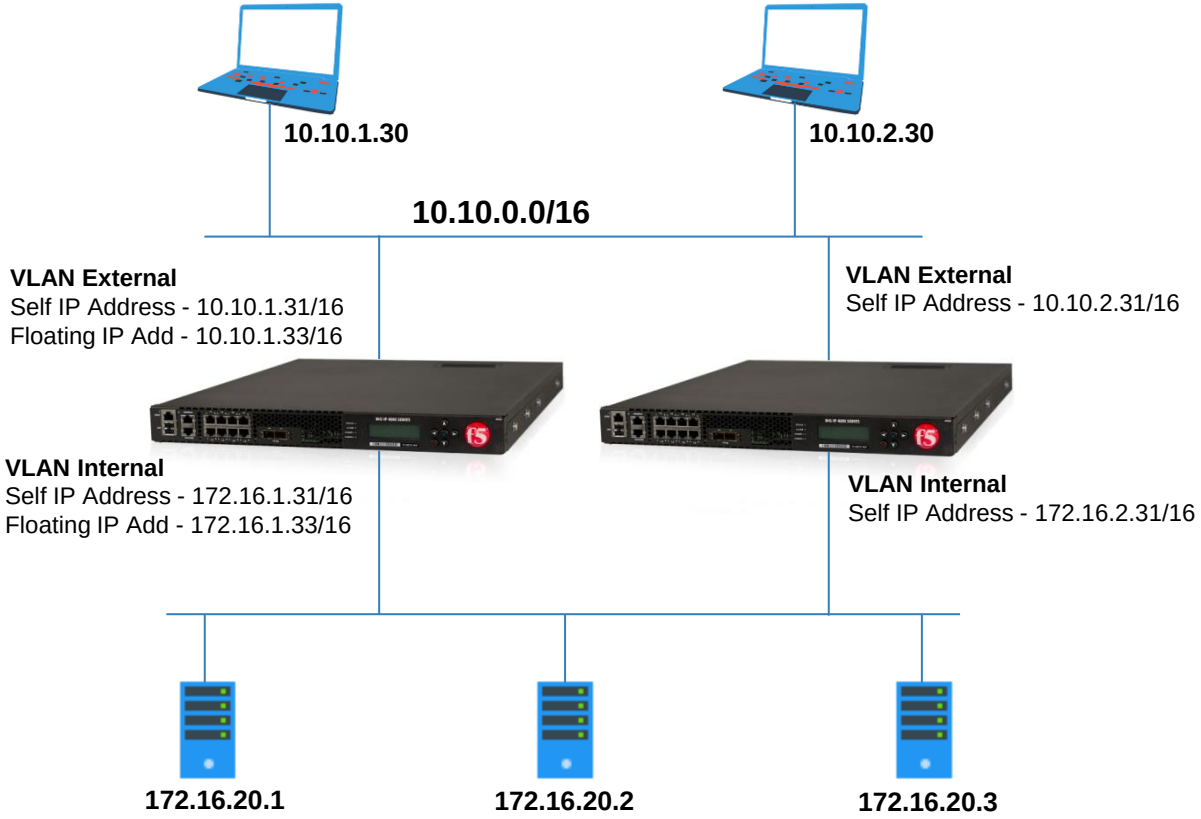
Hardware Failover

- BIG-IP appliance active/standby pair only
- Continuous voltage over special cable
- Must be in physical proximity of one another
- Use only in combination with network failover

Network Failover

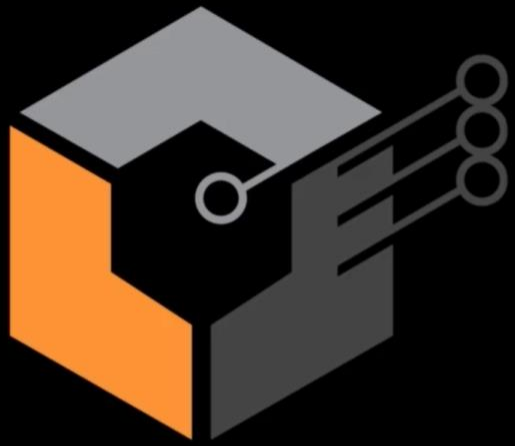
- Required for active/active or N+1 F5 devices
- Heartbeat packets transmitted over network
- Packets containers traffic and device status info

High Availability (HA)



F5 101 Exam Preparation

Application Delivery Controller Overview



ZURIEN

www.zurien.com