Cricket Liu's DNS APPLIANCE BEST PRACTICES ARCHITECTURE

Infoblox CONTROL YOUR NETWORK
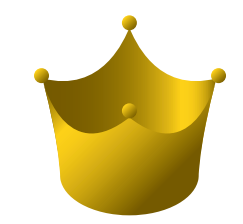
Grid Master, Hidden Internal Primary
Hosts the GUI, allowing single-point administration of appliances, configuration of DNS, DHCP, and other protocols. Coordinates communication of all appliances in Grid™ over a secure TLS VPN. Facilitates single-point, one-button upgrade of all Grid members. HA pair to ensure availability. Hidden primary manages the company's internal zone data. Located inside firewall for protection, ease of management. Hidden to prevent querying by other name servers.
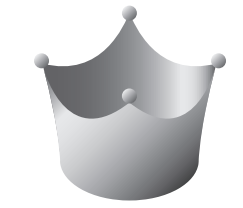
Grid Master Candidates, Secondaries
Backups for Grid Master. Either can be promoted to assume responsibilities of Grid Master in event of disaster or maintenance with no loss of data or state. Also function as secondary name servers, providing name service to local resolvers and internal name servers. HA pair to ensure availability, avoid costly resolver timeouts.
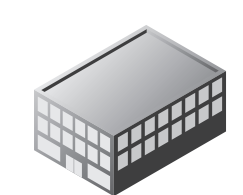
Headquarters
Hosts critical business applications and North American connection to the Internet. Most IT staff concentrated here. Very low tolerance for downtime or delay.
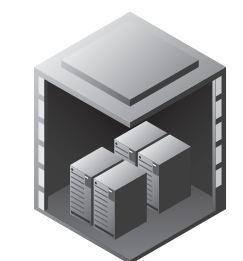
Major Sites
Host critical business applications as well as European and Asian connections to the Internet. Some local IT staff. Very low tolerance for downtime or delay. Desire to capitalize on local internet connection for resolution of "local" domain names and to answer queries from local recursive name servers.

Regional Offices
Host administrative and production users of desktop applications and headquarters-based business applications. Limited local IT staff. Some tolerance for delay, low tolerance for downtime. Nearby branch offices connect to corporate network here.

Branch Offices
Host small number of users of headquarters-based business applications. No local IT staff. Higher tolerance for delay, low tolerance for downtime.
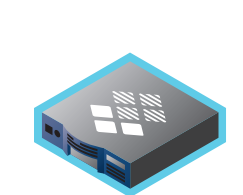
Infoblox Appliance Providing DNS
Infoblox appliances with the NS1® package provide the foundation for a secure, reliable DNS infrastructure with minimal administration and configuration.
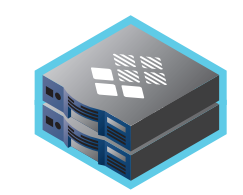
High-Availability (HA) Pair Providing DNS
Two appliances that share a single virtual IP address to deliver service redundancy. Configuration and state are transactionally synchronized between the pair.
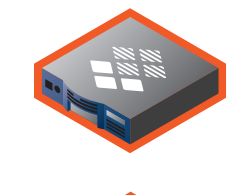
Infoblox Appliance Providing DNS/DHCP
Infoblox appliances with the NS1 package support DHCP as well as DNS.

High-Availability (HA) Pair Providing DNS/DHCP
DHCP can run on HA pairs for redundancy, or can use the DHCP failover protocol. DNS can run on HA pairs for redundancy or can use anycast.

Branch Office DNS Servers
Provide local recursive name service to resolvers hosted on smaller appliances, VMware®, Cisco® ISR routers or Riverbed® Steelhead® appliances. Microsoft® DNS servers are managed using NIOS's Microsoft management feature.
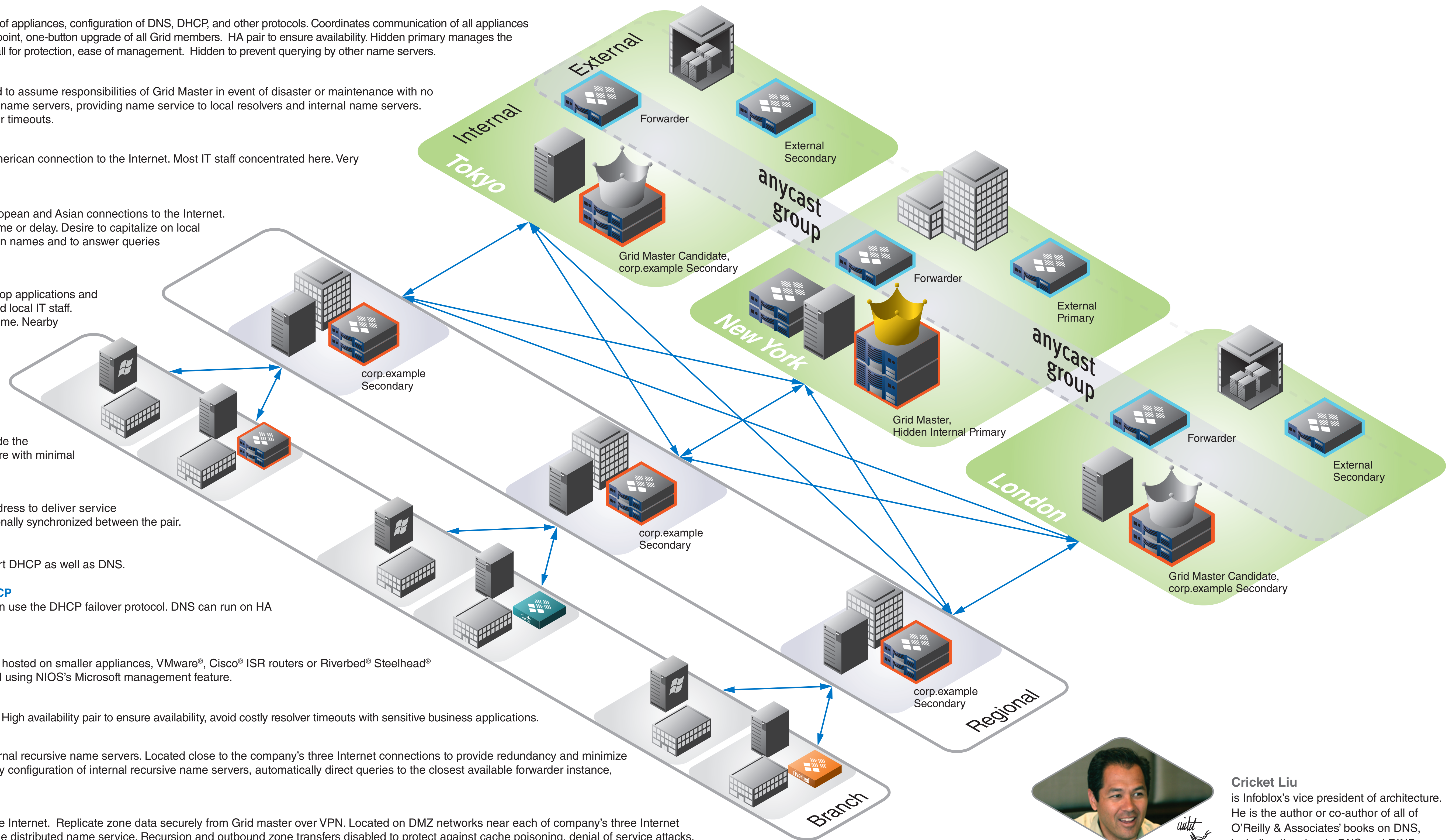
Internal Secondaries
Provide local recursive name service to resolvers. High availability pair to ensure availability, avoid costly resolver timeouts with sensitive business applications.

Forwarders
Resolve Internet domain names on behalf of internal recursive name servers. Located close to the company's three Internet connections to provide redundancy and minimize latency. Configured in an anycast group to simplify configuration of internal recursive name servers, automatically direct queries to the closest available forwarder instance, and avoid querying unavailable forwarders.

External Primary and Secondaries
Advertise the company's external zone data to the Internet. Replicate zone data securely from Grid master over VPN. Located on DMZ networks near each of company's three Internet connections to avoid single point of failure, provide distributed name service. Recursion and outbound zone transfers disabled to protect against cache poisoning, denial of service attacks.

Diagram labels

External

Internal

Tokyo

Forwarder

External Secondary

anycast group

Grid Master Candidate, corp.example Secondary

corp.example Secondary

New York

Forwarder

External Primary

anycast group

Grid Master, Hidden Internal Primary

London

Forwarder

External Secondary

Grid Master Candidate, corp.example Secondary

corp.example Secondary

Regional

Branch

Cricket Liu
is Infoblox's vice president of architecture. He is the author or co-author of all of O'Reilly & Associates' books on DNS, including the classic *DNS and BIND*.