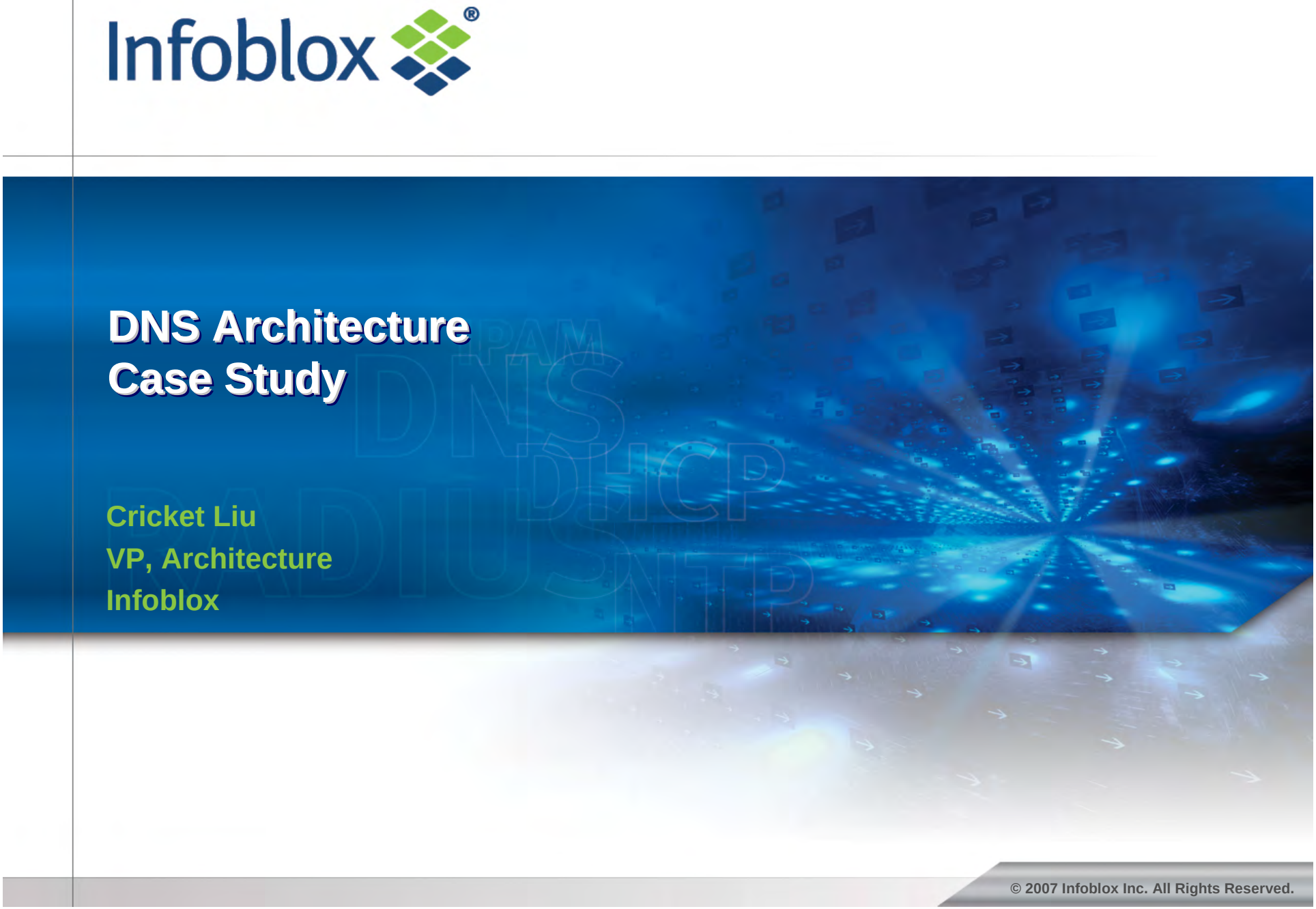
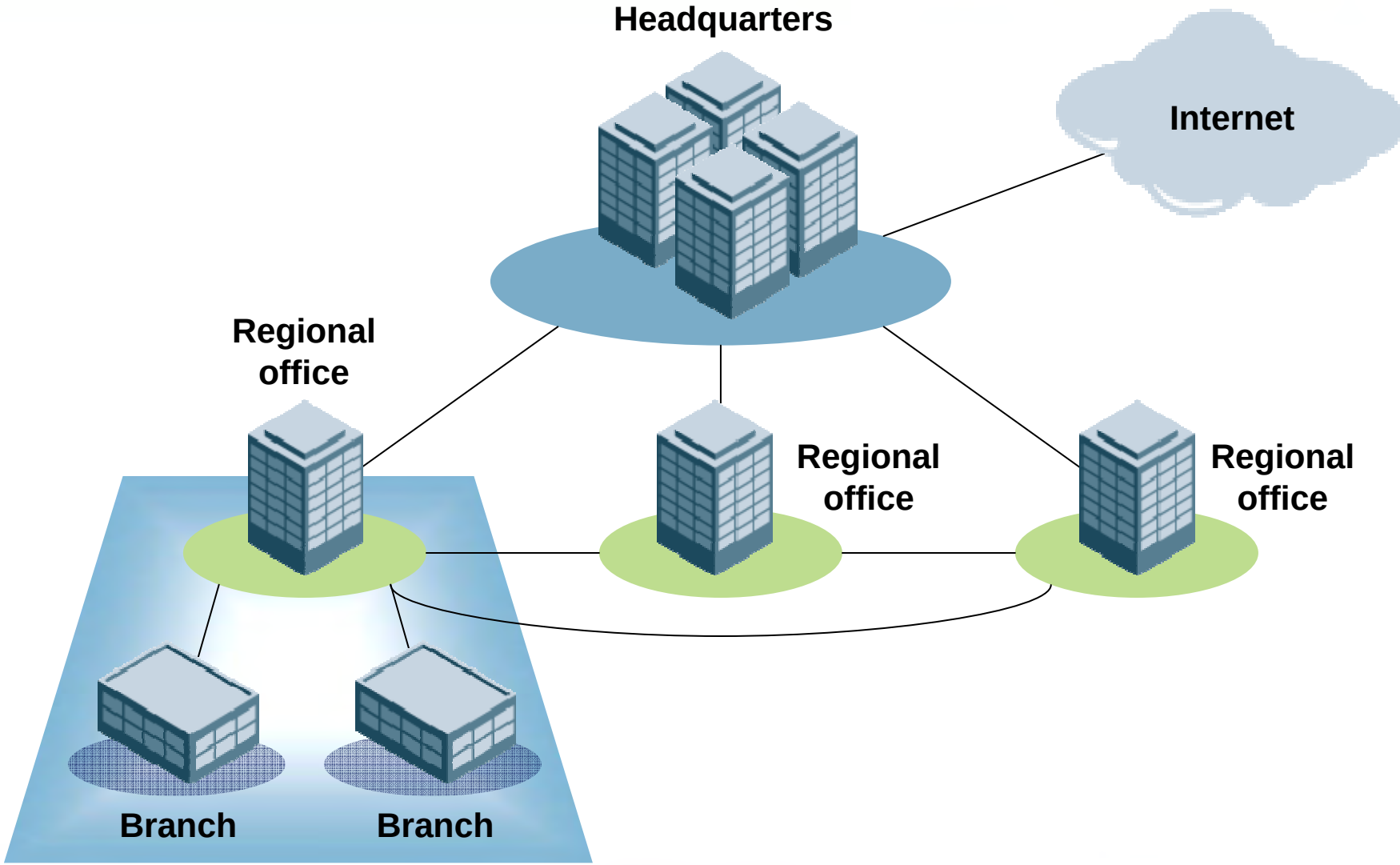


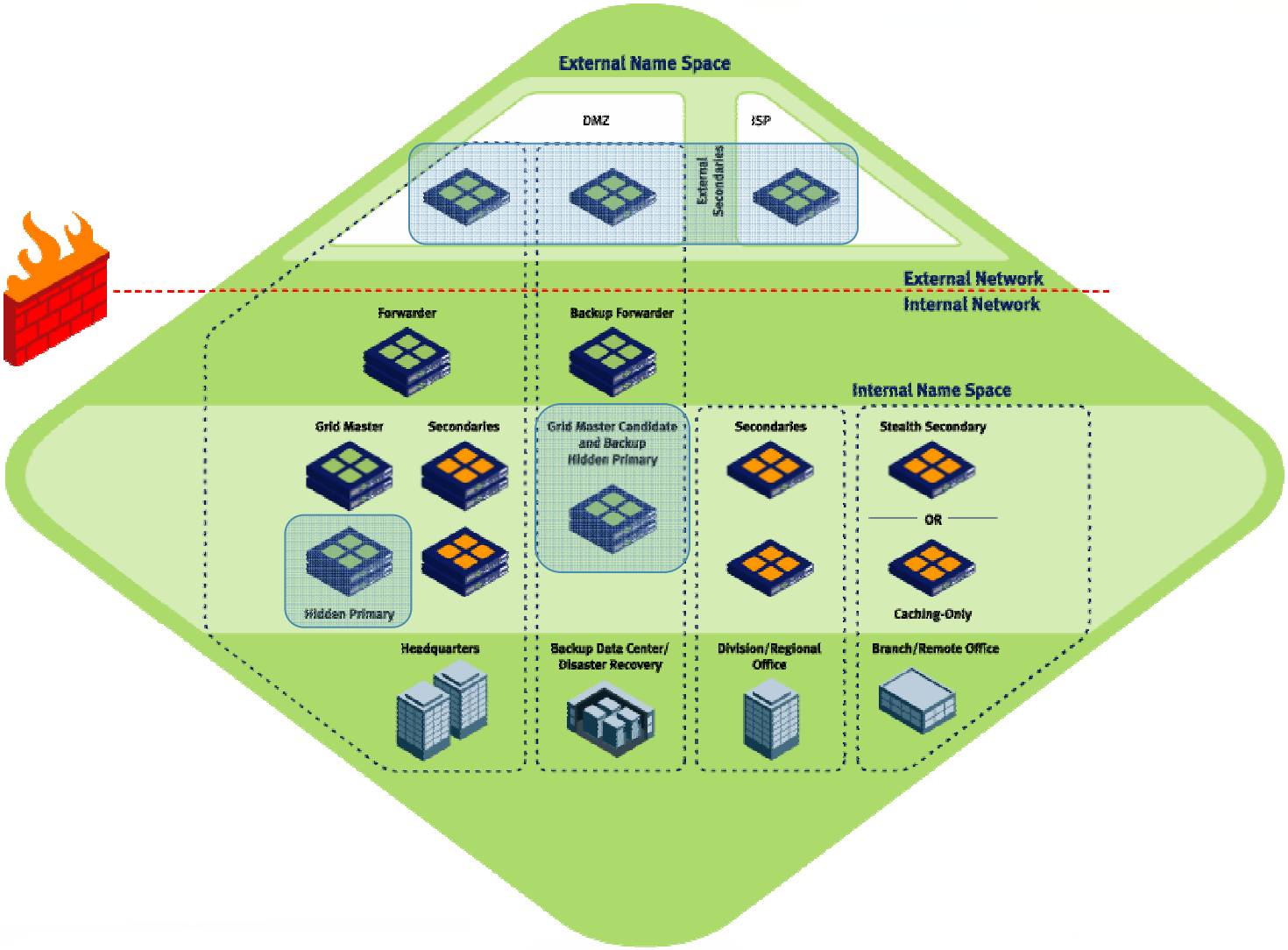
Company Background

- **Large U.S.-based company, Company Co. (*company.com*)**
- **Three categories of sites**
  - **Headquarters**
    - Roughly 2000 employees
    - Hosts all production applications (e.g., SAP), main connection to Internet
    - Hosts executive staff
    - Headquarters resources (e.g., hosts, printers) under *company.com*
  - **Regional offices**
    - 200 employees or fewer
    - Regional resources under *region.company.com*
    - Network connections to headquarters, two other regional offices
  - **Branch offices**
    - 12 employees or fewer
    - Each branch belongs to a region, resources under *region.company.com*
    - Network connection to supporting regional office
- **Single Active Directory domain, *company.com***
  - Domain Controllers at headquarters, regional offices

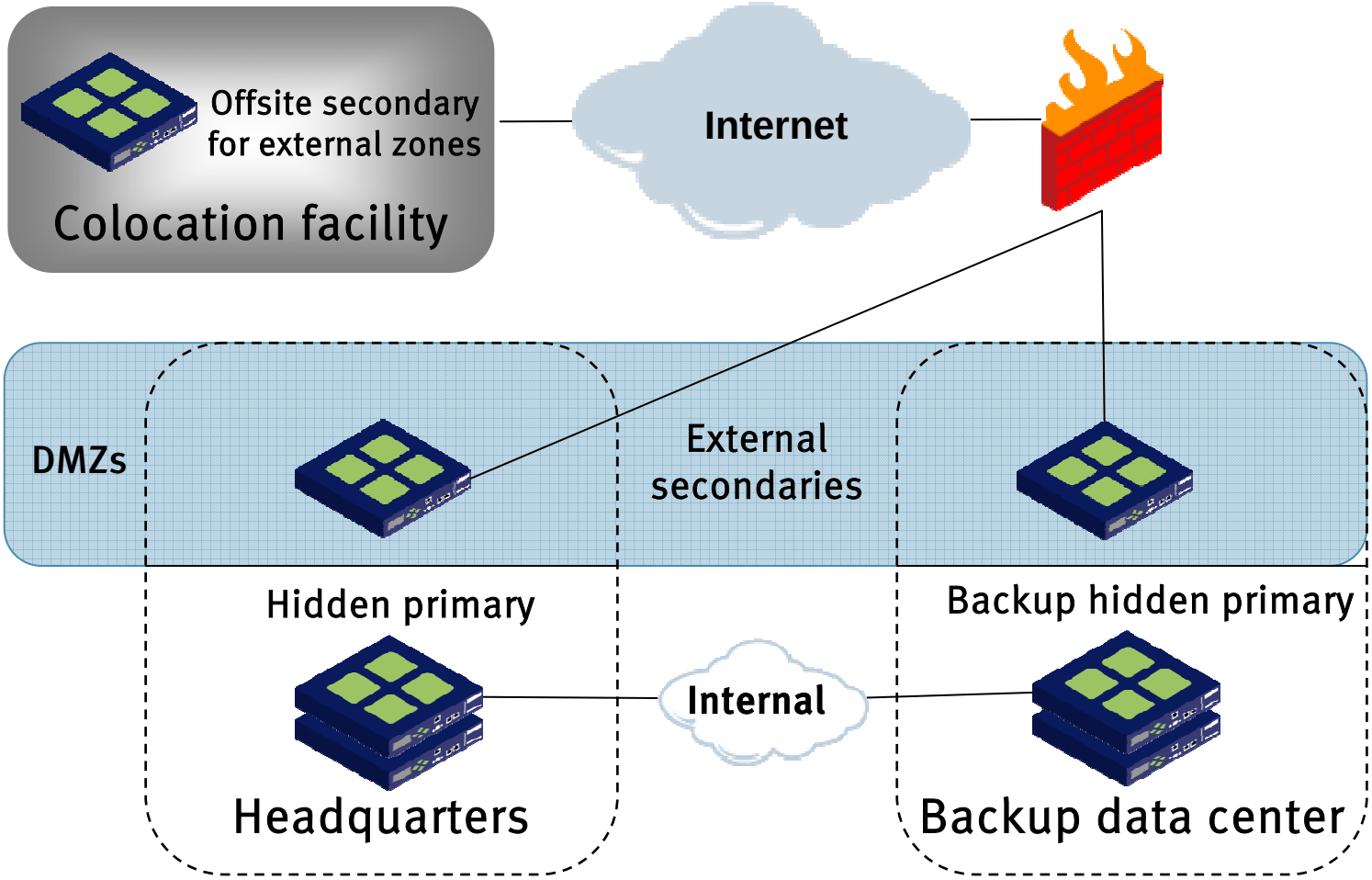
Corporate Network



DNS Architecture: External Authoritative DNS Infrastructure



External Authoritative DNS Infrastructure



External Authoritative DNS Infrastructure Notes

- **High availability hidden primary for external zones**
  - Inside firewall for protection
    - Secondaries are allowed to query, transfer zones
    - All other access from outside restricted, both via firewall and name server-based ACLs
  - Hidden to prevent external name servers from *trying* to query it
  - *High availability to protect "seat of administration"*
- **Two secondaries on DMZs**
  - One at headquarters
  - One at backup data center
  - Secured
    - Recursion disabled
    - Zone transfers disabled
    - *Hardened against attack*
    - *One-button upgrades to keep current*

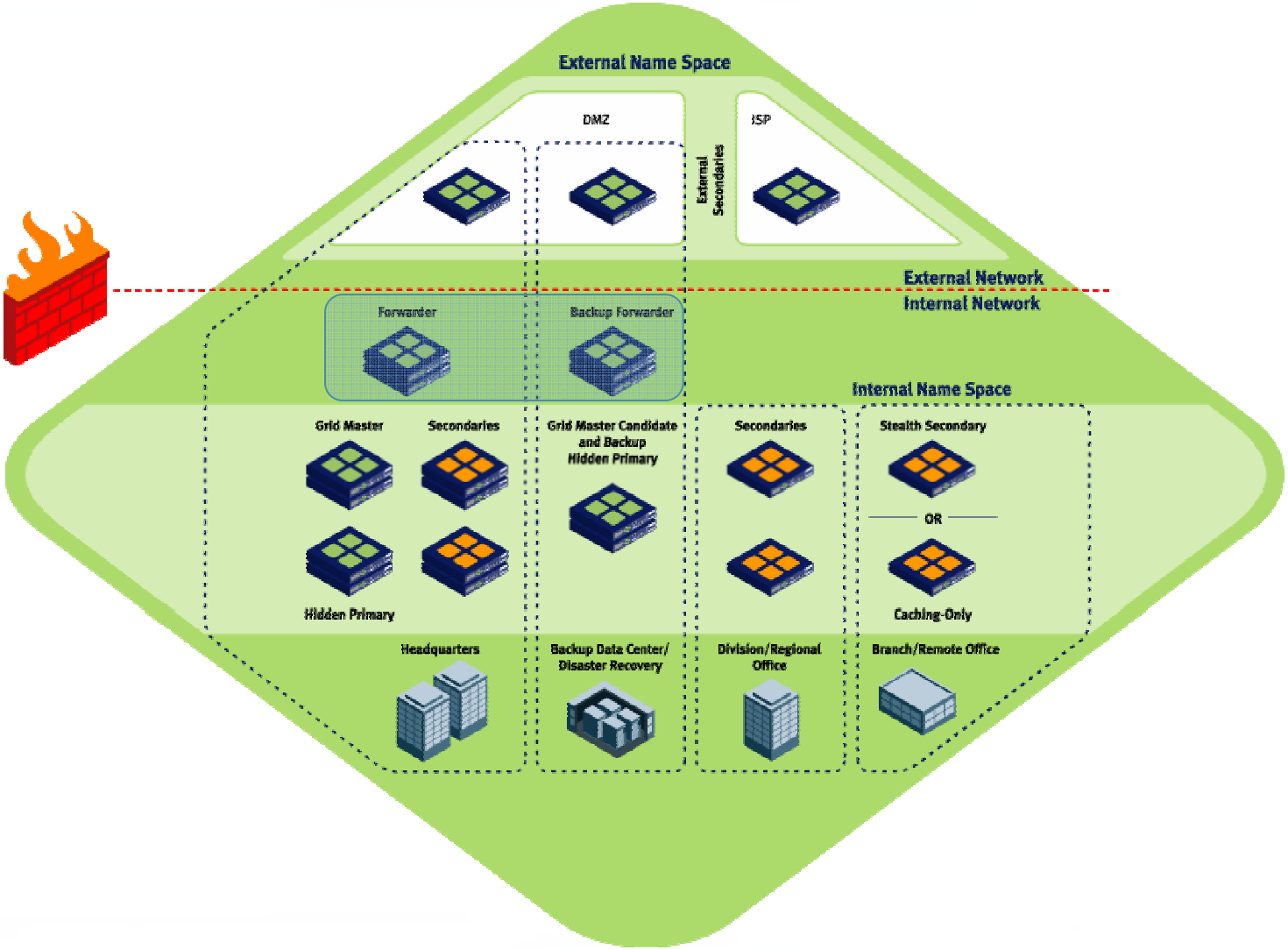
External Authoritative DNS Infrastructure Notes (cont.)

- **One secondary at colocation facility**
  - Provides offsite source of name service
  - Lower RTT than other name servers
    - Handles disproportionate share of queries
    - Keeps queries off link to Internet
  - **Secured**
    - Recursion disabled
    - Zone transfers disabled
    - *Hardened against attack*
    - *One-button upgrades to keep current*

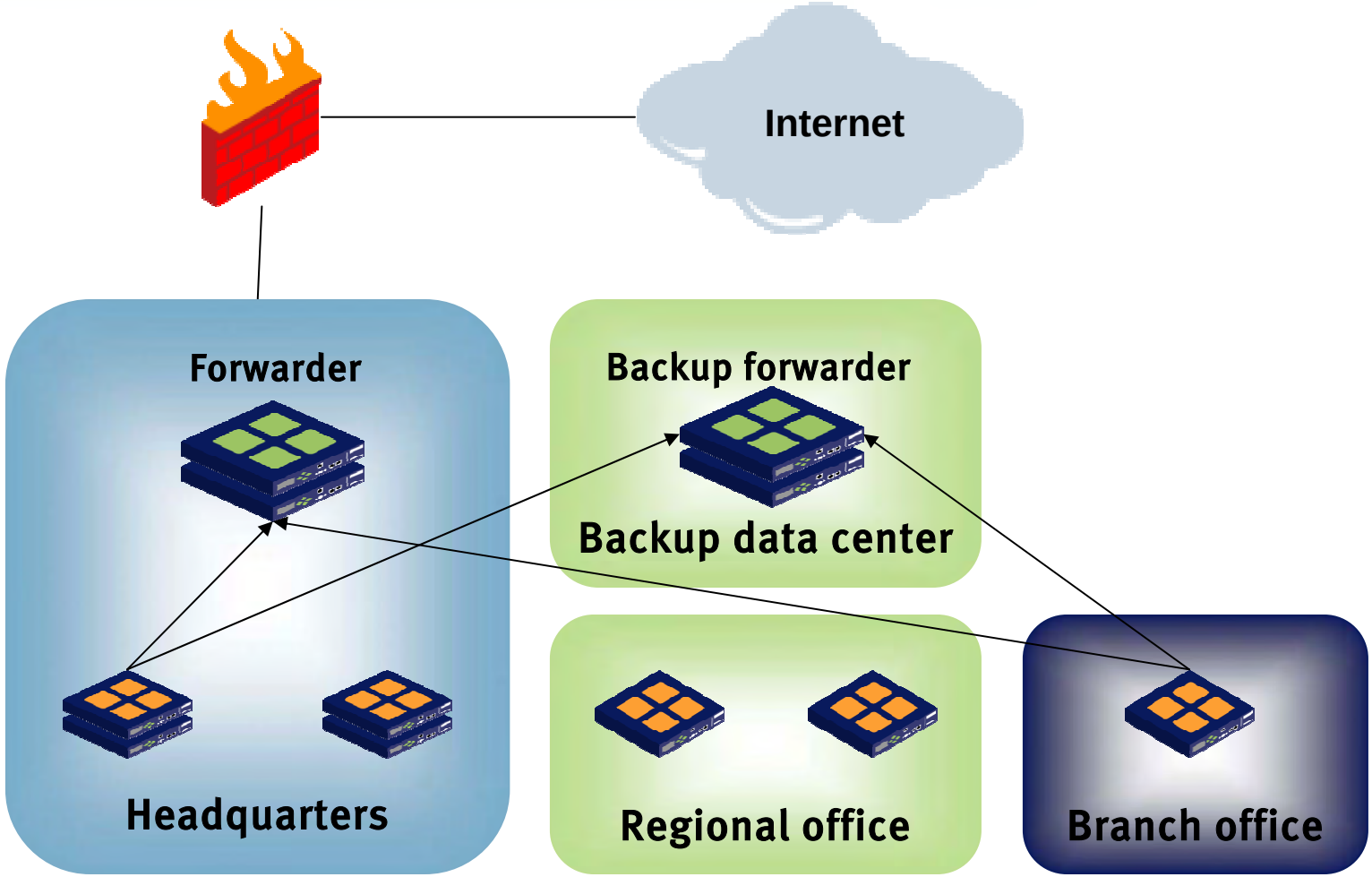
In a grid

- ***Single-point management of all appliances***
  - ***Also backup, restore, upgrade***
- ***Real-time propagation of changes***
- ***Changes to zone data with no interruption in service***
- ***Encrypted communication between grid members***

DNS Architecture:
Forwarding Infrastructure



Forwarding Infrastructure



Forwarding Infrastructure Notes

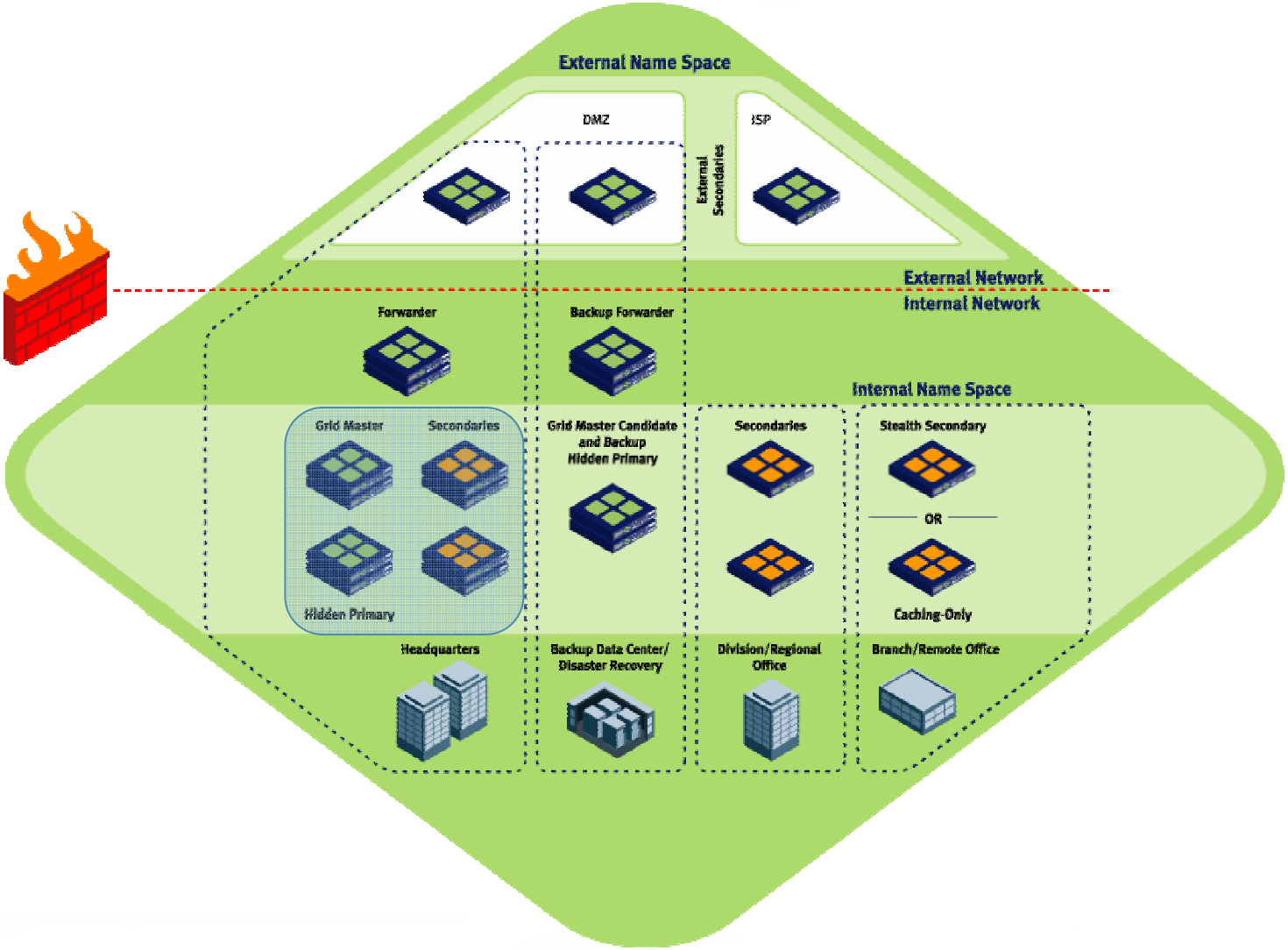
- **High availability forwarder**
  - Inside firewall for protection
    - State-based UDP filtering to allow forwarder to query Internet name servers, not vice versa
    - Redundant name server-based query ACL
  - High availability to provide nonstop name service
    - Name servers using multiple forwarders incur multi-second timeouts for each query if forwarders don't respond
- **High availability backup forwarder at backup data center**
  - To provide forwarding service in case of a catastrophic failure at headquarters
- **All internal recursive name servers forward to forwarders**
  - To avoid bottleneck in internal name resolution, forwarding is overridden for resolution of internal domain names

Forwarding Infrastructure Notes (cont.)

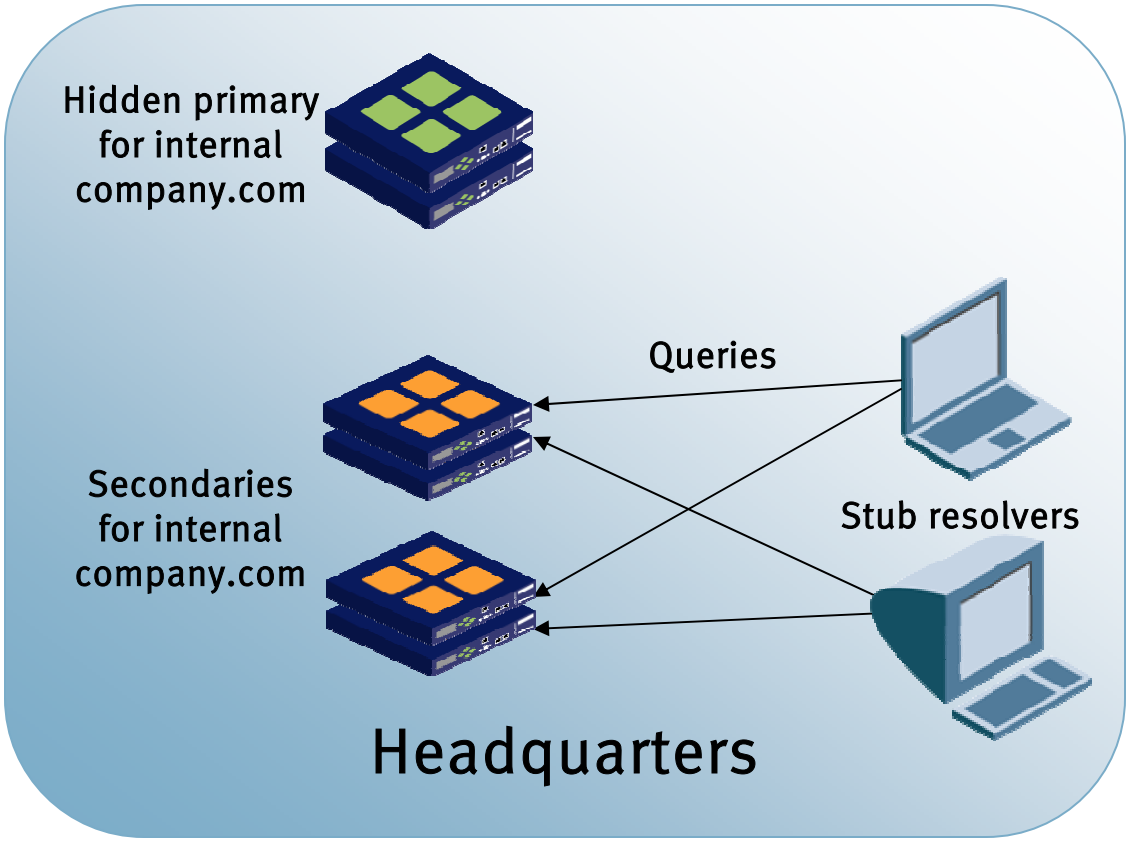
In a grid

- *Hierarchical configuration to reconfigure forwarding on all distribution-layer name servers at once*

DNS Architecture: Headquarters DNS Infrastructure



Headquarters DNS Infrastructure



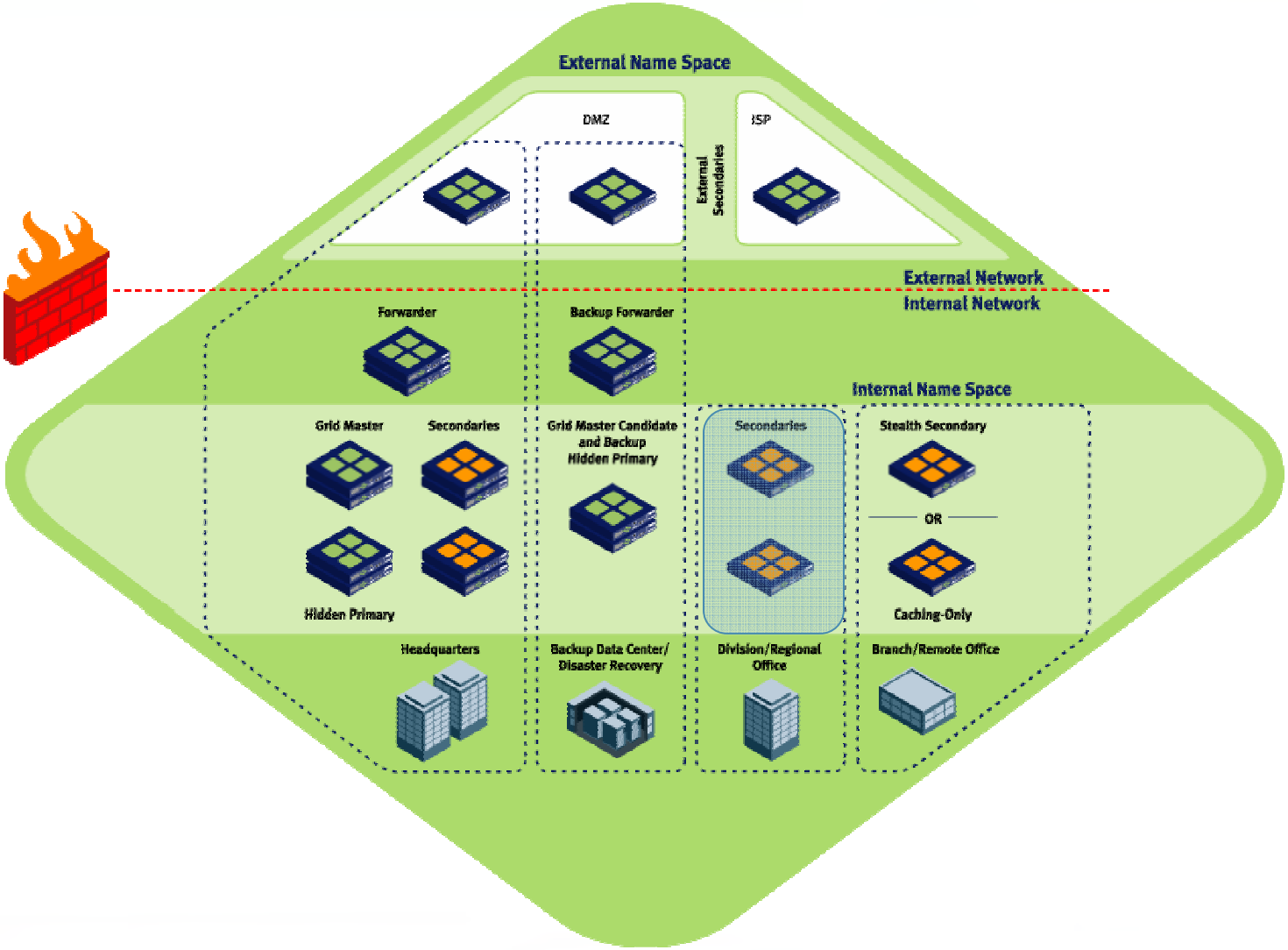
Headquarters DNS Infrastructure Notes

- **Hidden primary for internal *company.com***
  - Provides operational flexibility
  - *High availability to protect "seat of administration," processing of dynamic updates*
- **High availability secondaries for *company.com***
  - *High availability to provide nonstop name service*
    - Continue serving resolvers even during upgrades
  - Resolvers configured to query closer secondary first, then other secondary
    - Minimizes latency
    - Provides redundancy and load balancing
- ***GUI to simplify administration, help prevent mistakes, allow delegation of data management to junior staff or help desk, provide auditing***

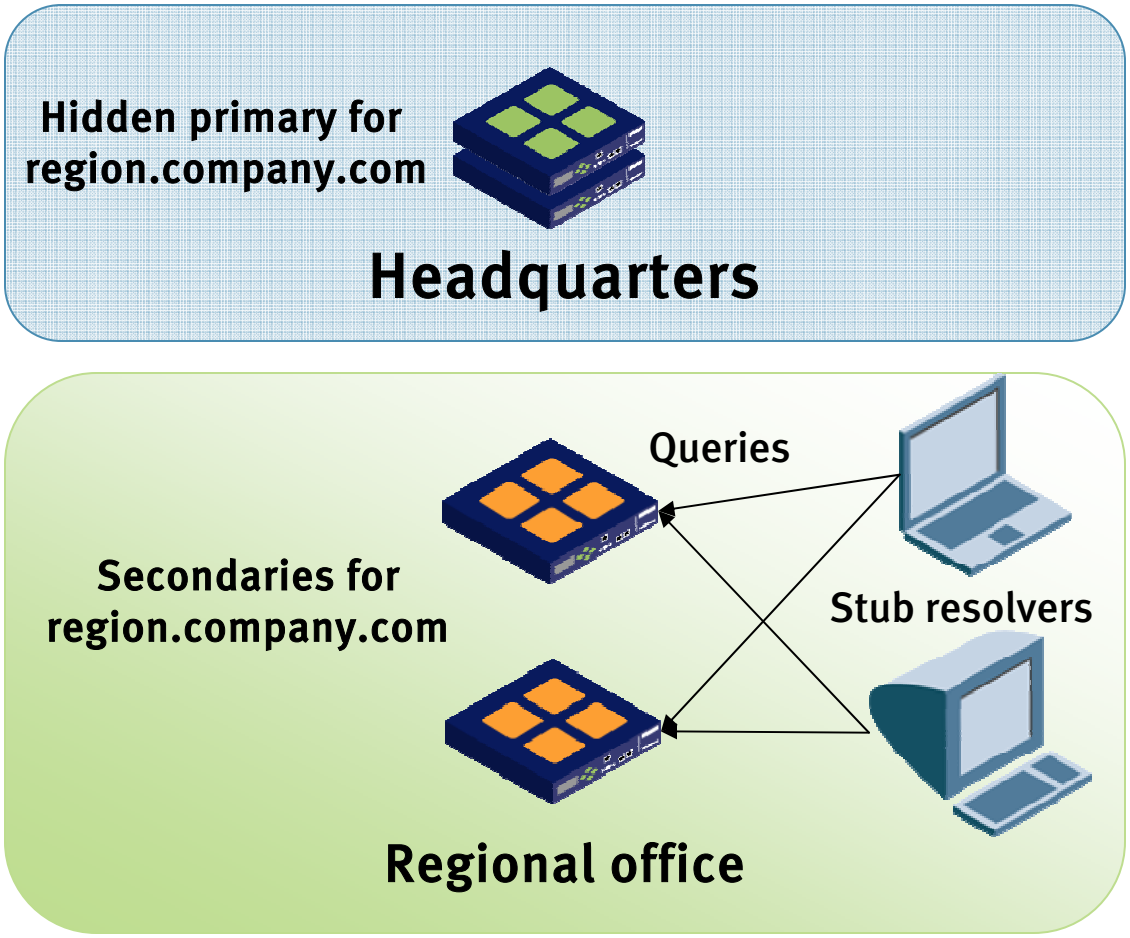
In a grid

- *Single-point management of all appliances*
- *Single-point management of complete corporate namespace, including internal and external views*
- *Hierarchical configuration with inheritance*
- *Shared grid authentication and authorization database*
- *IP Address Management (IPAM) functionality*

DNS Architecture: Regional Office DNS Infrastructure



Regional DNS Infrastructure



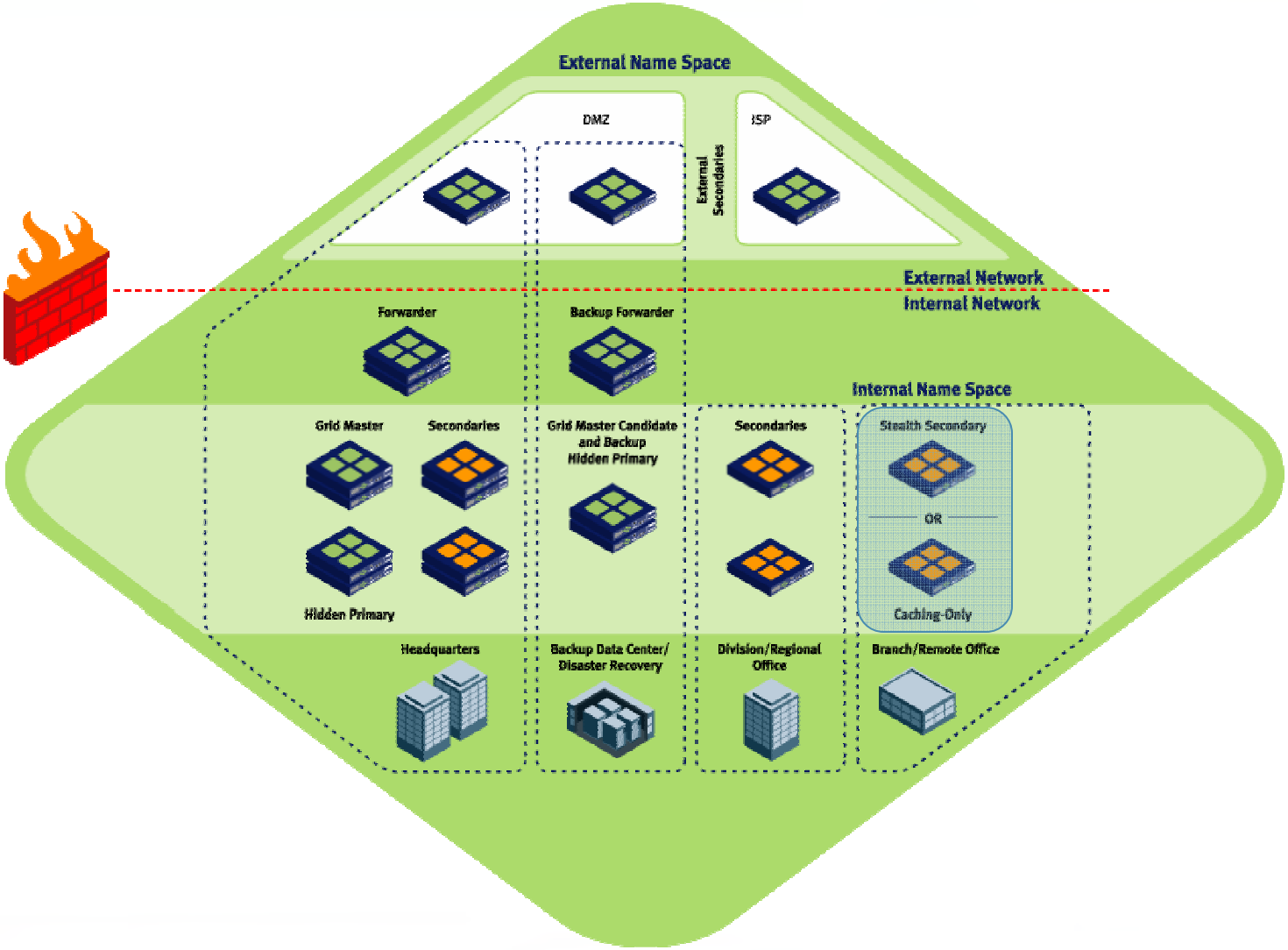
Regional DNS Infrastructure Notes

- **High availability hidden primary for *region.company.com***
  - Provides operational flexibility
  - *High availability to protect "seat of administration," processing of dynamic updates*
- **Secondaries for *region.company.com***
  - Resolvers configured to query closer secondary first, then other secondary
    - Minimizes latency
    - Provides redundancy and load distribution
- ***GUI allows headquarters staff to control configuration and administration of name server, while delegating management of region.company.com and relevant reverse-mapping zones to regional office staff***

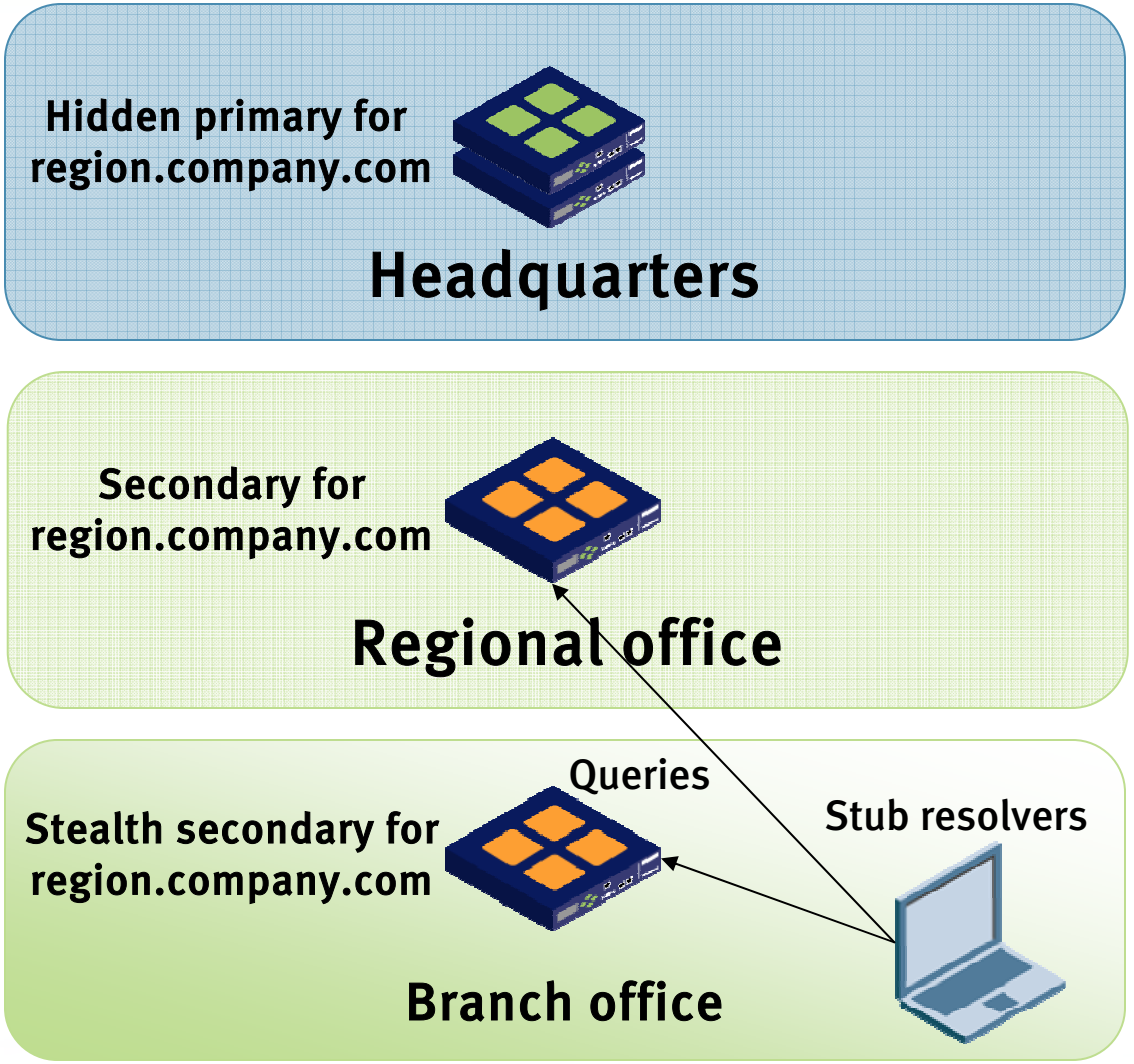
In a grid

- ***Single view of complete corporate namespace***
- ***Shared grid authentication and authorization database***
- ***Hierarchical configuration with inheritance***
- ***Appliance pre-provisioning and automatic recovery***

DNS Architecture: Branch DNS Infrastructure



Branch DNS Infrastructure



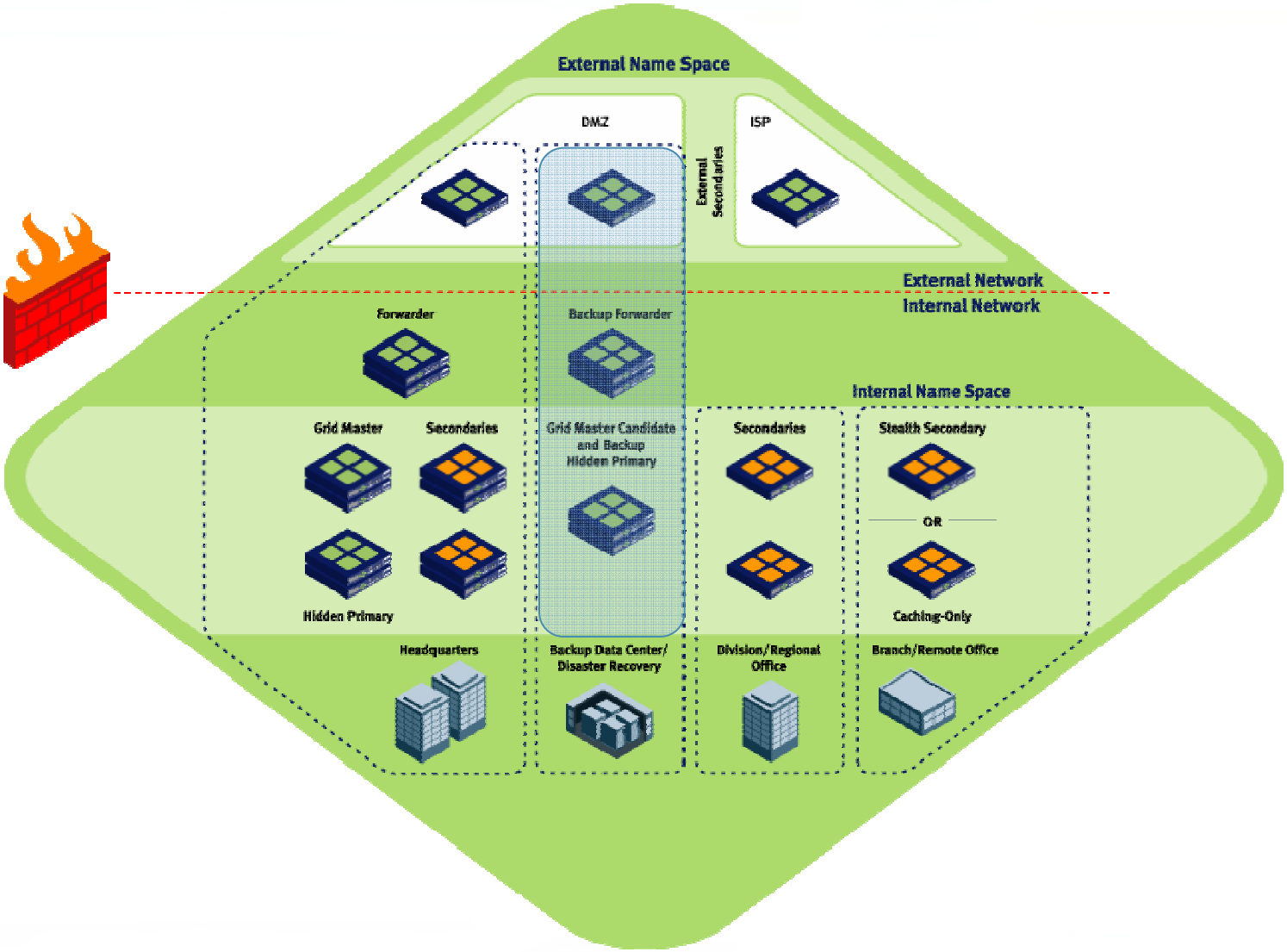
Branch DNS Infrastructure Notes

- **Stealth secondary for *region.company.com***
  - Provides a local source of all regional zone data
  - Stealth to prevent remote internal name servers from querying it and congesting link to network
- **Resolvers configured to query local secondary first, then secondary at regional office**
  - Minimizes latency
  - Provides redundancy and load distribution
- ***GUI allows headquarters staff to remotely configure and manage name server***
  - *Including all system administration, e.g., upgrades, backups*

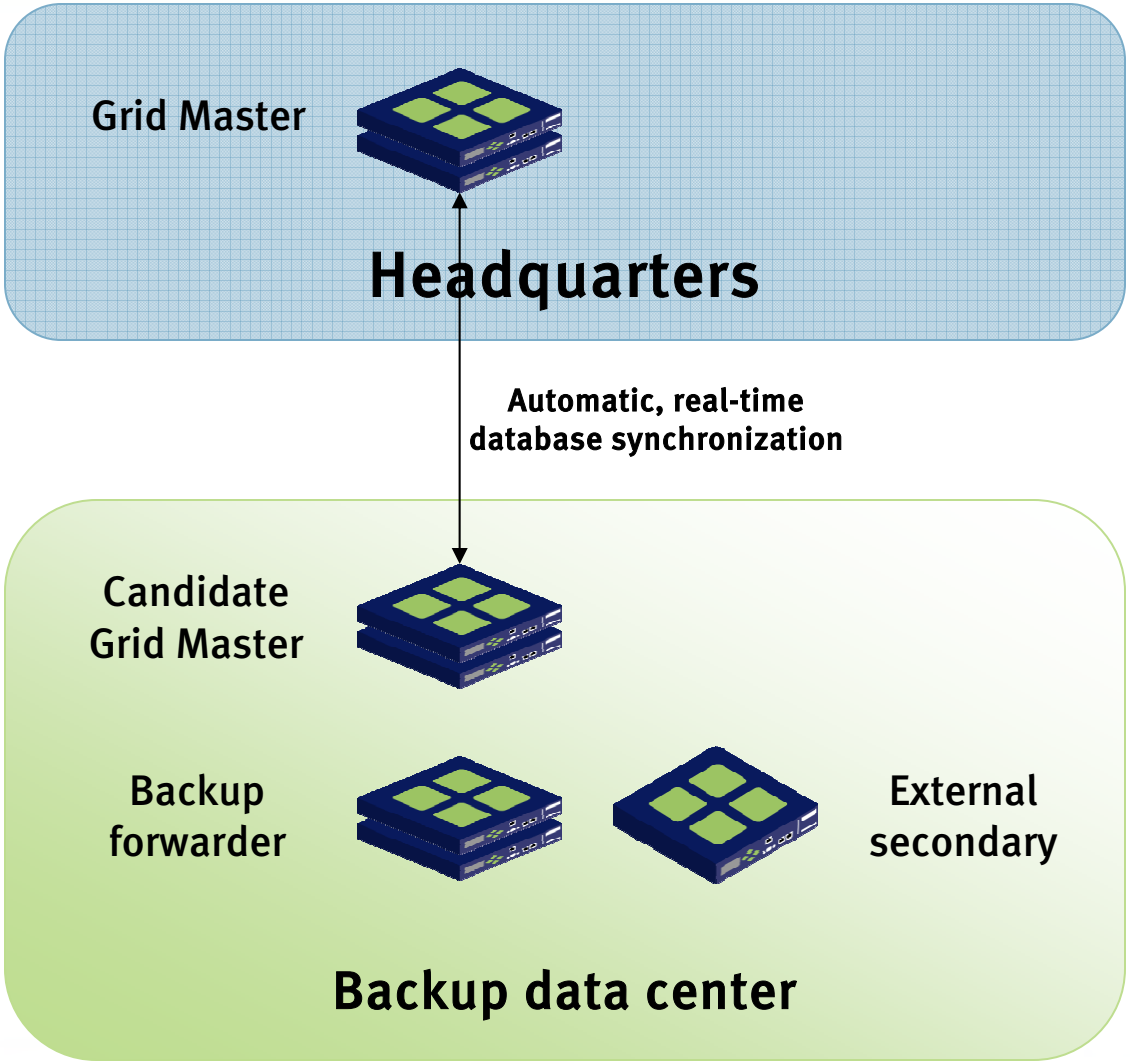
In a grid

- *Single-point management of all appliances*
  - *Also backup, restore, upgrade*
- *Hierarchical configuration with inheritance*
- *Appliance pre-provisioning and automatic recovery*

DNS Architecture: Disaster Recovery Infrastructure



Disaster Recovery Infrastructure

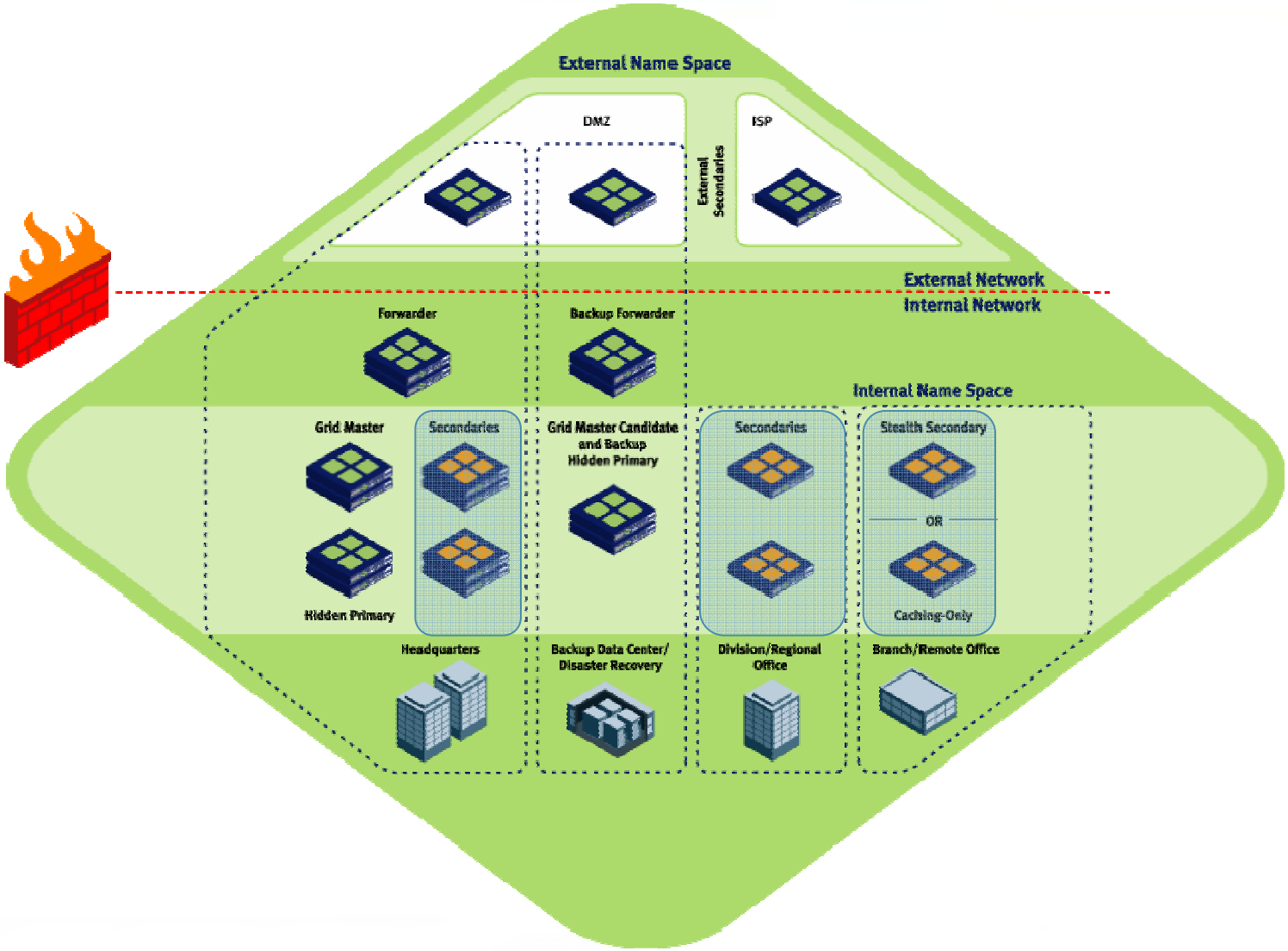


Disaster Recovery Notes

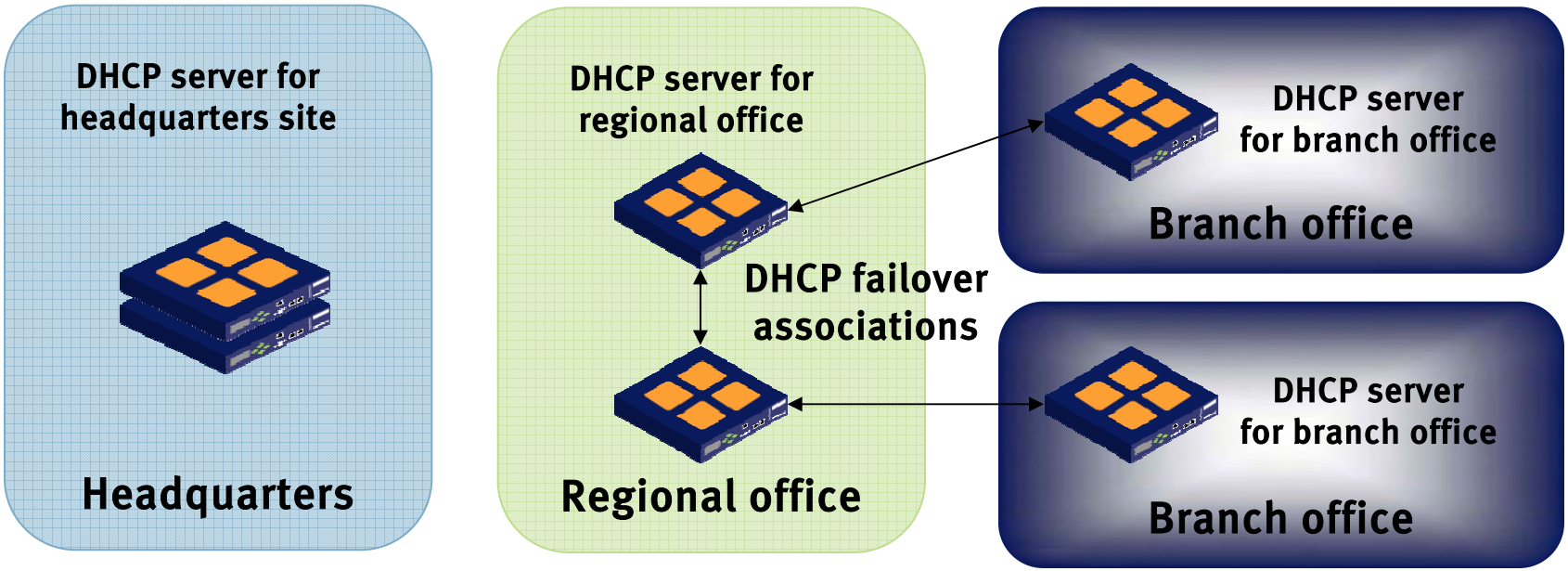
In a grid

- ***Single-point backup***
  - ***Backups include protocol and appliance configurations***
    - ***Everything required to restore entire grid***
- ***Automatic recovery***
- ***Disconnected operation***
- ***Candidate (Backup) Grid Master at backup data center***
  - ***In event of catastrophic loss of Grid Master, Candidate can be promoted without loss of data***
  - ***While Grid Master is unavailable, members continue serving DNS and DHCP, queuing updates***

DNS Architecture: DHCP Infrastructure



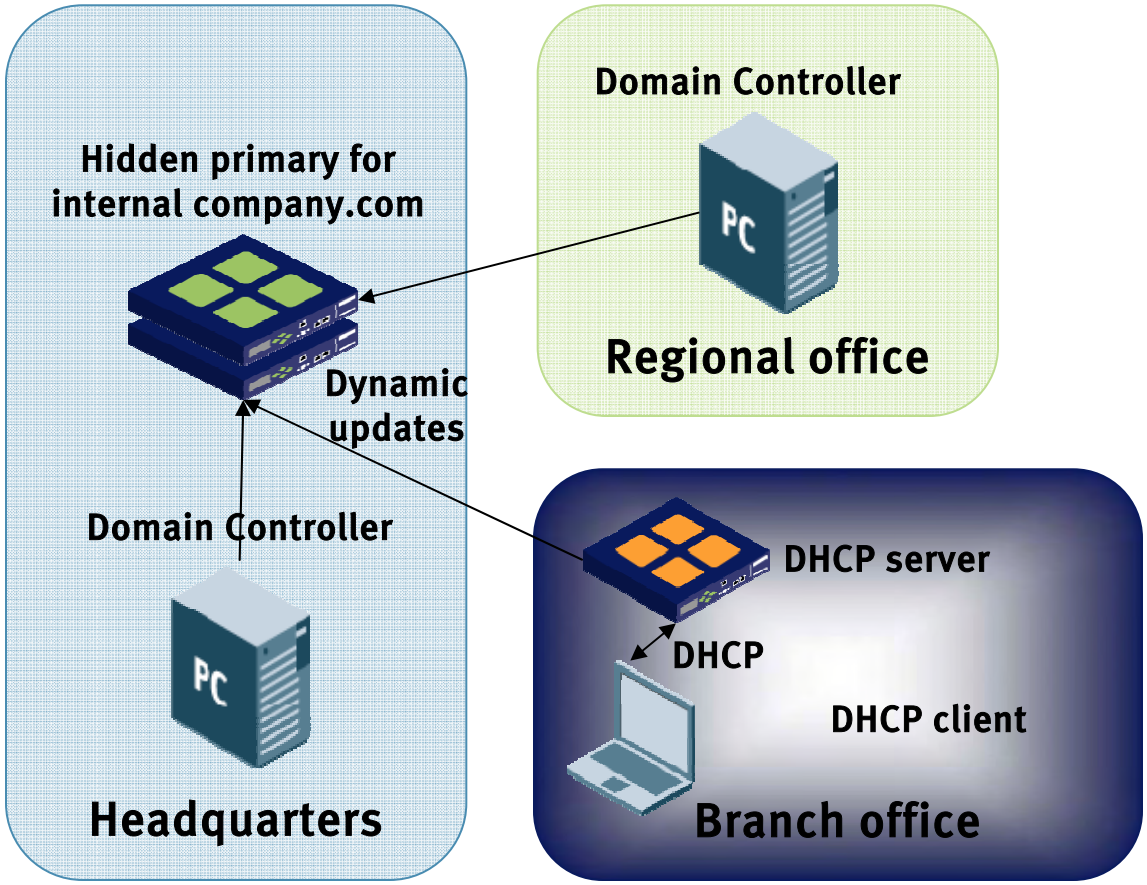
DHCP Infrastructure



DHCP Infrastructure Notes

- **All internal secondary name servers also run DHCP servers**
  - To provide DHCP to the local site
- **DHCP is always run in a high availability or failover configuration**
  - *At headquarters, DHCP runs on a high availability platform*
  - At regional offices, DHCP runs on failover peers
    - Both local secondaries
  - At branch offices, DHCP also runs on failover peers
    - Local stealth secondary and one regional office secondary
- **DHCP servers update appropriate primary name servers with DHCP clients' forward and reverse mappings**
  - Supports DHCP clients not able to manage forward and reverse mappings themselves
  - DHCP clients are not allowed to update zones directly, avoiding namespace pollution and security risk
- **Beginning rollout of "authenticated DHCP"**
  - Users on DHCP clients must authenticate themselves to a Domain Controller before being granted a permanent lease
  - User identity and leased IP address are captured and logged

Active Directory



Active Directory Notes

- **The company's Active Directory domain's name is *company.com***
- **To support Active Directory, Domain Controllers are allowed to update records that advertise services offered**
  - These records are in six zones:
    - *_msdcs.company.com*
    - *_sites.company.com*
    - *_tcp.company.com*
    - *_udp.company.com*
    - *DomainDNSZones.company.com*
    - *ForestDNSZones.company.com*
- ***GUI provides simple interface for configuring this***
  - *Only need to enter addresses of Domain Controllers*
  - *Zones are created automatically*
- ***All primary name servers run in high availability configurations to ensure that Domain Controllers' updates are received***

VoIP Notes

- **The requirement for redundant DHCP service was largely due to VoIP's dependence on DHCP**
  - Without DHCP, most VoIP devices don't operate
- **Redundant DHCP can be provided by**
  - High availability
  - DHCP Failover
  - A combination of these
- **Most VoIP devices also require custom DHCP options**
  - E.g., option 172 for Avaya SIP VoIP phones or option 176 for Avaya H.323 VoIP phones
- **Most VoIP devices require TFTP or HTTP to download configuration and firmware images**
  - All DHCP servers also run TFTP and HTTP to support this

In a grid

- **DHCP options can be defined for all DHCP servers in the grid**
- **Single-point configuration of TFTP and HTTP**
  - **Configuration files and firmware images are synchronized among all TFTP and HTTP servers**

Summary

- **This architecture provides**
  - Resiliency in the face of hardware or network failures
  - Good security, especially for name servers directly exposed to the Internet
  - Good separation of critical functions (e.g., external authoritative name servers and forwarders)
  - Local data administration and processing of dynamic updates
  - Protection and insulation from configuration and data administration mistakes
  - Local recursive name servers for all resolvers
  - Redundant DHCP service for all clients
  - Support for Active Directory and VoIP

A Special Bonus: DNS Advisor

- **Infoblox offers a free web service, DNS Advisor**
  - Performs 50 different tests on your external authoritative name servers, checking
    - Delegation
    - Responsiveness
    - Redundancy
    - Authority
    - Configuration (e.g., SOA RDATA)
    - Security (e.g., recursion, zone transfers, name server version)
    - Protocol compliance (e.g., TCP queries, EDNS0, SPF)
  - Allows you to create a PDF report from the output

dnsadvisor.infoblox.com

dnsadvisor.infoblox.com

Infoblox

Thank you

Take the Next Step to an Identity-Driven Network

Infoblox

- Schedule a DNS Health Check™ to expose immediate issues
  - Close security holes
  - Eliminate bottlenecks and failure points
- Conduct a detailed system audit and design review
  - Identify key initiatives and requirements
    - Wireless, VoIP, endpoint security, NAC, etc.
  - Develop a roadmap for DNS, DHCP, IPAM, and RADIUS implementation
- Schedule a DNSone evaluation at your facility
- Take advantage of the tools and programs offered by Infoblox and our IDeal™ Program Partners
  - DNS Best Practices Design Tools
  - Microsoft AD Best Practices Design Tools
  - Design services
  - Data migration services
  - Custom applications and API integration