US 20250260664A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0260664 A1**

Iyer et al. (43) **Pub. Date: Aug. 14, 2025**

(54) **TWO TIER DNS**

(71) Applicant: **VMware, Inc.**, Palo Alto, CA (US)

(72) Inventors: **Sreeram Iyer**, Bengaluru (IN); **Murali Basavaiah**, Los Altos, CA (US); **Prasad Rao**, Bengaluru (IN); **Shyam Prasad Anisetti**, Bengaluru (IN); **Naveen Dhillon**, Bengaluru (IN)

(21) Appl. No.: **19/193,322**

(22) Filed: **Apr. 29, 2025**

Related U.S. Application Data

(63) Continuation of application No. 18/211,553, filed on Jun. 19, 2023, now Pat. No. 12,316,601.

(30) **Foreign Application Priority Data**

Jul. 14, 2022 (IN) 202241040390

Publication Classification

(51) **Int. Cl.**

H04L 61/4511 (2022.01)

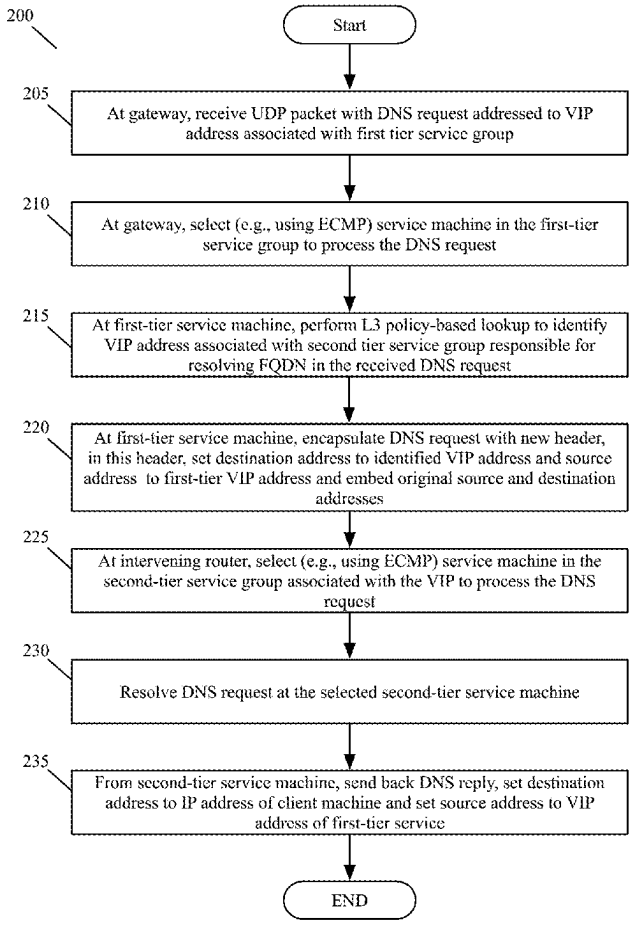
H04L 67/1004 (2022.01)

(52) **U.S. Cl.**

CPC ***H04L 61/4511*** (2022.05); ***H04L 67/1004*** (2013.01)

(57) **ABSTRACT**

Some embodiments provide a two-tier DNS (Domain Name System) service for processing DNS requests. In some embodiments, the two-tier DNS service deploys first and second tiers of service machines, with the second-tier having several groups of service machines each of which is configured to resolve DNS requests for a different set of domain names than the other second-tier group(s). Each service machine in the first-tier is configured to identify the second-tier group responsible for each particular DNS request that the service machine receives for each particular domain name, and to forward the particular DNS request to the second-tier group that it identifies for the particular DNS request. The first-tier DNS service in some embodiments has only one group of service machines. Each first or second service machine group in some embodiments can have one or more service machines, and can be scaled up or down to add or remove service machines to the group (e.g., through an active/active layer 3 scaleout with BGP). In some embodiments, two different second-tier service groups can process DNS requests for two or more different FQDNs (fully qualified domain names) that are part of the same domain, and/or for two or more different FQDNs that are part of different domains.



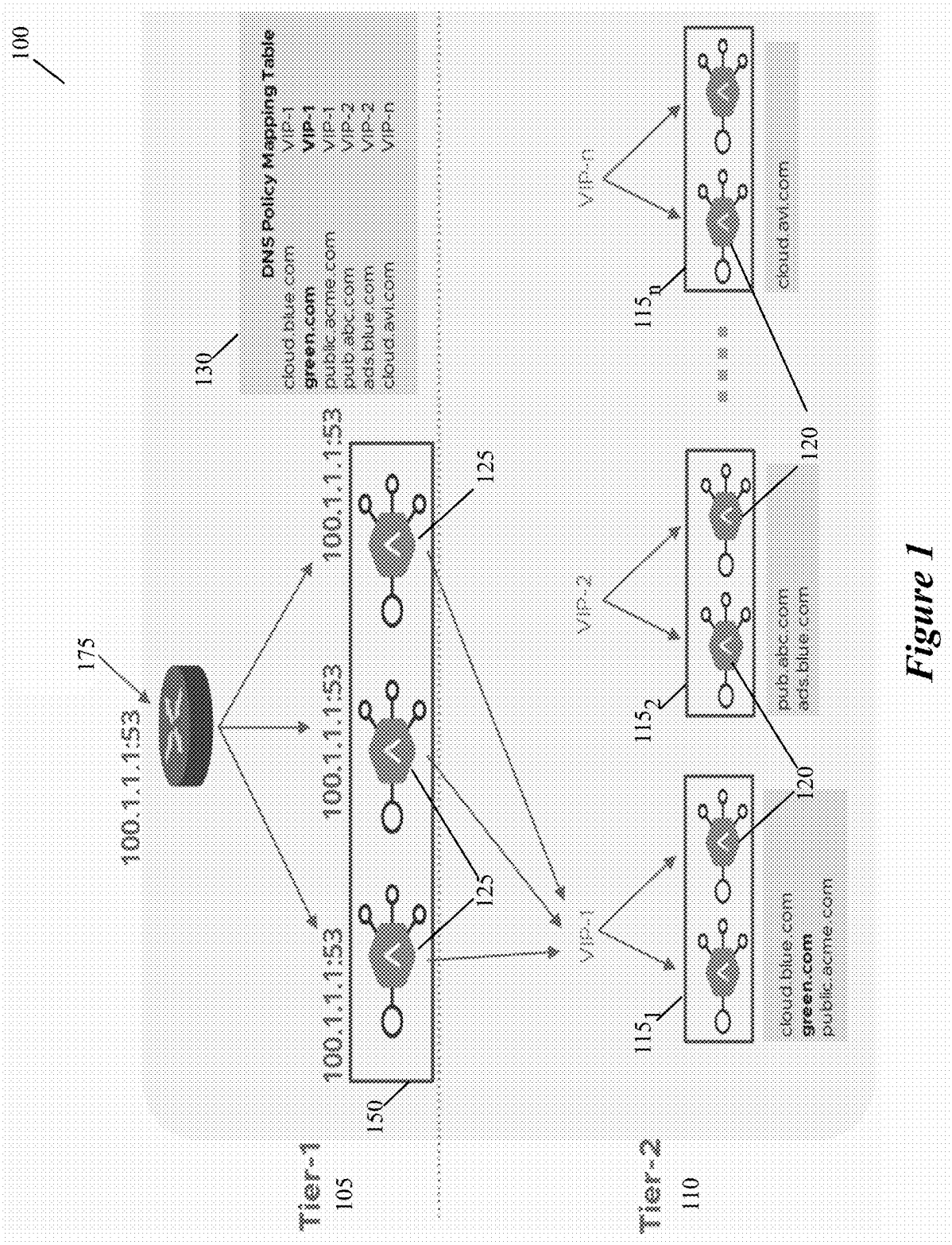

100
175
100.1.1.1:53
130
DNS Policy Mapping Table
VIP-1
cloud.blue.com
green.com
public.acme.com
pub.abc.com
ads.blue.com
cloud.avi.com
VIP-1
VIP-1
VIP-2
VIP-2
VIP-n
100.1.1.1:53
100.1.1.1:53
100.1.1.1:53
125
125
150
Tier-1
105
VIP-1
VIP-2
VIP-n
115₁
115₂
115n
120
120
cloud.blue.com
green.com
public.acme.com
pub.abc.com
ads.blue.com
cloud.avi.com
Tier-2
110

Figure 1

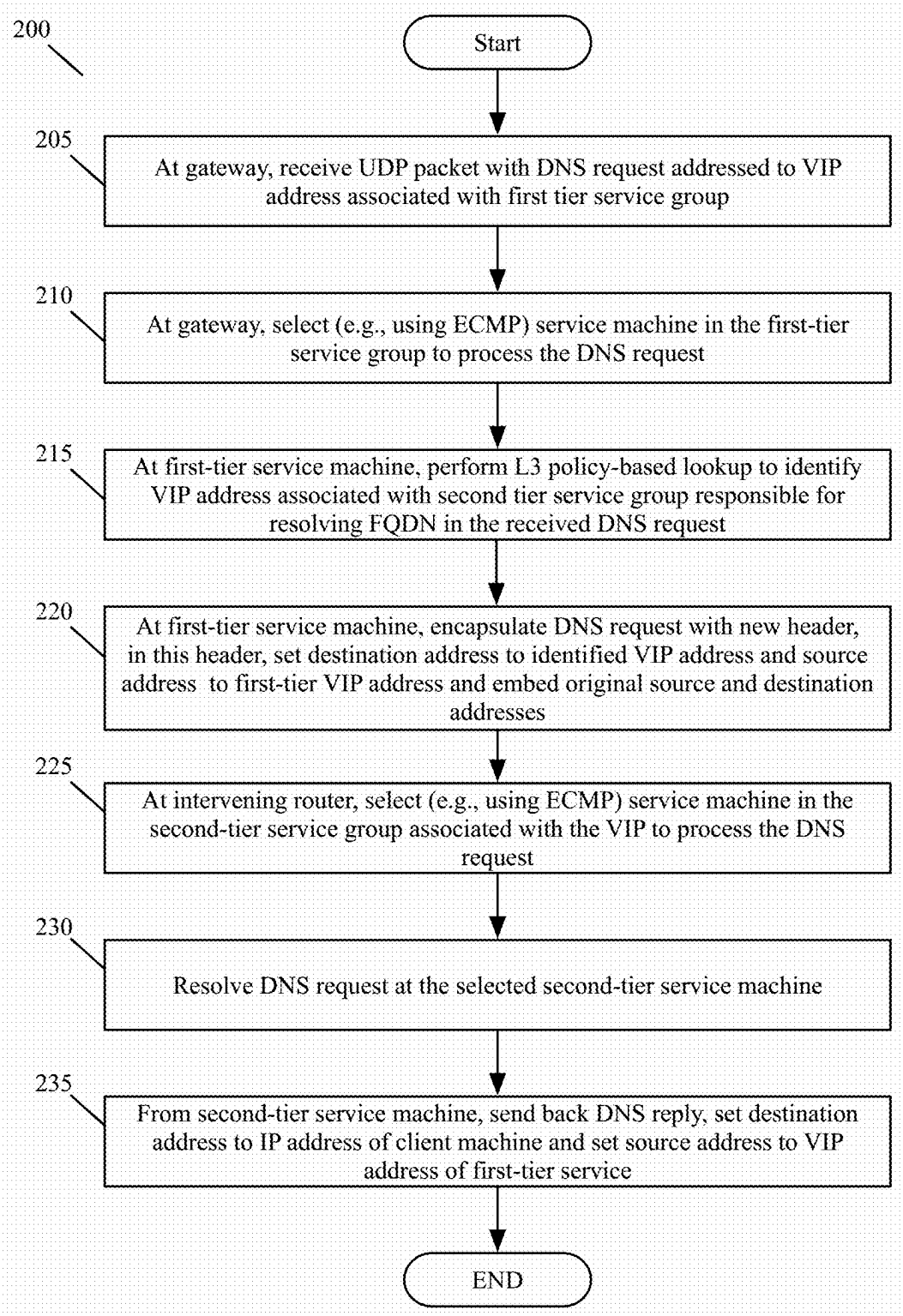

200
Start
205
At gateway, receive UDP packet with DNS request addressed to VIP address associated with first tier service group
210
At gateway, select (e.g., using ECMP) service machine in the first-tier service group to process the DNS request
215
At first-tier service machine, perform L3 policy-based lookup to identify VIP address associated with second tier service group responsible for resolving FQDN in the received DNS request
220
At first-tier service machine, encapsulate DNS request with new header, in this header, set destination address to identified VIP address and source address to first-tier VIP address and embed original source and destination addresses
225
At intervening router, select (e.g., using ECMP) service machine in the second-tier service group associated with the VIP to process the DNS request
230
Resolve DNS request at the selected second-tier service machine
235
From second-tier service machine, send back DNS reply, set destination address to IP address of client machine and set source address to VIP address of first-tier service
END

Figure 2

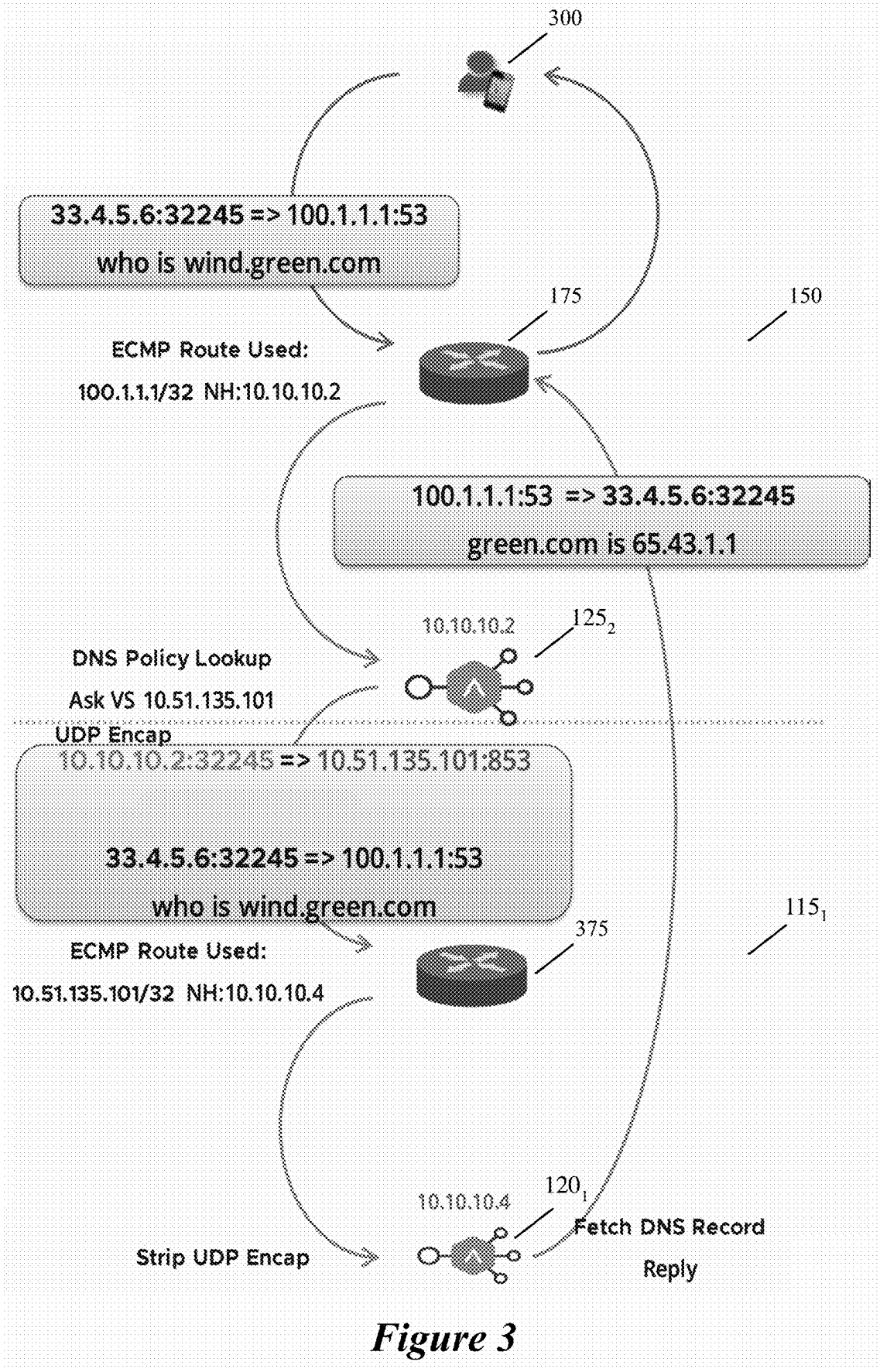

300
33.4.5.6:32245 => 100.1.1.1:53
who is wind.green.com
175
150
ECMP Route Used:
100.1.1.1/32 NH:10.10.10.2
100.1.1.1:53 => 33.4.5.6:32245
green.com is 65.43.1.1
10.10.10.2
125₂
DNS Policy Lookup
Ask VS 10.51.135.101
UDP Encap
10.10.10.2:32245 => 10.51.135.101:853
33.4.5.6:32245 => 100.1.1.1:53
who is wind.green.com
115₁
375
ECMP Route Used:
10.51.135.101/32 NH:10.10.10.4
120₁
10.10.10.4
Fetch DNS Record
Reply
Strip UDP Encap

Figure 3

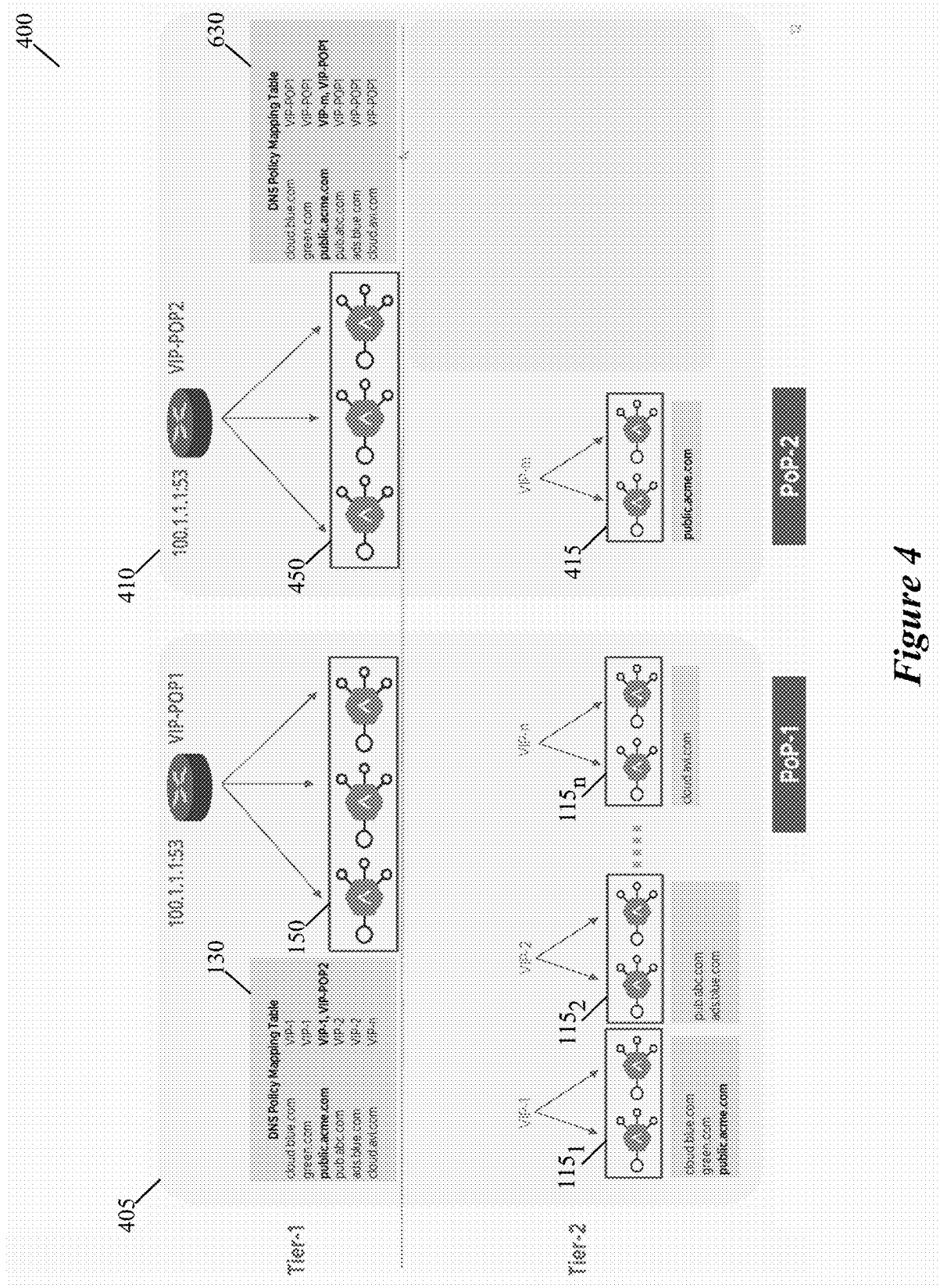

400
405
410
130
150
450
630
415
VIP-POP3
VIP-POP2
100.1.1.1:53
DNS Policy Mapping Table
VIP-1, VIP-POP2
VIP-n, VIP-POPn
public.acme.com
Tier-1
Tier-2
PoP-1
PoP-2

Figure 4

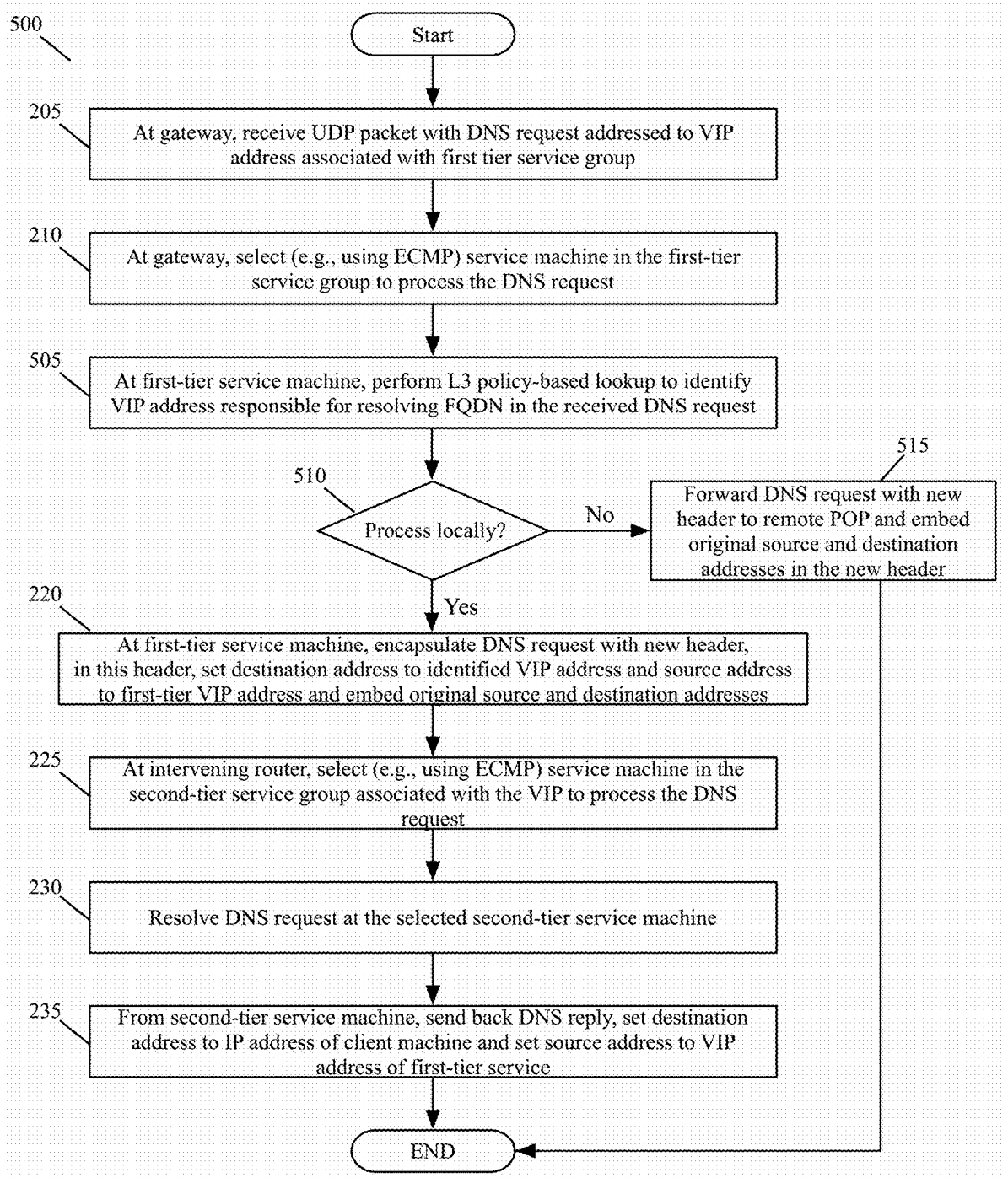

500
Start
205
At gateway, receive UDP packet with DNS request addressed to VIP address associated with first tier service group
210
At gateway, select (e.g., using ECMP) service machine in the first-tier service group to process the DNS request
505
At first-tier service machine, perform L3 policy-based lookup to identify VIP address responsible for resolving FQDN in the received DNS request
510
Process locally?
No
515
Forward DNS request with new header to remote POP and embed original source and destination addresses in the new header
Yes
220
At first-tier service machine, encapsulate DNS request with new header, in this header, set destination address to identified VIP address and source address to first-tier VIP address and embed original source and destination addresses
225
At intervening router, select (e.g., using ECMP) service machine in the second-tier service group associated with the VIP to process the DNS request
230
Resolve DNS request at the selected second-tier service machine
235
From second-tier service machine, send back DNS reply, set destination address to IP address of client machine and set source address to VIP address of first-tier service
END

Figure 5

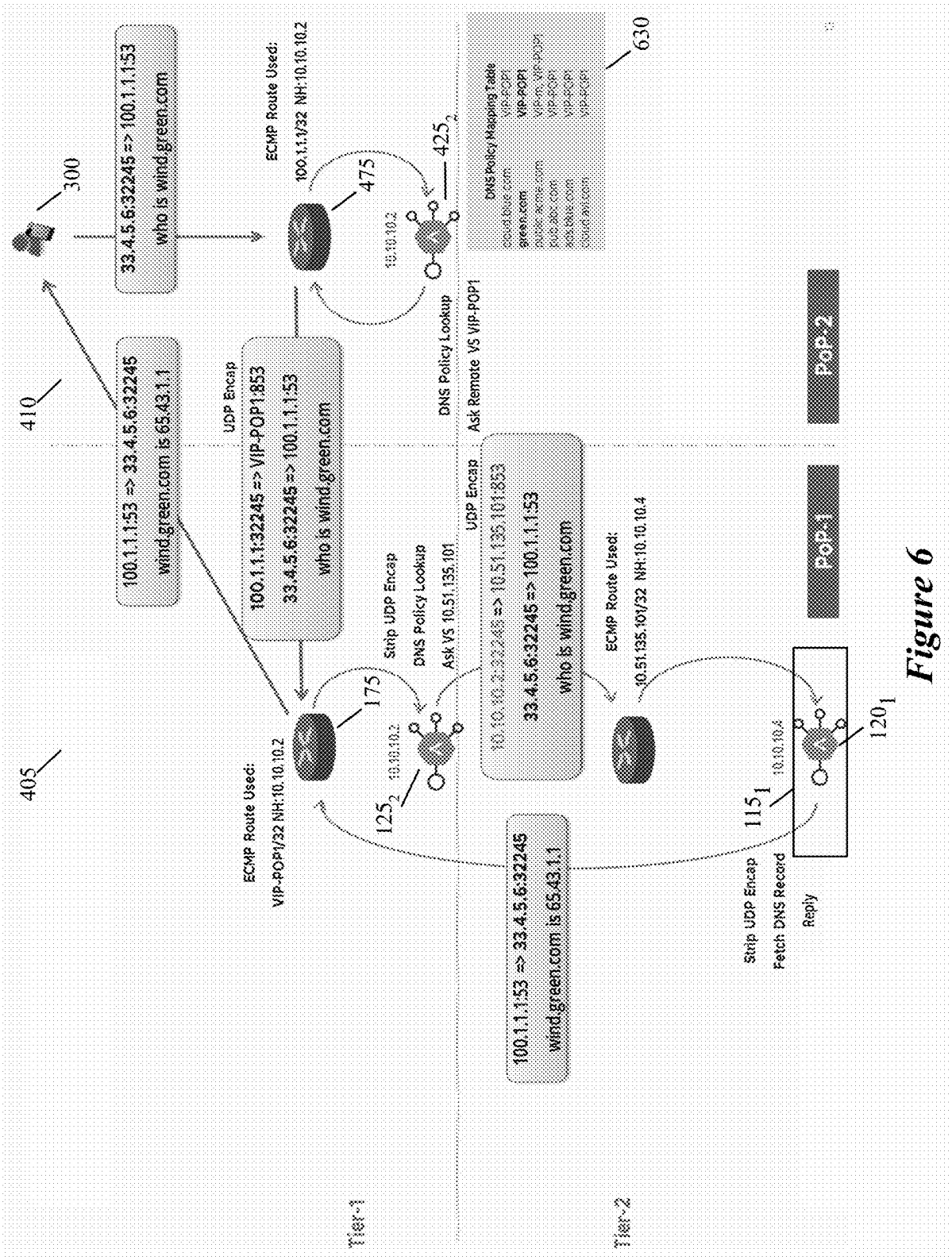

405
410
300
100.1.1.153 => 33.4.5.6:32245
wind.green.com is 65.43.1.1
33.4.5.6:32245 => 100.1.1.153
who is wind.green.com
ECMP Route Used:
100.1.1.1/32 NH:10.10.10.2
475
425$_2$
10.10.10.2
DNS Policy Lookup
Ask Remote VS VIP-POP1
DNS Policy Mapping Table
630
UDP Encap
100.1.1.1:32245 => VIP-POP1:853
33.4.5.6:32245 => 100.1.1.153
who is wind.green.com
Strip UDP Encap
DNS Policy Lookup
Ask VS 10.51.135.101
175
125$_2$
10.10.10.2
ECMP Route Used:
VIP-POP1/32 NH:10.10.10.2
UDP Encap
10.10.10.2:32245 => 10.51.135.101:853
33.4.5.6:32245 => 100.1.1.153
who is wind.green.com
ECMP Route Used:
10.51.135.101/32 NH:10.10.10.4
POP-1
POP-2
100.1.1.153 => 33.4.5.6:32245
wind.green.com is 65.43.1.1
Strip UDP Encap
Fetch DNS Record
Reply
115$_1$
10.10.10.4
120$_1$
Tier-1
Tier-2

Figure 6

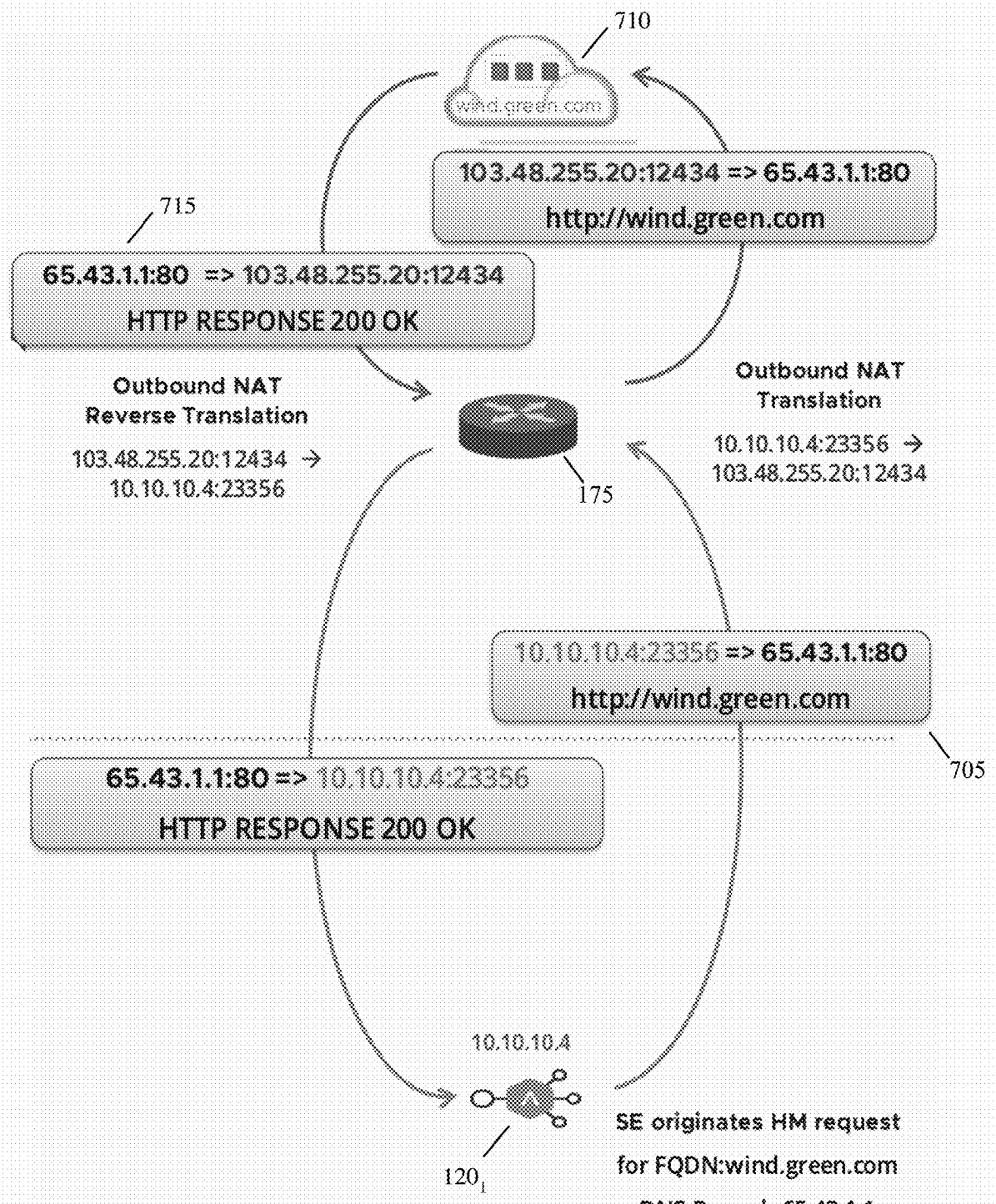

710
wind.green.com
103.48.255.20:12434 => 65.43.1.1:80
http://wind.green.com
715
65.43.1.1:80 => 103.48.255.20:12434
HTTP RESPONSE 200 OK
Outbound NAT
Reverse Translation
103.48.255.20:12434 →
10.10.10.4:23356
Outbound NAT
Translation
10.10.10.4:23356 →
103.48.255.20:12434
175
10.10.10.4:23356 => 65.43.1.1:80
http://wind.green.com
705
65.43.1.1:80 => 10.10.10.4:23356
HTTP RESPONSE 200 OK
10.10.10.4
120i
SE originates HM request
for FQDN:wind.green.com
DNS Record: 65.43.1.1

Figure 7

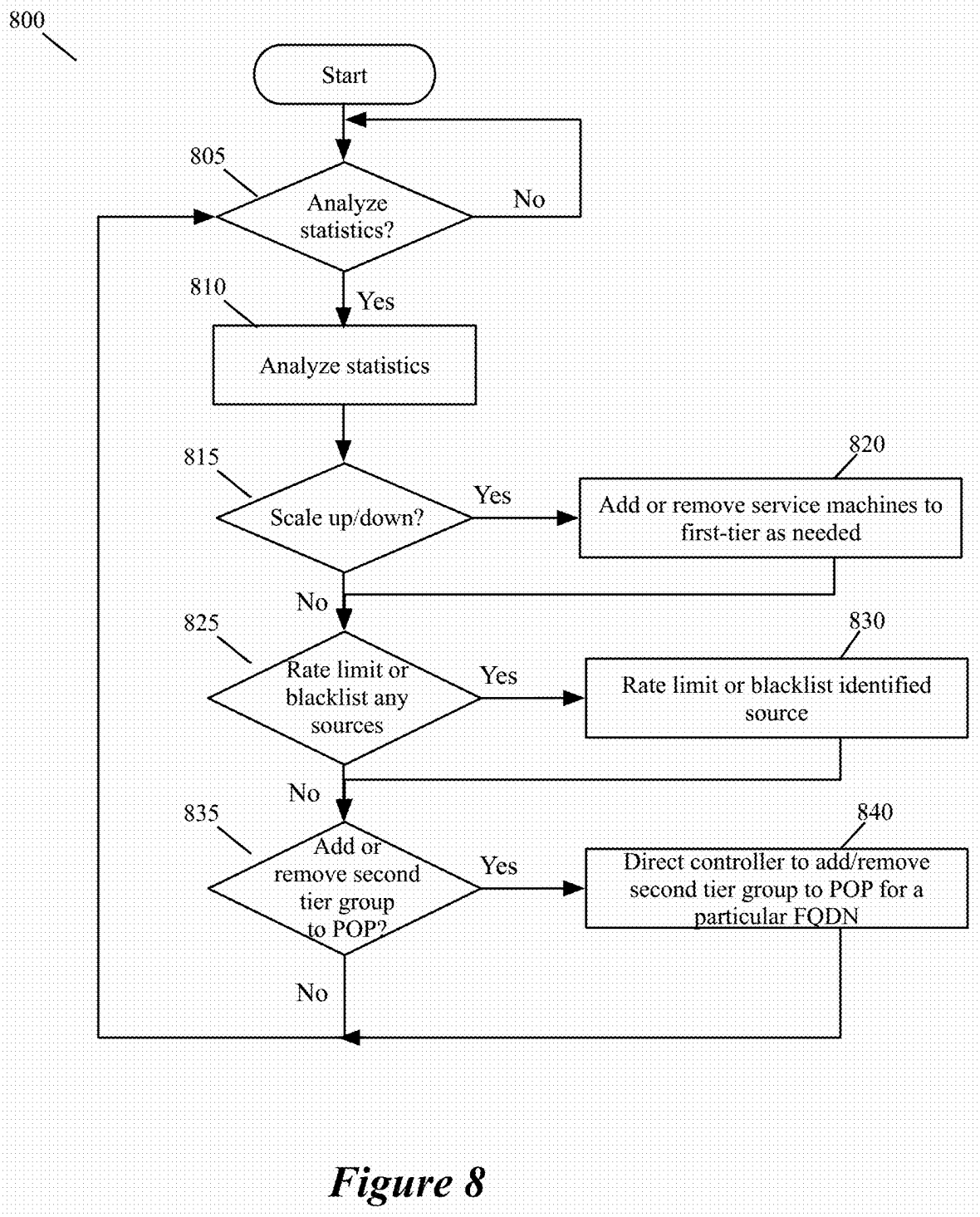

800
Start
805
Analyze statistics?
No
Yes
810
Analyze statistics
815
Scale up/down?
Yes
820
Add or remove service machines to first-tier as needed
No
825
Rate limit or blacklist any sources
Yes
830
Rate limit or blacklist identified source
No
835
Add or remove second tier group to POP?
Yes
840
Direct controller to add/remove second tier group to POP for a particular FQDN
No

Figure 8

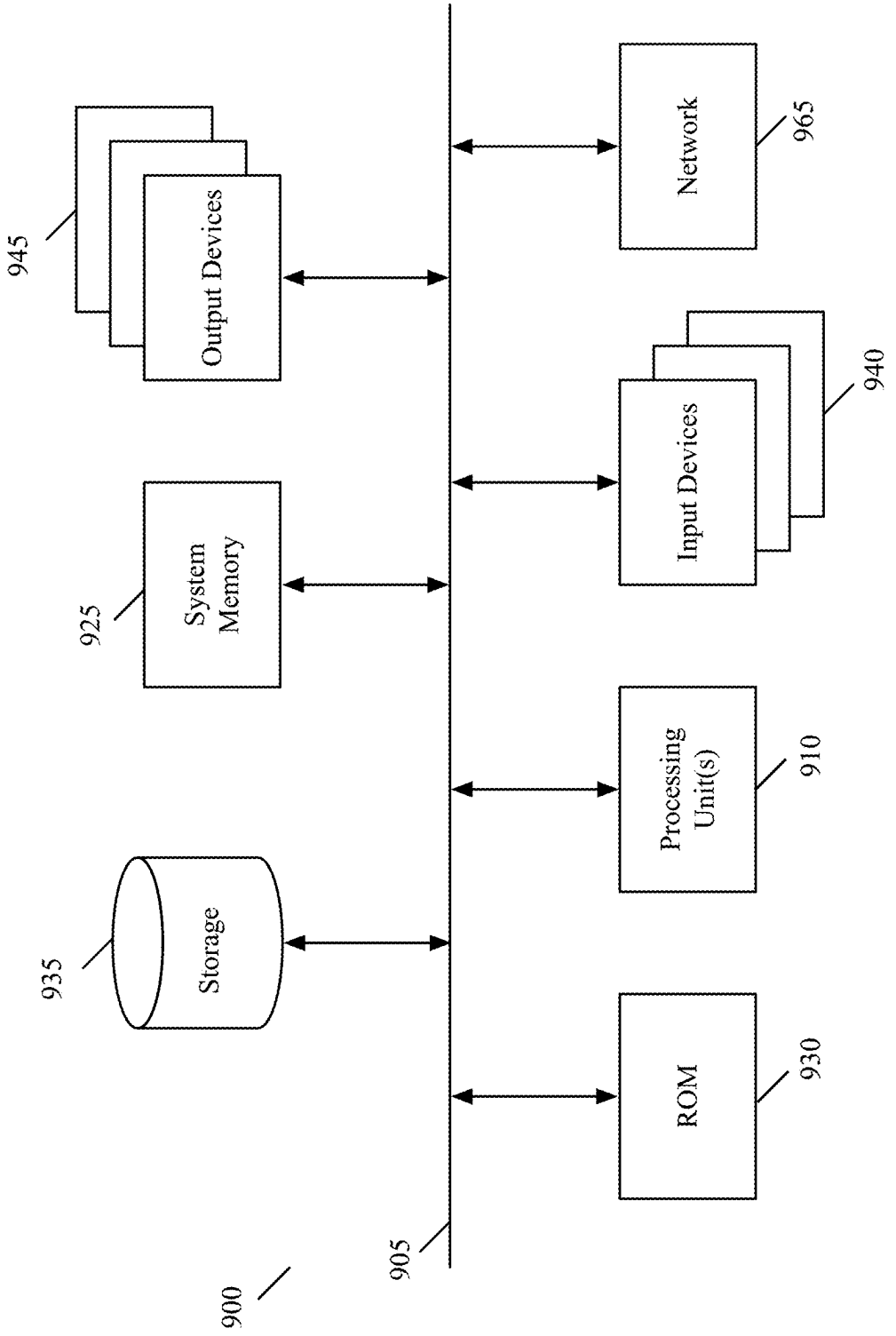

900
905
Bus
935
Storage
925
System Memory
945
Output Devices
930
ROM
910
Processing Unit(s)
940
Input Devices
965
Network

Figure 9

TWO TIER DNS

CLAIM OF BENEFIT TO PRIOR APPLICATION

[0001] The present application is a continuation application of U.S. application Ser. No. 18/211,553 filed Jun. 19, 2023, and published on Jan. 18, 2024, under Publication No. 2024-0022539. U.S. application Ser. No. 18/211,553 claims the benefit of Indian Patent Application number 202241040390, filed Jul. 14, 2022. These applications are incorporated herein by reference their entireties for all purposes.

BACKGROUND

[0002] Domain Name System (DNS) service is commonly used today to identify IP addresses associated with domain names. A typical approach to providing DNS service is to distribute all records to all DNS servers, making each server consume a lot of computation and memory resources. Some also provide different DNS service end points (public IP address or DNS names) for the name server records. Existing solutions also typically provide one IP address for the DNS server, and then provide more IP addresses when it is necessary to scale up the DNS service.

BRIEF SUMMARY

[0003] Some embodiments provide a two-tier DNS (Domain Name System) service for processing DNS requests. In some embodiments, the two-tier DNS service deploys first and second tiers of service machines, with the second-tier having several groups of service machines each of which is configured to resolve DNS requests for a different set of domain names than the other second-tier group(s). Each service machine in the first-tier is configured to identify the second-tier group responsible for each particular DNS request that the service machine receives for each particular domain name, and to forward the particular DNS request to the second-tier group that it identifies for the particular DNS request. The first-tier DNS service in some embodiments has only one group of service machines.

[0004] Each first or second service machine group in some embodiments can have one or more service machines, and can be scaled up or down to add or remove service machines to the group (e.g., through an active/active layer 3 scaleout with BGP). In some embodiments, two different second-tier service groups can process DNS requests for two or more different FQDNs (fully qualified domain names) that are part of the same domain, and/or for two or more different FQDNs that are part of different domains. Also, in some embodiments, one second-tier service group can be dedicated to one FQDN.

[0005] Each second-tier group in some embodiments processes DNS requests for a different subset of domain names. As such, each second-tier group serves as a smaller failure domain for only the subset of domain names that it processes. Each second-tier group provides a virtual DNS service that processes the DNS requests for a subset of domain names, and that is addressable through a different virtual IP (Internet Protocol) address than the virtual IP (VIP) address of other second-tier groups. In some embodiments, the first-tier service machines forward each particular DNS request to the identified second-tier group by addressing the particular DNS request to a particular VIP address of the identified second-tier group.

[0006] Also, in some embodiments, each DNS request is received at each first-tier service machine addressed to a first VIP address of the first-tier group that is different than the VIP addresses used by the second-tier groups. The first VIP address in some embodiments is an anycast VIP address, which is an IP address used by several different groups of first-tier service machines in several different geographic sites (e.g., several different buildings, cities, counties, states, countries, etc.). These different geographic sites are referred to below as Points of Presence (POPs), with each POP being one geographic site and having one group of first-tier service machines and one or more groups of second-tier service machines. The POPs are part of one wide-area network (WAN) in some embodiments.

[0007] In some embodiments, the POPs have gateway routers that advertise the anycast VIP address of the first-tier groups to external routers of external network(s) (e.g., to the Internet). Each external router outside of the POP networks (e.g., outside of the POP LANs or POP WAN) forwards each DNS request that it receives to a first-tier group of one of the POPs. For instance, for each DNS request, each external router in some embodiments identifies a next-hop interface that is associated with a first-tier group of one of the POPS, and forwards the DNS request to the identified interface so that it can eventually be forwarded to the associated first-tier group. When an external router uses a BGP routing protocol, the next-hop interface is the interface associated with the "closest" first-tier group (e.g., the first-tier group within the fewest hops to the external router).

[0008] The VIP address of each second-tier group in some embodiments is a private VIP address defined within the internal network of each POP (e.g., within the LAN of each POP or within the POP WAN). This private VIP address is not directly accessible to external machines operating in networks outside of POP network(s) (e.g., POP LANs or WAN). This is in contrast to the first VIP address of the first-tier service machines, which is a public VIP address directly accessible to external machines.

[0009] In some embodiments, the set of one or more gateway routers of each POP is configured to select, for each DNS request that is addressed to the first VIP address, a first-tier service machine of the POP and to forward the DNS request to the selected first-tier service machine. In some embodiments, the gateway router set is configured to perform ECMP to select the first-tier service machine for each DNS request. A POP's gateway router set in other embodiments is configured to distribute the DNS requests among its POP's first-tier service machines through other weighted or unweighted load balancing scheme.

[0010] The preceding Summary is intended to serve as a brief introduction to some embodiments of the invention. It is not meant to be an introduction or overview of all inventive subject matter disclosed in this document. The Detailed Description that follows and the Drawings that are referred to in the Detailed Description will further describe the embodiments described in the Summary as well as other embodiments. Accordingly, to understand all the embodiments described by this document, a full review of the Summary, Detailed Description, the Drawings and the Claims is needed. Moreover, the claimed subject matters are not to be limited by the illustrative details in the Summary, Detailed Description, and Drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The novel features of the invention are set forth in the appended claims. However, for purposes of explanation, several embodiments of the invention are set forth in the following figures.

[0012] FIG. **1** conceptually illustrates an example of a two-tier DNS service of some embodiments.

[0013] FIG. **2** conceptually illustrates a process that the different components of the two-tier DNS service in FIG. **1** perform to process a DNS request that is sent as a UDP packet.

[0014] FIG. **3** conceptually illustrates an example of the processing of a DNS request.

[0015] FIG. **4** conceptually illustrates a multi-POP DNS service with two POPs.

[0016] FIG. **5** conceptually illustrates a process that the components of a multi-POP DNS service perform to process a DNS request that is sent as a UDP packet.

[0017] FIG. **6** illustrates an example of the multi-POP DNS service processing of a DNS request.

[0018] FIG. **7** conceptually illustrates the gateway of the DNS service in FIG. **1** performing an SNAT operation on a health monitoring message sent from the second-tier service machine to the server associated with the FQDN.

[0019] FIG. **8** conceptually illustrates a process that is performed at a POP to scale up or down a first-tier security group of the POP based on statistics collected by the first-tier security group.

[0020] FIG. **9** conceptually illustrates a computer system with which some embodiments of the invention are implemented.

DETAILED DESCRIPTION

[0021] In the following detailed description of the invention, numerous details, examples, and embodiments of the invention are set forth and described. However, it will be clear and apparent to one skilled in the art that the invention is not limited to the embodiments set forth and that the invention may be practiced without some of the specific details and examples discussed.

[0022] Some embodiments provide a two-tier DNS (Domain Name System) service for processing DNS requests. FIG. **1** illustrates an example of a two-tier DNS service **100** of some embodiments. As shown, the DNS service **100** has first and second tiers **105** and **110** of service machines. The service machines in some embodiments can be standalone computers or appliances, and/or other types of machines (such as virtual machines (VMs), Pods, containers, etc.) executing on host computers.

[0023] The second-tier **110** has several groups **115** of service machines **120** with each group **115** configured to resolve DNS requests for a different set of FQDNs than the other second-tier group **115**. In this example, the second-tier group $\mathbf{115}_1$ responds to DNS requests for cloud.blue.com, green.com and public.acme.com, the second-tier group $\mathbf{115}_2$ responds to DNS requests for pub.abc.com and ads.blue.com, and the second-tier group $\mathbf{115}_n$ responds to DNS requests for cloud.avi.com.

[0024] In some embodiments, two second-tier service groups can process DNS requests for two or more FQDNs (fully qualified domain names) that are part of the same domain, and/or for two or more FQDNs that are part of different domains. For example, the second-tier group $\mathbf{115}_1$ resolves DNS requests for cloud.blue.com, while the second-tier group $\mathbf{115}_2$ resolves DNS requests for ads.blue.com. Also, in some embodiments, one second-tier service group (e.g., second-tier group $\mathbf{115}_n$) can be dedicated to one FQDN (e.g., cloud.avi.com).

[0025] In the first-tier **105**, each service machine **125** is configured to identify the second-tier group **115** responsible for each particular DNS request that the service machine **125** receives for each particular domain name, and to forward the particular DNS request to the second-tier group **115** that it identifies for the particular DNS request. To identify the second-tier group responsible for each DNS request, the first-tier service machines in some embodiments use identical policy mapping tables **130** that associate different FQDNs with VIP addresses associated with different second-tier groups, as further described below. The first-tier DNS service **105** in some embodiments has only one group **150** of service machines. In some embodiments, each first or second service machine group can have one or more service machines, and can be scaled up or down to add or remove service machines to the group (e.g., through an active/active layer 3 scaleout with BGP).

[0026] Given that each second-tier group in some embodiments processes DNS requests for a different subset of domain names, each second-tier group serves as a smaller failure domain for only the subset of domain names that it processes. Each second-tier service machine group provides a virtual DNS service that processes the DNS requests for a subset of domain names, and that is addressable through a different VIP address than the VIP address of other second-tier service machine groups.

[0027] In the example illustrated in FIG. **1**, the three second-tier groups $\mathbf{115}_1$, $\mathbf{115}_2$, and $\mathbf{115}_n$ have VIP address VIP-**1**, VIP-**2** and VIP-n. As shown by the policy mapping tables **130**, the FQDNs cloud.blue.com, green.com and public.acme.com are associated with the VIP-**1** address of the second-tier group $\mathbf{115}_1$, the FQDNs pub.abc.com and ads.blue.com are associated with VIP-**2** address of the second-tier group $\mathbf{115}_2$, and the FQDN cloud.avi.com is associated with VIP-n address of the second-tier group $\mathbf{115}_n$.

[0028] For a DNS request that it receives, each first-tier service machine **125** in some embodiments uses its policy mapping table **130** to perform a policy-based L3 and DNS lookup to identify the VIP address associated with the FQDN that is the subject of the received DNS request. The first-tier service machine **125** then forwards the DNS request to the identified VIP address (e.g., by addressing the particular DNS request to this VIP), which belongs to the second-tier service machine group that processes DNS requests for the FQDN.

[0029] In some embodiments, an intervening set of one or more forwarding elements (not shown) between the first and second tiers **105** and **110** forward the DNS request to one of the second-tier service machines of the second-tier group associated with the identified VIP address. These forwarding elements are different in different embodiments. For instance, as further described below, the intervening set of forwarding elements are routers in some embodiments that perform ECMP, or another weighted or unweighted distribution scheme, to select, for each DNS request, a next hop interface associated with one service machine from the second-tier group associated with the identified VIP address.

[0030] The intervening forwarding elements in other embodiments are load balancers. When processing each

DNS request that it receives, each such load balancer receives the DNS request addressed to a particular second-tier DNS group. The load balancer then selects (based on a set of load balancing criteria) one DNS server in the particular second-tier DNS group to process the DNS request, and then changes the destination IP address in this request from the VIP address of the particular second-tier group to individual IP addresses of the DNS server that the load balancer selected for this request. Still other embodiments forward the DNS requests from the first-tier DNS group to the second-tier DNS groups differently. For instance, in some embodiments, for each DNS request, each first-tier service machine selects the service machines (in the second-tier group that the first-tier service machine identifies for the DNS request) that should process the DNS request, and uses another forwarding scheme (e.g., L2 tunneling) to forward the DNS request to the selected service machine.

[0031] In some embodiments, each DNS request is received at each first-tier service machine addressed to a VIP address of the first-tier group that is different than the VIP addresses used by the second-tier groups. In FIG. **1**, the VIP address of the first-tier service group is 100.1.1.1, which is an IP address that is advertised to external network(s) (e.g., Internet) by a gateway router **175** of the two-tier DNS service **100**. This VIP address (100.1.1.1) is different than the second-tier group VIP addresses (e.g., VIP-**1**, VIP-**2** and VIP-n addresses), which are private VIP addresses that are directly addressable to the second-tier groups from external machines in the external network.

[0032] This is in contrast to the VIP address of the first-tier service machines, which is a public VIP address directly addressable by the external machines. As further described below by reference to FIG. **4**, the first-tier group's VIP address in some embodiments is an anycast VIP address that is used by multiple first-tier groups of multiple different sites that provide the two-tier DNS service.

[0033] FIG. **2** illustrates a process **200** that the different components of the two-tier DNS service **100** perform to process a DNS request that is sent as a UDP packet. This process will be described by reference to FIG. **3**, which illustrates an example of the processing of a DNS request. As shown, the process **200** starts (at **205**) when the gateway router **175** of the DNS service **100** receives a DNS request as a UDP packet. This packet has a destination IP address that is the VIP address of the first-tier service machine group **150**. In some embodiments, a client sends the DNS request for an FQDN via a DNS resolver, and the DNS authority for this is the Tier-1 anycast address.

[0034] FIG. **3** illustrates the gateway router **175** receiving a DNS request with a source IP address 33.4.5.6 and a destination IP address 100.1.1.1. The source IP address is the IP address of a client machine **300** that sent the DNS request, while the destination IP address is the anycast VIP address of the first-tier service machine group **150**. In this example, the DNS request is for the FQDN wind.green.com. This DNS request is sent from the client machine **300** through external routers to the gateway router **175** of the two-tier DNS **100**.

[0035] After receiving this request, the gateway router **175** selects (at **210**) a service machine **125** of the first-tier group **150** to process this DNS request. In some embodiments, the gateway router **175** performs an ECMP operation to select this service machine. This operation in some embodiments selects the router's next-hop interface that is associated with one first-tier service machine from several next-hop interfaces that are associated with the several service machines of the first-tier group **150**, and passes the DNS request along this next-hop interface. FIG. **3** shows the gateway router **175** passing the DNS request to the selected service machine $\mathbf{125}_2$ along its next-hop interface associated with the internal IP address 10.10.10.2 of this service machine.

[0036] At **215**, the selected first-tier service machine (e.g., the service machine $\mathbf{125}_2$ in FIG. **3**) then performs an L3 and DNS policy-based lookup for the FQDN in the DNS request (e.g., for wind.green.com) in its policy mapping table **130**. This lookup identifies the VIP address of the second-tier service group that should process the DNS request. In FIG. **3**, the identified second-tier service group is the second-tier service group $\mathbf{115}_1$ as it handles all the DNS requests for the domain green.com.

[0037] The selected first-tier service machine adds (at **220**) a UDP encapsulating header, which has a destination IP address of the identified second-tier service group. In some embodiments, this encapsulating header also has the VIP address of the first-tier service group as its source IP address. This header also stores the IP address of the source client machine as additional data that the DNS resolving second-tier machine can use to send the DNS reply directly back to the client machine.

[0038] FIG. **3** illustrates the first-tier machine $\mathbf{125}_2$ (1) adding a new UDP encapsulating header to the DNS request, (2) changing the destination IP address from 10.10.10.2 to the VIP address 10.51.135.101 of the second-tier service group $\mathbf{115}_1$ identified at **215**, and (3) changing the source IP address to 10.1.1.1 from the IP address 33.4.5.6 of the client machine **300**. The IP address 33.4.5.6 is stored in the UDP encapsulating header.

[0039] Next, an intervening router between the first and second-tiers directs (at **225**) the newly encapsulated DNS request to one service machine in the second-tier service group $\mathbf{115}_1$ identified at **215**. In some embodiments, this intervening router performs an ECMP operation to select this service machine. This operation in some embodiments selects the router's next-hop interface that is associated with a service machine of the identified second-tier group, from several next-hop interfaces that are associated with the service machines of the identified second-tier service group, and passes the DNS request along this next-hop interface.

[0040] FIG. **3** shows the intervening router **375** passing the DNS request with its new UDP encapsulated header to the service machine $\mathbf{120}_1$ along its next-hop interface associated with the internal IP address 10.10.10.4 of the service machine $\mathbf{120}_1$ of the identified second-tier service group $\mathbf{115}_1$. As shown, the intervening router **375** performs an ECMP operation to select the service machine in the identified second-tier service group $\mathbf{115}_1$. In some embodiments, the intervening router **375** is the gateway router **175** as this router handles both north-south traffic and east-west traffic for the two-tier DNS service. In other embodiments, the intervening router **375** is a different router of the two-tier DNS service **100** than the gateway router **175**.

[0041] As mentioned above, other embodiments use other schemes for forwarding the DNS requests from the first-tier DNS group to the DNS servers of the second-tier DNS groups. For instance, when the intervening forwarding elements are load balancers, each load balancer selects (based on a set of load balancing criteria) one DNS server in the particular second-tier DNS group to process each DNS

request that it receives, and then changes the destination IP address in this request from the VIP address of the particular second-tier group to individual IP addresses of the DNS server that the load balancer selected for this request.

[0042] At **230**, the selected second-tier service machine strips the encapsulating UDP header and resolves the DNS request. This resolution entails selecting one IP address associated the FQDN that is subject of the DNS request, from one or more available IP addresses that are associated with this FQDN. In FIG. **3**, the second-tier machine $\mathbf{120}_1$ produces the IP address 65.43.1.1 as the IP address that corresponds to the FQDN wind.green.com.

[0043] From the encapsulating UDP header, the selected second-tier service machine identifies the IP address of the client machine that is the source of the original UDP packet that contained the DNS request. Hence, at **235**, the selected second-tier service machine formulates a DNS reply (containing the IP address produced from the DNS resolution), and specifies the client machine's IP address as a destination IP address and the first-tier service group's VIP as the source IP address of the DNS reply. FIG. **3** shows the service machine $\mathbf{120}_1$ sending the DNS reply to the IP address 33.4.5.6 from the VIP 10.1.1.1 along the same ports (32245 and 53) that were used by the DNS request. It also shows the gateway router **175** passing this DNS reply to the source client machine **300** through intervening external routers (not shown). After **235**, the process then ends.

[0044] In some embodiments, the two-tier DNS service **100** handles DNS requests that are sent as TCP packets slightly differently. For instance, in some embodiments, the second-tier service machine that resolves the DNS request does not send the DNS reply directly to the source client machine. Instead, in these embodiments, it sends the DNS reply to the first-tier service machine that forwarded the DNS request to its second-tier service group, and this first-tier service machine sends the DNS reply back to the source client machine.

[0045] FIG. **3** illustrates that the VIP address of the first-tier service group in some embodiments is an anycast VIP address, 100.1.1.1 that for a DNS request is accessible through port 53. An anycast VIP address is an IP address used by several different groups of first-tier service machines in several different geographic sites (e.g., several different buildings, cities, counties, states, countries, etc.). These sites are referred to below as Points of Presence (POPs), with each POP having one group of first-tier service machines and one or more groups of second-tier service machines. The POPs are part of one wide-area network (WAN) in some embodiments.

[0046] Instead of using UDP encapsulation, other embodiments use other encapsulation techniques to forward DNS requests from the first-tier DNS group to selected second-tier DNS groups. For instance, a first-tier DNS server in some embodiments uses an IP-on-IP encapsulation that encapsulates a DNS request's original IP header with another IP header that stores the VIP address of the second-tier DNS group that the first-tier DNS server identifies for processing the DNS request. Under this approach, the original source and destination IP addresses in the original IP header are left unchanged by the first-tier DNS server, so that the second-tier DNS server that eventually processes the DNS request can use the original source and destination IP addresses when formulating the DNS reply for direct forwarding to the client machine that was the original source of the DNS request.

[0047] FIG. **4** illustrates a multi-POP DNS service **400** with two POPs **405** and **410**. These two POPs implement a common two-tier DNS service that has one first-tier service group **150** or **450** in each POP and one or more second-tier service groups **115** or **415** in each POP. These two POPs are in two geographic sites (e.g., two different cities, states, countries, or continents) but their first-tier service groups **150** and **450** are accessible through the same anycast VIP address 100.1.1.1. In addition, each POP's first-tier service group has a POP-specific public IP that is used by the first-tier service group of the other POP to send DNS requests that are not processed by the other POP's first-tier service group. In this case, the first-tier service group **150** of POP **405** has a VIP-POP**1** while the first-tier service group **450** of the second POP **410** has a VIP-POP**2**.

[0048] Also, in this example, the POP **405** has the three second-tier service groups **115** that processed DNS requests for the FQDNs discussed above, while the POP **410** has one second-tier service group **415** that processes DNS requests for public.acme.com. As mentioned above, second-tier service group $\mathbf{115}_1$ also processes DNS requests for public.acme.com. When the POP **410** receives a DNS request for public.acme.com, the first-tier service group **450** of this POP can decide to have its second-tier service group **450** processes this DNS request, or it can re-direct this request to the POP **405**.

[0049] In some embodiments, the first-tier service group of each POP is biased towards using its own second-tier service group for an FQDN that is also handled by other second-tier service group(s) in other POP(s). However, in some cases, the first-tier service group of a POP might re-direct a DNS request that its second-tier service group can process to another POP when the first-tier service group detects a condition that merits such a re-direct (e.g., too much load on its own second-tier service group).

[0050] The first-tier service group **450** of the POP **410** also re-directs DNS requests to the POP **405** when the DNS requests are for FQDNs that are not serviced by the second POP's second-tier service group **415**. In this example, these are all DNS requests for cloud.blue.com, green.com, pub.abc.com, ads.blue.com and cloud.avi.com. To identify the second-tier VIPs responsible for the FQDNs associated with each DNS request, each first-tier service group of each POP uses similar policy mapping tables **130** that may only differ in the VIP addresses of FQDNs that are handled by multiple POPs. When a POP processes DNS requests for an FQDN along with one or more other POPs, the policy-mapping table **130** or **630** of the POP stores the VIP address of its second-tier service group (if any) that processes the FQDN DNS queries, along with the VIP address of the first-tier service group (if any) of each other POP that processes DNS queriers for the same FQDN.

[0051] In FIG. **4**, this means that for public.acme.com (1) the policy-mapping table **130** of the first POP **405** stores VIP-**1** of second-tier service group $\mathbf{115}_1$ of the first POP, and VIP-POP**2** of the first-tier service group **450** of the second POP, and (2) the policy-mapping table **630** of the second POP **410** stores VIP-m of second-tier service group **415** of the second POP, and VIP-POP**1** of the first-tier service group **150** of the first POP. For the rest of the FQDNs, the policy mapping table **630** of FIG. **6** stores the VIP-POP**1** address

that is associated with the first-tier service group **150** of the POP **405**. This is because these rest of the FQDNs are processed by the second-tier service groups of the POP **405**.

[0052] Even though the POPs share the same policy mapping tables and the same second-tier service groups, each POP maintains its own metrics and logs for each DNS service offered by each second-tier service group. In some embodiments, each POP periodically distributes its metrics and logs to other POPs, while in other embodiments the POPs do not distribute their metrics and logs to other POPs. Each POP uses its metrics and logs to assess when it needs to scale up or down the service machines in its first-tier service group or one of its second-tier service group.

[0053] In some embodiments, the gateway routers of the POPS advertise (e.g., through BGP) the anycast VIP address to the external routers of the external network(s) (e.g., to the Internet). Also, in some embodiments, the POP-private VIP addresses of each second-tier group is advertised to other routers that are in the same POP as the second-tier service group.

[0054] Each external router outside of the POP networks (e.g., outside of the POP LANs or POP WAN) forwards each DNS request that it receives to a first-tier group of one of the POPs. For instance, for each DNS request, each external router in some embodiments identifies a next-hop interface that is associated with a first-tier group of one of the POPS, and forwards the DNS request to the identified interface so that it can eventually reach the associated first-tier group. When an external router uses a BGP routing protocol, the next-hop interface is the interface associated with the "closest" first-tier group (e.g., the first-tier group within the fewest hops to the external router).

[0055] To re-direct a DNS request from a first POP (e.g., **410**) to a second POP (e.g., **405**), the first-tier service group of the first POP (**410**) encapsulates the DNS request with a new UDP encapsulating header. This header has the POP-to-POP VIP address of the second POP (e.g., **405**) as a destination IP address, and the anycast VIP as a source IP address. In some embodiments, this encapsulating header also stores the IP address of the source client machine as additional data that the DNS resolving second-tier machine of the second POP (e.g., **405**) can use to send the DNS reply directly back to the client machine.

[0056] The first-tier service groups of the POPs do not use anycast VIP for the DNS requests that they re-direct to the first-tier service groups of other POPs for several reasons. First, using the encapsulating UDP headers instead of anycast VIP ensures that the re-directed DNS requests are not sent back to the re-directing first-tier service groups. Second, the encapsulating UDP headers allow the first-tier service groups that receive the re-directed DNS requests to detect that the DNS requests have been re-directed to them from other first-tier service groups, and account for this in performing their second-tier service group selection and in their metric data collection.

[0057] FIG. **5** illustrates a process **500** that the components of a multi-POP DNS service (e.g., DNS service **400**) perform to process a DNS request that is sent as a UDP packet. This process **500** is identical to the process **200** of FIG. **2**, except that it has three extra operations **505-515**. The process **500** will be described by reference to FIG. **6**, which illustrates an example of the multi-POP DNS service **400** processing of a DNS request. As shown, the process **500** starts when a gateway router of one of the POPS receives (at **205**) a DNS request as a UDP packet. This packet has the DNS service's anycast VIP as its destination IP address.

[0058] FIG. **6** illustrates the gateway router **475** receiving a DNS request with a source IP address 33.4.5.6 and a destination IP address 100.1.1.1. The source IP address is the IP address of a client machine **300** that sent the DNS request, while the destination IP address is the anycast VIP address of the first-tier DNS service **105** (used by the first-tier groups **150** and **450**). In this example, the DNS request is again for the FQDN wind.green.com, and is sent from the client machine **300** through external routers to the gateway router **475** of the two-tier DNS **400**.

[0059] After receiving this request, the gateway router **475** selects (at **210**) a service machine **425** of the first-tier group **450** to process this DNS request. In some embodiments, the gateway router **475** performs an ECMP operation to select this service machine. This operation in some embodiments selects the router's next-hop interface that is associated with one first-tier service machine from several next-hop interfaces that are associated with the several service machines of the first-tier group **450**, and passes the DNS request along this next-hop interface. FIG. **6** shows the gateway router **475** passing the DNS request to the selected service machine $\mathbf{425}_2$ along its next-hop interface associated with the internal IP address 10.10.10.2 of this service machine.

[0060] Next, at **505**, the process **500** has the selected first-tier service machine perform an L3 policy-based lookup for the FQDN that is subject of the DNS request. The first-tier service machine performs this lookup using its policy mapping table that maps FQDNs to VIP addresses of second-tier service groups within the same POP and/or VIP address(es) of first-tier service group(s) in other POP(s). In FIG. **6**, the policy mapping table **630** stores for green.com the VIP-POP**1** address of POP**1** that is associated with the first-tier service group **150** of POP **405**.

[0061] A lookup at **505** can identify a VIP address of a local second-tier service group that can resolve the DNS request (i.e., for the FQDN that is subject of the DNS request), and/or one or more VIP addresses of one or more remote first-tier service groups of other POPs. Hence, the first-tier service machine that performed the lookup determines (at **510**) whether the DNS request should be locally processed by a second-tier service group of the same POP.

[0062] When the first-tier service machine's lookup identifies just a VIP address of a local second-tier service group, the process **500** performs the operations **220-235**, which were described above for FIG. **2**. On the other hand, when the lookup just identifies one or more VIP addresses of one or more remote first-tier service groups of other POPs, the first-tier service machine has to select the first-tier service group of another POP, and forward the DNS request to this other POP.

[0063] Also, when the lookup identifies a VIP address of a local second-tier service group and one or more VIP addresses of one or more remote first-tier service groups of other POPs, the first-tier service machine has to determine whether to process the DNS request locally or remotely. As mentioned above, the first-tier service group of any POP is biased towards using its own POP's second-tier service group for a DNS request that can be processed locally or remotely, but does overcome this biasing when it detects certain conditions, such as failure of or too much load on its own second-tier service group.

[0064] To forward a DNS request to the first-tier service group of another POP, the first-tier service machine adds (at **515**) a UDP encapsulating header, which has the VIP address of the first-tier service group of the other POP as a destination IP address, and the anycast VIP as a source IP address. In some embodiments, this encapsulating header also stores the IP address of the source client machine as additional data that the DNS resolving second-tier machine of the other POP can use to send the DNS reply directly back to the client machine.

[0065] FIG. **6** illustrates the first-tier machine $\mathbf{425}_2$ (1) adding a new UDP encapsulating header to the DNS request, (2) changing the destination IP address from 10.10.10.2 to the VIP-POP**1** address of the first-tier service group **150** of the POP **405**, (3) changing the source IP address to the anycast VIP 10.1.1.1, and (4) storing the IP address 33.4.5.6 of the client machine **300** as additional data in the UDP encapsulating header.

[0066] At POP **405**, the gateway router **175** receives the encapsulated UDP packet, selects (e.g., through an ECMP operation or other weighted or unweighted distribution operation) a service machine $\mathbf{125}_2$ of the first-tier group **150** to process this DNS request, and then forwards the received UDP packet to the selected first-tier service machine (e.g., along its next-hop interface associated with the selected first-tier service machine). The first-tier service machine $\mathbf{125}_2$ removes the encapsulating UDP header and performs an L3 policy-based lookup for the FQDN wind.green.com in its policy mapping table **130**, and identifies the VIP address of the second-tier service group $\mathbf{115}_1$ that should process the DNS request.

[0067] The first-tier machine $\mathbf{125}_2$ then (1) adds a new UDP encapsulating header to the DNS request, (2) changes the destination IP address from 10.10.10.2 to the VIP address 10.51.135.101 of the second-tier service group $\mathbf{115}_1$, (3) changes the source IP address to 10.1.1.1, and (4) stores the source client machine's IP address 33.4.5.6 in the UDP encapsulating header. Next, an intervening router between the first and second tiers identifies (e.g., through ECMP or other distribution scheme) one service machine $\mathbf{120}_1$ in the second-tier service group $\mathbf{115}_1$ to receive the UDP encapsulated DNS request, and directs this request to this service machine $\mathbf{125}_2$ by passing the DNS request packet along its next-hop interface associated with the internal IP address 10.10.10.4 of the service machine $\mathbf{120}_1$ of the identified second-tier service group $\mathbf{115}_1$.

[0068] The selected second-tier service machine then receives the DNS request, strips the encapsulating UDP header and resolves the DNS request. This resolution entails selecting one IP address associated the FQDN that is the subject of the DNS request, from one or more available IP addresses that are associated with this FQDN. In FIG. **6**, the second-tier machine $\mathbf{120}_1$ produces the IP address 65.43.1.1 as the IP address that corresponds to the FQDN wind.green.com.

[0069] From the encapsulating UDP header, the selected second-tier service machine identifies the IP address of the client machine that is the source of the original UDP packet that contained the DNS request. Hence, the selected second-tier service machine $\mathbf{120}_1$ formulates a DNS reply (containing the IP address produced from the DNS resolution), and specifies the source client machine's IP address as a destination IP address and the first-tier service group's VIP as the source IP address of the DNS reply. The gateway router **175** then passes this DNS reply to the source client machine **300** through intervening external routers (not shown).

[0070] As mentioned above, other embodiments use other encapsulation techniques to forward DNS requests from the first-tier DNS group to selected second-tier DNS groups instead of using UDP encapsulation. For instance, as mentioned above, a first-tier DNS server in some embodiments uses an IP-on-IP encapsulation that encapsulates a DNS request's original IP header with another IP header that stores the VIP address of the second-tier DNS group that the first-tier DNS server identifies for processing the DNS request. Under this approach, the original source and destination IP addresses in the original IP header are left unchanged by the first-tier DNS server, so that the second-tier DNS server that eventually processes the DNS request can use the original source and destination IP addresses when formulating the DNS reply for direct forwarding to the client machine that was the original source of the DNS request.

[0071] In some embodiments, the second-tier service machines perform health-monitoring operations to ensure that the servers that service the FQDNs are operating at an acceptable operational level. As mentioned above, one FQDN can be directed to multiple servers that execute programs that are accessible to client machines through the FQDN. In such cases, the service machines of a second-tier service group can resolve the DNS request for the FQDN to the IP address of any one of these servers. To ensure that all the server machines are operating at an acceptable operational level, the second-tier service machines perform health-monitoring operations for all the servers that are associated with the same FQDN.

[0072] Given that the second-tier service machines have an internal VIP address within the two-tier DNS service, the two-tier DNS service in some embodiments has to perform SNAT (source network address translation) on health monitoring messages that the second-tier service machines send to the external servers that are associated with the FQDNs, and DNAT (destination NAT) on replies that the external servers send back to the second-tier service machine in response to the health monitoring messages.

[0073] FIG. **7** illustrates one such approach for performing these NAT operations. Specifically, this figure shows the gateway **175** of the DNS service **100** performing an SNAT operation on a health monitoring message **705** sent from the second-tier service machine $\mathbf{120}_1$ to the server **710** associated with the wind.green.com FQDN. This SNAT operation changes the source IP address from the internal IP address of the second-tier service machine $\mathbf{120}_1$ to the public unicast VIP address of the POP of the second-tier service machine. The port addresses are also translated as shown.

[0074] FIG. **7** shows the server **710** receiving the health monitoring message after it has been network address translated, and sending back a reply message **715** with a destination IP address set to the POP's public VIP address. It further shows the gateway **175** performing a DNAT operation that changes this destination IP address to the internal IP destination address of the second-tier service machine $\mathbf{120}_1$. The health monitoring reply message has a time value (**200**) for the http response, which can be used as a metric value to gauge the health of the server **710**.

[0075] The two-tier DNS service of some embodiments has several security and scaling advantages. It has superior security advantages as the first-tier security group in a POP

shields the second-tier security groups in the same POP or other POPs from external attacks, such as spurious DNS requests that are part of distributed denial of service (DDOS) attacks. Based on statistics collected by each POP's first-tier security group, each first-tier security group can scale up with additional service machines to handle the extra load from DDOS attacks, and it can rate limit DNS requests from source IP addresses that are sending too many DNS requests. Also, some embodiments use a common control plane that orchestrates Tier-1 and Tier-2 DNS services. Through this control plane, DDOS prevention policies can be pro-actively placed on other Tier-1s and Tier-2s, based on threat intelligence from one Tier-1 or Tier-2.

[0076] Based on these statistics, first-tier security group(s) can also be configured to reject or rate-limit DNS requests that emanate from known malicious source IP addresses. The first-tier security groups of each POP essentially shields the second-tier service machines of its POP and other POPs from undue load of malicious DNS attacks. In some embodiments, the statistics collected by a first-tier security group of a first POP regarding DNS requests that are re-directed to other first-tier security group(s) of other POP(s) are also analyzed to assess whether a second-tier security group should be added to the first POP.

[0077] FIG. **8** conceptually illustrates a process **800** that is performed at a POP to scale up or down a first-tier security group of the POP based on statistics collected by the first-tier security group. In some embodiments, this process is performed by one or more processes of a controller operating at the POP. In other embodiments, this process is performed by the first-tier security group service machines of the POP as part of one or more other processes. In still other embodiments, some parts of the process **800** are performed by the first-tier security group service machines, while other parts are performed by the controller operating at the POP.

[0078] At **805**, the process determines whether statistics collected by the first-tier security group of the POP have to be analyzed. This determination ensures that the process **800** is periodically performed in some embodiments. Also, this determination is implemented in terms of a timer that expires and is re-set periodically. The process **800** remains at **805** until it determines that the statistics collected by the first-tier service group has to be analyzed, and which time, it analyzes (at **810**) the statistics collected by the different service machines in the first-tier service group.

[0079] Based on this analysis, the process then determines (at **815**) whether it should add or remove service machines to the first-tier service group. The process in some embodiments adds service machines when the load on existing machines in the first-tier service group exceeds a first threshold value for a duration of time, while it removes service machines when the load on the existing machines in the first-tier service group falls below a second threshold for a duration of time.

[0080] The ability to add service machines to the first-tier service group allows the two-tier DNS service of some embodiments to dynamically grow the first-tier to address additional legitimate or malicious load on the first-tier. Example of malicious load are spurious DNS requests from a DDOS attack. Also, dynamically removing a service machine from the first-tier service group allows the two-tier DNS service to reduce the amount of resource consumed by the first-tier when the legitimate or malicious load on the first-tier subsides.

[0081] When the process determines (at **815**) that it should not add or remove service machines to the first-tier service group, it transitions to **825**. On the other hand, when the process determines (at **815**) that it should add or remove service machines to the first-tier service group, the process (at **820**) adds or removes a service machine to or from the first-tier service group, and then transitions to **825**. After adding or removing service machines from the first-tier service group, the gateway routers are configured (e.g., through BGP or through a control plane) to update next-hop forwarding records to account for the added or removed service machines.

[0082] Based on the analysis of the collected statistics, the process determines (at **825**) whether it should rate limit or blacklist any source IP addresses that are used to send DNS requests. In some embodiments, these are source IP addresses that are sending more than a threshold number of DNS requests and/or that in conjunction with other source IP addresses are sending more than a threshold amount of DNS requests for a particular set of one or more FQDNs. The rate-limited or blacklisted IP addresses are also the IP addresses identified by third-party services as common sources (e.g., as BOTs) of non-legitimate DNS requests.

[0083] When the process determines (at **815**) that it should not rate limit or blacklist any source IP addresses that are used to send DNS requests, it transitions to **835**. On the other hand, when the process determines (at **825**) that it should rate limit or blacklist any source IP addresses that are used to send DNS requests, the process (at **830**) rate limits or blacklists any source IP addresses that are used to send DNS requests, and then transitions to **835**. Rate limiting in some embodiments involves only queuing the DNS requests that come from a particular source and only processing these DNS requests at a particular lower rate. This queuing might result in some of the DNS requests being dropped in some embodiments. Also, blacklisting source IP addresses in some embodiments entails generating firewall rules for a firewall of the gateway router or other firewall to enforce, in order to ensure that DNS requests coming from a blacklisted source IP address is dropped before reaching the first-tier service group.

[0084] Based on the analysis of the collected statistics, the process determines (at **835**) whether it should add one or more second-tier service group for one or more FQDNs that currently do not have their DNS requests processed locally. In some embodiments, the process determines that such a second-tier service group should be added when the statistics indicate that more than a threshold value of DNS requests are being received at the local first-tier service group of the POP for an FQDN and these requests are being re-directed to other POP(s) as no local second-tier service group processes the DNS requests for the FQDN.

[0085] The process **800** also determines (at **835**) whether it should remove one or more second-tier service group for one or more FQDNs that currently have their DNS requests processed locally. In some embodiments, the process determines that such a second-tier service group should be removed when the statistics indicate the POP currently is not received a sufficient number of DNS requests for an FQDN that is being processed by a local second-tier service group.

[0086] When the process determines (at **835**) that it should not add or remove a second-tier service group for one or more FQDNs to the POP, the process returns to **805**. On the other hand, when the process determines (at **835**) that it

should add or remove a second-tier service group, it adds or removes (at **840**) the second-tier service group to the POP, and then returns to **805**. After adding or removing service machines from the second-tier service group, one or more internal routers of the POP are configured (e.g., through BGP or through a control plane) to update next-hop forwarding records to account for the added or removed service machines.

[0087] In addition to performing the process **800** of FIG. **8**, some embodiments also perform scale-up/down operations for each second-tier security group at each POP. In some embodiments, this operation is performed by the controller cluster (not shown) at each POP. For this scale up/down operation, the controller cluster at each POP collects and analyzes statistics from the DNS servers (e.g., service machines) of each second-tier security group. Based on this analysis, the controller cluster adds additional DNS servers to each second-tier security group when the group's DNS servers are overloaded, and removes DNS from to each second-tier security group when the group's DNS servers are under utilized.

[0088] Many of the above-described features and applications are implemented as software processes that are specified as a set of instructions recorded on a computer readable storage medium (also referred to as computer readable medium). When these instructions are executed by one or more processing unit(s) (e.g., one or more processors, cores of processors, or other processing units), they cause the processing unit(s) to perform the actions indicated in the instructions. Examples of computer readable media include, but are not limited to, CD-ROMs, flash drives, RAM chips, hard drives, EPROMs, etc. The computer readable media does not include carrier waves and electronic signals passing wirelessly or over wired connections.

[0089] In this specification, the term "software" is meant to include firmware residing in read-only memory or applications stored in magnetic storage, which can be read into memory for processing by a processor. Also, in some embodiments, multiple software inventions can be implemented as sub-parts of a larger program while remaining distinct software inventions. In some embodiments, multiple software inventions can also be implemented as separate programs. Finally, any combination of separate programs that together implement a software invention described here is within the scope of the invention. In some embodiments, the software programs, when installed to operate on one or more electronic systems, define one or more specific machine implementations that execute and perform the operations of the software programs.

[0090] FIG. **9** conceptually illustrates a computer system **900** with which some embodiments of the invention are implemented. The computer system **900** can be used to implement any of the above-described computers and servers. As such, it can be used to execute any of the above described processes. This computer system includes various types of non-transitory machine readable media and interfaces for various other types of machine readable media. Computer system **900** includes a bus **905**, processing unit(s) **910**, a system memory **925**, a read-only memory **930**, a permanent storage device **935**, input devices **940**, and output devices **945**.

[0091] The bus **905** collectively represents all system, peripheral, and chipset buses that communicatively connect the numerous internal devices of the computer system **900**. For instance, the bus **905** communicatively connects the processing unit(s) **910** with the read-only memory **930**, the system memory **925**, and the permanent storage device **935**.

[0092] From these various memory units, the processing unit(s) **910** retrieve instructions to execute and data to process in order to execute the processes of the invention. The processing unit(s) may be a single processor or a multi-core processor in different embodiments. The read-only-memory (ROM) **930** stores static data and instructions that are needed by the processing unit(s) **910** and other modules of the computer system. The permanent storage device **935**, on the other hand, is a read-and-write memory device. This device is a non-volatile memory unit that stores instructions and data even when the computer system **900** is off. Some embodiments of the invention use a mass-storage device (such as a magnetic or optical disk and its corresponding disk drive) as the permanent storage device **935**.

[0093] Other embodiments use a removable storage device (such as a flash drive, etc.) as the permanent storage device. Like the permanent storage device **935**, the system memory **925** is a read-and-write memory device. However, unlike storage device **935**, the system memory is a volatile read-and-write memory, such a random access memory. The system memory stores some of the instructions and data that the processor needs at runtime. In some embodiments, the invention's processes are stored in the system memory **925**, the permanent storage device **935**, and/or the read-only memory **930**. From these various memory units, the processing unit(s) **910** retrieve instructions to execute and data to process in order to execute the processes of some embodiments.

[0094] The bus **905** also connects to the input and output devices **940** and **945**. The input devices enable the user to communicate information and select commands to the computer system. The input devices **940** include alphanumeric keyboards and pointing devices (also called "cursor control devices"). The output devices **945** display images generated by the computer system. The output devices include printers and display devices, such as cathode ray tubes (CRT) or liquid crystal displays (LCD). Some embodiments include devices such as a touchscreen that function as both input and output devices.

[0095] Finally, as shown in FIG. **9**, bus **905** also couples computer system **900** to a network **965** through a network adapter (not shown). In this manner, the computer can be a part of a network of computers (such as a local area network ("LAN"), a wide area network ("WAN"), or an Intranet, or a network of networks, such as the Internet. Any or all components of computer system **900** may be used in conjunction with the invention.

[0096] Some embodiments include electronic components, such as microprocessors, storage and memory that store computer program instructions in a machine-readable or computer-readable medium (alternatively referred to as computer-readable storage media, machine-readable media, or machine-readable storage media). Some examples of such computer-readable media include RAM, ROM, read-only compact discs (CD-ROM), recordable compact discs (CD-R), rewritable compact discs (CD-RW), read-only digital versatile discs (e.g., DVD-ROM, dual-layer DVD-ROM), a variety of recordable/rewritable DVDs (e.g., DVD-RAM, DVD-RW, DVD+RW, etc.), flash memory (e.g., SD cards, mini-SD cards, micro-SD cards, etc.), magnetic and/or solid state hard drives, read-only and recordable Blu-Ray® discs,

ultra-density optical discs, and any other optical or magnetic media. The computer-readable media may store a computer program that is executable by at least one processing unit and includes sets of instructions for performing various operations. Examples of computer programs or computer code include machine code, such as is produced by a compiler, and files including higher-level code that are executed by a computer, an electronic component, or a microprocessor using an interpreter.

[0097] While the above discussion primarily refers to microprocessor or multi-core processors that execute software, some embodiments are performed by one or more integrated circuits, such as application specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs). In some embodiments, such integrated circuits execute instructions that are stored on the circuit itself.

[0098] As used in this specification, the terms "computer", "server", "processor", and "memory" all refer to electronic or other technological devices. These terms exclude people or groups of people. For the purposes of the specification, the terms display or displaying means displaying on an electronic device. As used in this specification, the terms "computer readable medium," "computer readable media," and "machine readable medium" are entirely restricted to tangible, physical objects that store information in a form that is readable by a computer. These terms exclude any wireless signals, wired download signals, and any other ephemeral or transitory signals.

[0099] While the invention has been described with reference to numerous specific details, one of ordinary skill in the art will recognize that the invention can be embodied in other specific forms without departing from the spirit of the invention. Thus, one of ordinary skill in the art would understand that the invention is not to be limited by the foregoing illustrative details, but rather is to be defined by the appended claims.

1. A device comprising:
- a processor;
- a memory storing instructions that, when executed by the processor, cause the device to:
- analyze statistics related to DNS service operations;
- determine whether to scale up or down based on the analyzed statistics;
- add or remove service machines to a first-tier DNS service group based on the determination; and
- direct a controller to add or remove a second-tier DNS service group to a point of presence (POP) for a particular fully qualified domain name (FQDN).

2. The device of claim **1**, wherein the instructions further cause the device to:
- determine whether to rate limit or blacklist any sources based on the analyzed statistics; and
- rate limit or blacklist an identified source based on the determination.

3. The device of claim **1**, wherein the instructions further cause the device to:
- receive a DNS request at a gateway;
- select a service machine in the first-tier DNS service group to process the DNS request;
- perform a policy-based lookup to identify a virtual IP (VIP) address associated with the second-tier DNS service group responsible for resolving the FQDN in the DNS request; and
- encapsulate the DNS request with a new header setting a destination address to the identified VIP address.

4. The device of claim **3**, wherein the instructions further cause the device to:
- forward the encapsulated DNS request to an intervening router;
- select, by the intervening router, a service machine in the second-tier DNS service group to process the DNS request; and
- resolve the DNS request at the selected second-tier service machine.

5. The device of claim **1**, wherein the processor and the memory are connected to a bus system.

6. The device of claim **1**, further comprising a storage device connected to the bus system.

7. A method comprising:
- analyzing, by a processing unit, statistics related to DNS service operations;
- determining, by the processing unit, whether to scale up or down based on the analyzed statistics;
- adding or removing, by the processing unit, service machines to a first-tier DNS service group based on the determination; and
- directing, by the processing unit, a controller to add or remove a second-tier DNS service group to a point of presence (POP) for a particular fully qualified domain name (FQDN).

8. The method of claim **7**, further comprising:
- determining whether to rate limit or blacklist any sources based on the analyzed statistics; and
- rate limiting or blacklisting an identified source based on the determination.

9. The method of claim **7**, further comprising:
- receiving a DNS request at a gateway;
- selecting a service machine in the first-tier DNS service group to process the DNS request;
- performing a policy-based lookup to identify a virtual IP (VIP) address associated with the second-tier DNS service group responsible for resolving the FQDN in the DNS request; and
- encapsulating the DNS request with a new header setting a destination address to the identified VIP address.

10. The method of claim **9**, further comprising:
- forwarding the encapsulated DNS request to an intervening router;
- selecting, by the intervening router, a service machine in the second-tier DNS service group to process the DNS request; and
- resolving the DNS request at the selected second-tier service machine.

11. The method of claim **7**, wherein the processing unit is connected to a bus system.

12. The method of claim **11**, further comprising storing data related to the DNS service operations in a storage device connected to the bus system.

13. A system comprising:
- a bus system;
- a storage device connected to the bus system;
- a processing unit connected to the bus system, wherein the processing unit executes program instructions to:
- analyze statistics related to DNS service operations;
- determine whether to scale up or down based on the analyzed statistics;

add or remove service machines to a first-tier DNS service group based on the determination; and

direct a controller to add or remove a second-tier DNS service group to a point of presence (POP) for a particular fully qualified domain name (FQDN).

14. The system of claim **13**, wherein the processing unit further executes program instructions to:

determine whether to rate limit or blacklist any sources based on the analyzed statistics; and

rate limit or blacklist an identified source based on the determination.

15. The system of claim **13**, wherein the processing unit further executes program instructions to:

receive a DNS request at a gateway;

select a service machine in the first-tier DNS service group to process the DNS request;

perform a policy-based lookup to identify a virtual IP (VIP) address associated with the second-tier DNS service group responsible for resolving the FQDN in the DNS request; and

encapsulate the DNS request with a new header setting a destination address to the identified VIP address.

16. The system of claim **15**, wherein the processing unit further executes program instructions to:

forward the encapsulated DNS request to an intervening router;

select, by the intervening router, a service machine in the second-tier DNS service group to process the DNS request; and

resolve the DNS request at the selected second-tier service machine.

17. The system of claim **13**, further comprising a network connection for communicating with the first-tier DNS service group and the second-tier DNS service group.

18. The system of claim **13**, wherein the storage device stores policy mapping tables for the first-tier DNS service group.

19. The system of claim **13**, further comprising input devices and output devices connected to the bus system.

20. The system of claim **13**, wherein the processing unit comprises multiple processing units for parallel processing of DNS service operations.

* * * * *