Array NETWORKS
Access. Security. Performance.

Firewall Load Balancing

2009-12-11

L2 MAC SLB (FWLB)

Firewall load balance

Clients access web servers, two firewalls sit before web servers to protect them from attacks.

Two firewalls to load balance and failover purpose

TMs are used to balance network traffic between two firewalls (please notice, SLB is not performed on web servers)

Analysis

IP packets are between clients and web servers, firewalls are not the destinations of the packets

Source and destination IP addresses can't be changed in TMs so L4/L7 SLB is not applicable

L2 SLB is useful by connecting two firewalls with two different TM interfaces. Input traffic from clients are balanced across multiple output interfaces

Traffic from web servers also need to pass thru firewalls, another TM is needed for SLB between web servers and two firewalls

Clients, web servers and firewalls should have the default gateway or some static route gateway configured as one of the TMs' IP addresses so that the traffic can go through TMs.

Equipment

Clients: web clients

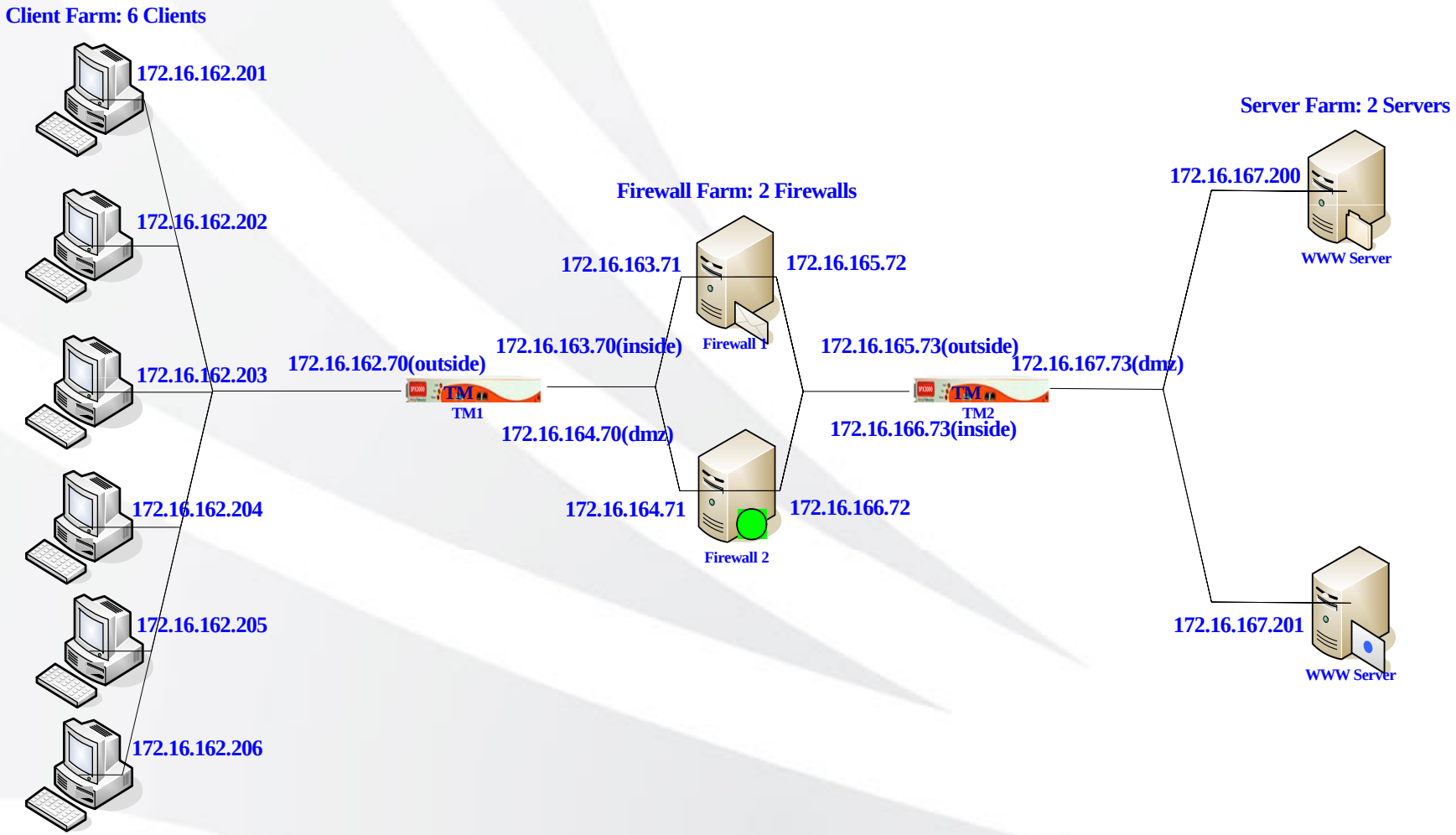
Firewall servers: L2 SLB real servers

Web servers: Destination servers

TMs: perform L2 server load balance for firewall load balance purpose

L2 MAC SLB (FWLB)

Network Topology



L2 MAC SLB (FWLB)

Configuration sample -- TM1

Define system IP addresses

AN(config)#ip address outside 172.16.162.70 255.255.255.0
AN(config)#ip address inside 172.16.163.70 255.255.255.0
AN(config)#ip address dmz 172.16.164.70 255.255.255.0

Define L2 virtual service

AN(config)#slb virtual l2ip vs1 172.16.162.70

Define L2 real services (by either real servers' IPs or MACs)

AN(config)#slb real l2ip rs1 172.163.71 3 3
AN(config)#slb real l2ip rs2 172.164.71 3 3

Or

AN(config)#slb real l2mac rs1 00:e0:81:03:36:e4 inside
AN(config)#slb real l2mac rs2 00:30:48:81:54:9c dmz

Add real service health checks (this is optional!)

AN(config)#slb real health rs1 172.16.165.73 0
AN(config)#slb real health rs2 172.16.166.73 0

Note, the above additional health checks intend to check TM2' accessibility so that the whole path is unblocked

Define SLB group and add L2 real services

AN(config)#slb group method g1 rr direct
AN(config)#slb group member g1 rs1 1
AN(config)#slb group member g1 rs2 1

Associate virtual service with the group

AN(config)#slb policy default vs1 g1

L2 MAC SLB (FWLB)

Configuration sample -- TM2

Define system IP addresses

AN(config)#ip address outside 172.16.165.73 255.255.255.0
AN(config)#ip address inside 172.16.166.73 255.255.255.0
AN(config)#ip address dmz 172.16.167.73 255.255.255.0

Define L2 virtual service

AN(config)#slb virtual l2ip vs1 172.16.167.73

Define L2 real services (by either real servers' IPs or MACs)

AN(config)#slb real l2ip rs1 172.165.72 3 3
AN(config)#slb real l2ip rs2 172.166.72 3 3

Or

AN(config)#slb real l2mac rs1 00:e0:81:03:36:e5 outside
AN(config)#slb real l2mac rs2 00:30:48:81:54:9d inside

Add real service health checks (this is optional!)

AN(config)#slb real health rs1 172.16.163.70 0
AN(config)#slb real health rs2 172.16.164.70 0
Please notice, the above additional health checks intend to check TM1' accessibility so that the whole path is unblocked

Define SLB group and add real services

AN(config)#slb group method g1 rr direct
AN(config)#slb group member g1 rs1 1
AN(config)#slb group member g1 rs2 1

Associate L2 virtual service with the group

AN(config)#slb policy default vs1 g1