accessmyLAN™

High Availability White Paper

Introduction

High Availability (HA) is an integrated feature of AccessMyLan which provides service continuity in the event of a system or network failure at the customer site. AccessMyLan HA is implemented by deploying multiple VPN Agents on the LAN and optionally configuring routing to support multiple Internet circuits. High Availability services support all access methods including VPN Client, Web Portal, ActiveSync and Mobile APN without requiring any special configuration of the client device.

Asavie Technologies Ltd.
24 Herbert Lane
Dublin 2
Ireland

w: www.accesssmylan.com
e: sales@accessmylan.com
t: +353 1 6763585 (Int)
+1 866 576 9266 (USA)
+44 158 263 5013 (UK)

VPN Agents

LAN connectivity to the AccessMyLan service cloud is provided by VPN Agent(s) running as a Windows service. Upon startup, a VPN Agent establishes an outbound SSL connection to the AccessMyLan service cloud that is mutually authenticated using digital certificates. The VPN Agent then registers with the service and informs the service of the subnets on the LAN are routable and the location of DNS services. Once a VPN Agent successfully registers with the AccessMyLan service, remote user traffic on the VPN for the subnets advertised is routed via the VPN Agent. Remote user traffic packets are multiplexed via the SSL connections to the VPN Agent which proxies the traffic to the appropriate host on the local subnets.

Deploying Multiple VPN Agents for HA

High availability is achieved by deploying more than one VPN Agent on separate Windows systems on the local network. Deploying additional VPN Agents simply involves adding the VPN Agent on the VPN Administration site and downloading and installing the VPN Agent software. By default, no configuration of the newly deployed VPN Agents is required as they automatically register routable networks and DNS services.

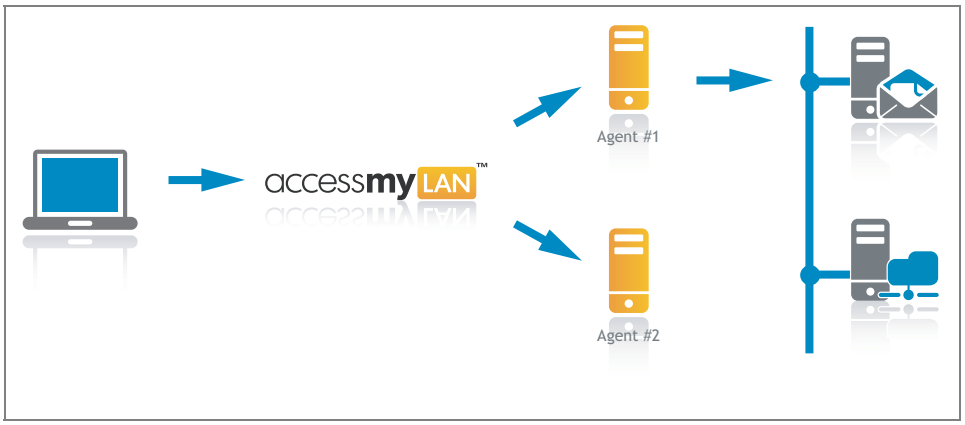

Figure 1- Traffic routing with multiple VPN Agents

When more than one VPN Agent is installed, the first VPN Agent to register with the service is the lowest-cost route to the local subnets. By default, VPN Agents that subsequently register advertise higher-cost routes to the local subnets. This default routing stance can be configured by assigning route costs to each VPN Agent and also by enabling VPN Agent access control lists (ACL) to route traffic based on protocol.

VPN Agent Failover

In a multi-agent deployment, when a VPN Agent that is actively routing traffic loses connectivity, the AccessMyLan service cloud will automatically re-route traffic to the VPN Agent that provides the lowest cost route. This failover happens transparently without remote clients having to reconnect as this re-routing happens within the AccessMyLan service cloud. VPN agents may lose connectivity due to failure of the system hosting the agent or Internet connectivity issues.

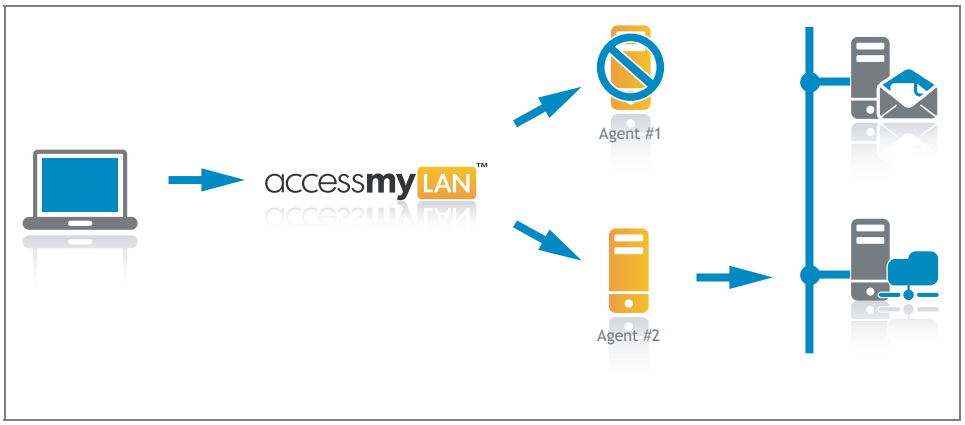

Figure 2 - Traffic Routing with failed VPN Agent

One VPN Agent licence is included in the AccessMyLan base package. Additional VPN Agents can be purchased as required. There is no practical limit to the number of VPN Agents configured on a VPN.

Internet Connectivity Failover

VPN Agents establish connectivity via the Internet to the AccessMyLan service cloud via the Internet routes defined on the host Windows system. Should connectivity to the AccessMyLan service cloud be lost, the VPN Agent will automatically attempt to re-establish connectivity through any available route.

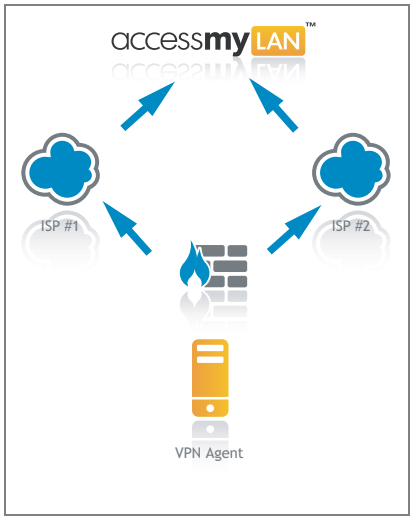

Figure 3 - Agent Connectivity using multiple Internet Routes

The capability to automatically re-establish connectivity allows the exploitation of multiple Internet circuits from different providers without having to reconfigure any clients, Internet DNS or routing.