

Introduction

Remote access plays a critical role in successfully executing a business recovery plan both in terms of providing access for existing remote users and accommodating the potential increase in demand for displaced staff. The Recovery Time Objective (RTO) for key business processes can be adversely impacted by delays in providing access to recovered applications as user devices may need to be reconfigured and name server updates are propagated across the Internet.

AccessMyLan addresses the key business recovery demands of rapid failover, end-user transparency and scalability without the cost and complexity associated with deploying duplicate equipment or enabling network resilience.

Asavie Technologies Ltd.
24 Herbert Lane
Dublin 2
Ireland

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

Service Architecture

AccessMyLan is a hosted remote access service that enables access to corporate networks from remote PCs (VPN Client), mobile phones (ActiveSync), Mobile APN and from any web browser. Remote clients connect and authenticate with the service cloud before access is granted to the corporate network. The corporate network connectivity to the service cloud is established and maintained by VPN Agents installed on the corporate network. VPN Agents (hosted on any Windows platform) establish outbound SSL connections to the AccessMyLan service cloud which are mutually authenticated using digital certificates.

This architecture removes any remote access dependency on the Internet DNS name and IP address of a site by routing remote user traffic via the SSL tunnels established by the VPN Agents.

Routing and DNS

Routing Architecture

Upon startup, VPN Agents register with the AccessMyLan service cloud and notify the service of the subnets that are reachable by the VPN Agent. The VPN Agent automatically provides VPN routes to each subnet configured on the host machine. Additional 'static' routes can be configured to provide routes to other subnets which are available via gateways on the LAN. In a multi-site scenario, each deployed VPN Agent provides routes to the site subnets as shown in Figure 1 - Multi site routing below.

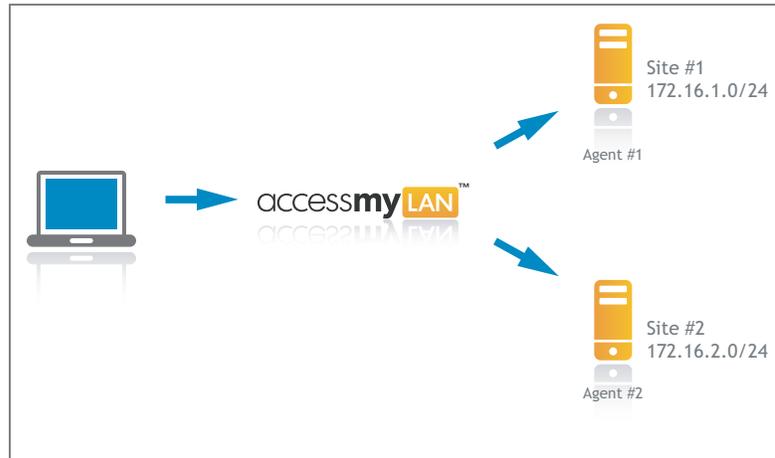


Figure 1 - Multi site routing to different address ranges

In Figure 1 - Multi site routing, VPN Agent #1 provides a route to the subnet 172.16.1.0/24 while VPN Agent #2 provides a route to 172.16.2.0/24. Remote clients have concurrent connectivity to both networks.

Where sites share the same subnet IP address ranges, traffic is routed by default to the first VPN Agent that registers with the service. In the event of the first VPN Agent losing connectivity, traffic is automatically and transparently routed to the second VPN Agent.

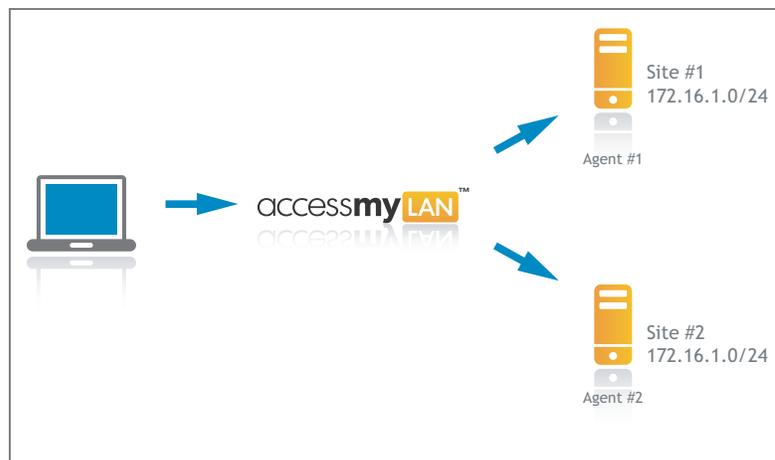


Figure 2 - Multi site routing to same address range

The default routing can be configured to assign VPN Agent specific route 'costs' creating a primary/secondary configuration. VPN Agent routing can be further

controlled via VPN Agent access control lists (ACL) which allow traffic to be routed based on the application protocol. This dynamic routing is transparent to remote clients as all traffic is routed to the service cloud which then forwards traffic via the least cost route.

DNS Integration

VPN Agents serve as DNS proxies, forwarding remote client name resolution requests to either the DNS server configured on the host or to DNS server defined by the VPN Administrator. AccessMyLan updates the client DNS settings on login to a virtual DNS server in the service cloud which forwards requests to the VPN Agent for resolution.

In a disaster recovery scenario, DNS resolution is transparent to the remote device as requests are forwarded to the virtual DNS server address in the cloud which will select the recovery site VPN Agent for DNS resolution.

Integrating a Disaster Recovery site

A recovery site is integrated with the remote access VPN by installing a VPN Agent at the recovery site. Upon installation, the recovery site VPN Agent will register with the service cloud and provide routing and DNS for the recovery site. The following examples show how remote access continuity is provided by AccessMyLan in a number of recovery scenarios.

Recovery to an Exact Mirror

In this scenario, the recovery site is an exact replica of the primary site with the same subnet IP addressing and host names configured on both sites. From an AccessMyLan VPN point of view, the service has two routes (provided by the VPN Agents) to the subnet and will route to the VPN Agent with the lowest cost. By default the lowest cost VPN Agent is the first Agent connected which may result in VPN traffic being routed to the recovery site if the recovery site VPN Agent is started before the primary site. To ensure that VPN traffic is only routed to the recovery site in the event of a disaster, the route costs for the secondary VPN Agent should be configured or alternatively the recovery VPN Agent can be stopped and started manually as part of the recovery process.

The recovery VPN Agent will proxy DNS requests to the recovery site DNS server which replicates the namespace of the primary site.

In a recovery scenario, remote access clients will not require a VPN disconnect & reconnect as routing and DNS settings will not have changed. No reconfiguration of client applications is required although individual applications may require a restart to re-establish application context with the recovery site.

Recovery to a Different Topology

Many disaster recovery sites are provided by 3rd parties where the subnets used to host recovery are not the same as the primary site. In this scenario, a VPN Agent installed at the recovery site will advertise routes to the recovery site subnet and provide DNS services from the recovery site DNS server.

In a disaster recovery scenario, remote client DNS requests are forwarded to the recovery VPN Agent for resolution by the recovery DNS server. The requests are resolved to IP addresses of the application hosts on the recovery site providing total namespace transparency for remote clients.

DNS caching on remote clients may cause application connect failures until the cached entries expire and are then resolved by the recovery DNS server. It is important that all remote application configurations use a server's DNS name rather than IP Address to ensure transparent failover to the recovery site.

Coping with increased demand

In a disaster situation, the primary physical workplace may not be available with staff being accommodated in alternative locations or working from home. With traditional VPN solutions, capacity has to be put in place to cope with the peak demand projected. With AccessMyLan, there is no limit to the number of subscribers that can be added so that there is no requirement to purchase idle capacity or pre-purchase licences. Registered subscribers can use any access method to connect to the recovery site including VPN Client, Web Portal and Mobile Phone providing the widest possible device coverage. The Web Portal provides clientless access enabling rapid rollout to the user community. The VPN Client provides a self-install process which simplifies the rollout of full network access to remote users.

Where an Internet connection at the recovery site reaches saturation, AccessMyLan provides the capability to split traffic based on protocol and/or destination host across multiple Internet circuits (which may be from different providers). This is achieved by deploying multiple VPN Agents at the recovery site on hosts configured with different Internet routes and implementing VPN Agent access control lists (ACLs) to split traffic across the VPN Agents as appropriate.