accessmyLAN™

Technical White Paper

Introduction

AccessMyLan is a hosted software-as-a-service (SaaS) remote access solution that provides a single solution for remote access via VPN clients, web browsers and mobile devices such as data cards and phones.

The service is offered on a per subscriber basis, and requires no up front investment in hardware or software. Requiring no CPE (Customer Premise Equipment), the AccessMyLan 'footprint' on the customer network consists of a software agent that makes an outbound SSL connection to the AccessMyLan service cloud which is hosted in multiple data centres around the globe. Typically, no firewall changes are required at the customer’s network perimeter and deployment in DMZ-style scenarios is fully supported.

With no open inbound ports, no published DNS and no routes, there is no attack surface at the customer’s network edge and dependency on fixed external IP's or specific ISP's is removed. Multiple agents can be deployed at a single site for resiliency. Also, multiple agents can be placed at different sites, binding multiple locations into a single network for remote users.

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)

Service Architecture

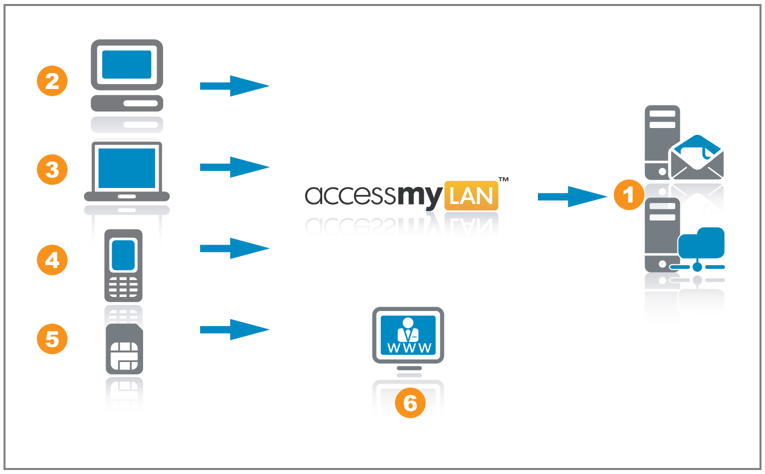


Figure 1 - Service Architecture

1 The VPN Agent installed in the LAN establishes an SSL connection to the AccessMyLan service cloud

2 The Web Portal provides web access to file shares and web based applications from any Internet Browser

3 The VPN Client provides full network connectivity to the LAN from Laptop and Desktop systems via the Internet

4 Mobile handsets access Exchange services via the ActiveSync proxy

5 The AccessMyLan APN provides network level access for Mobile handsets, laptops with mobile broadband and mobile routers

6 The service is administered via an intuitive web interface

Service Management

The service is managed via the administration web site hosted in the AccessMyLan cloud. This web site provides all the interfaces for user management, security configuration, reporting, service status and remote device deployment. Custom VPN administration roles can be defined to delegate administration tasks to persons other than the VPN administrator and access to the administration site can be restricted by IP address if so desired.

Integrated Logging and Reporting

The service provides as standard logging of all user sessions and user login attempts which can be viewed online or downloaded for further processing and analysis. The session report includes the time the user connected, when they disconnected and the amount of data uploaded and downloaded.

Detailed logging can be enabled on the VPN to provide W3C style logs of session activity. These logs provide detail on what services on the LAN the remote user connected to and are stored on the VPN Agent host.

VPN Agents

Connectivity between the customer network and the service cloud is maintained by VPN Agents. VPN Agents run as a service on any Windows platform (Windows 2000 or later) and establish a permanent SSL connection to the AccessMyLan data centre. In the event of an Internet connection failure, the VPN Agent will automatically attempt to re-establish connectivity to the data centre over any available Internet route. This capability to re-establish connectivity is totally transparent to the remote users of the service and occurs without any client logouts.

Multiple VPN Agents can be deployed to provide resilience in the event of hardware or network failure. In a default configuration, the first VPN Agent to connect provides the route for remote traffic. If the first VPN Agent loses connectivity due to hardware or network problems, the other VPN agent will immediately start providing the route for remote traffic. VPN Agents may be deployed across multiple sites to enable totally transparent failover of remote access in a disaster recovery scenario or to provide concurrent connectivity to several sites. VPN Agents provide policy based routing which can be used to split remote traffic between VPN agents based on the service type and/or destination host.

Because the VPN Agent establishes an outbound SSL session from within the LAN, it provides an easy and secure way to provide access to services and applications deep within a network behind multiple layers of firewalls. The alternative would require opening inbound ports and configuring routing on each firewall to enable traffic to pass.

VPN Client

The VPN Client provides full network connectivity to the customer LAN via the service and is currently supported on Windows 2000, XP and Vista systems. With the VPN Client installed, remote users can access all applications on the corporate network without any reconfiguration of applications on the PC. The VPN Client is an extension to the standard Microsoft IPSec/L2TP client and provides advanced authentication, routing, security, diagnostic and DNS services. The extensions added to the client also compensate for low-quality Internet connections with configurable session keep-alive and packet fragmentation settings.

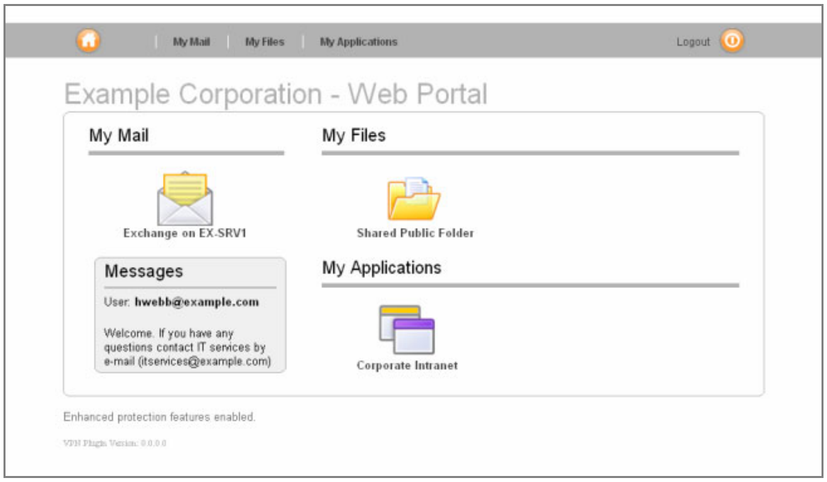
The VPN Client is installed from the web (~1.5MB download) and as part of the installation a machine digital certificate is transparently installed on the client PC. The client install can be optionally performed by the remote user via an e-mail invitation from the VPN Administrator. This simplifies the process of rolling the service out to a community of remote users.

The VPN client leverages the core of the Microsoft VPN stack and is maintained by the Windows update process. This reduces the overhead of maintaining systems in the field because no updates or security patches need to be pushed out as they would for proprietary VPN clients.

Web Portal

The Web Portal provides secure access to web applications and file shares on the LAN from any Internet browser. Using the Web Portal, access to files and applications can be easily and securely provided to non-corporate controlled devices including home PCs, business partner devices and kiosk browsers. By using the Web Portal, web and files services are not exposed to the Internet and are only accessible once users have successfully authenticated. The Web Portal uses a Verisign certificate and SSL for all communications between the client browser and the portal. Where the application supports SSL, the portal will act as an SSL bridge.

Any well formed web application is supported by the Web Portal including Outlook Web Access, Microsoft CRM, and Lotus Notes. The portal provides access to WebDAV file shares on the LAN. WebDAV is supported for file share access on Windows, Apple and Unix/Linux systems. The remote user is subject to the file-system access controls implemented by the server hosting the WebDAV share and the VPN administrator can also define any share as being read-only.



User: **hwebb@example.com**

Welcome. If you have any questions contact IT services by e-mail (itservices@example.com)

Enhanced protection features enabled.

VPN Plugin Version: 0.0.0.0

Figure 2 - Web Portal User Interface

The portal supports granular access control policies. Access to the portal can be enabled or disabled on a per user basis with the capability to further control access by each user to individual applications. Access can be further refined by specifying application URLs that are blocked from access regardless of the user settings.

Restrictions can be applied based on the characteristics of the remote system and browser. The remote browser characteristics are established by a browser plug-in which also performs session cleanup upon session termination.

Where an internal authentication server is configured on the VPN (Single Sign On is configured), credentials used to authenticate to the Web portal are passed to portal applications providing a seamless user experience.

ActiveSync

ActiveSync is a Microsoft protocol that enables synchronisation of e-mail, calendar, tasks and contacts between a handheld device and an Exchange server on the corporate network.

While ActiveSync is included as a no-charge feature on some smartphones and PDAs (e.g. Apple iPhone, Windows Mobile and Nokia S60) and in Exchange 2003 and later, there is considerable complexity associated with securely configuring an Exchange server and mobile handsets for mobility. AccessMyLan removes the complexity associated with ActiveSync deployment and provides enhanced security features as standard.

The Microsoft recommended approach includes the deployment of an ISA server to protect the Exchange infrastructure and host security processing. It is also necessary to open inbound ports on the firewall to allow access to the ISA server from the Internet. The AccessMyLan approach removes the complexity associated with deploying an ISA server, installing digital certificates and reconfiguring firewalls.

The AccessMyLan ActiveSync proxy provides the following features

- Enforcement of SSL encryption over the Internet with the remote device
- Authorisation of the remote handset based on the unique device ID and locking the handset to the user
- Supervision of ActiveSync requests to the corporate Exchange server
- Enforcement of login failure lockout policies

AccessMyLan delivers high availability as a standard feature for all types of connections including ActiveSync. High availability with ISA servers, as recommended by Microsoft, requires each ISA server to be a member of the Active Directory domain. As large organisations may have Exchange servers across multiple domains, deployment of a highly available environment would require multiple ISA server arrays. AccessMyLan decouples the firewalling and inspection function from the domain environment and can easily support multiple Exchange servers in multiple domains in a highly available configuration – a feature that is especially valuable for IT departments running multiple divisions or business units.

Mobile APN

Mobile APN (e.g. GPRS, HSDPA, 3G, UMTS) access provides a rapid and secure method of connecting any device on a mobile network to the office network without installing any client software on the mobile device. The Mobile APN provides network level access to the LAN from mobile handsets, laptops with mobile broadband and mobile routers simply by configuring an APN (Access Point Name) on the device,

Mobile APN access provides an easy method of enforcing Internet access policies on remote users by removing access to the Internet APN (enforced by the mobile network). With the Internet APN removed, Internet Access is provided via a proxy on the corporate LAN allowing corporate Internet access policies to be applied to remote devices.

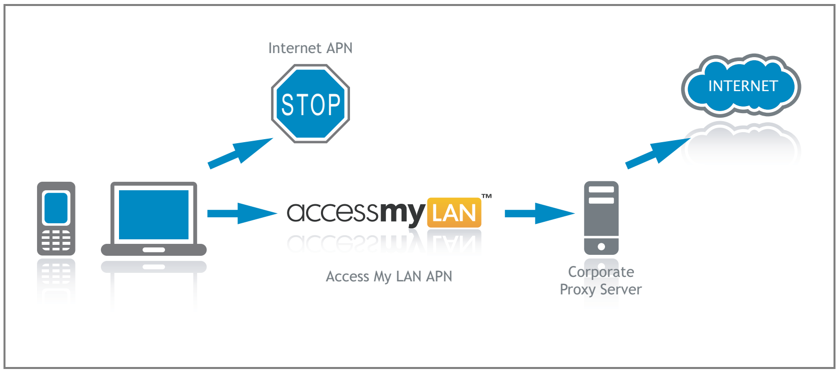


Figure 3 - Controlling Internet Access via Mobile APN services

The service can provision devices with application and APN configurations via PIN protected SMS messages minimising deployment time and eliminating manual configuration errors. Where SMS provisioning is not supported by the remote device, personalized configuration instructions are generated for the device setup.

With APN connected devices, the device SIM is used along with the user credentials for authorisation. This approach binds the device to a specific user and provides two-factor authentication for APN connected devices.

Mobile APN provides a cost effective, scalable and secure alternative to implementing a Private APN with an operator. The cost and complexity (to both operator and customer) associated with implementing a Private APN are significant especially where business critical features such as high availability are required. As an alternative, Mobile APN access provides an on-demand APN for customers of all sizes that is easily configured, does not require any CPE, is highly available and includes advanced security features. Mobile APN also provides access to a portfolio of APN's in multiple countries removing the cost and complexity of integrating with multiple mobile operators.

Network Architecture

The VPN Agent behaves like a NAT proxy and all remote user traffic on the LAN has a source address of the system hosting the VPN Agent. Upon startup, the VPN Agent automatically discovers routable subnets and DNS services which are configured at connect time on remote devices.

When a remote device authenticates successfully, the service assigns an IP address to the remote device from an AccessMyLan address pool and configures DNS and routing. The client DNS is configured to use the DNS proxy on the AccessMyLan network which forwards requests to the VPN Agent for resolution. Routes are defined on the client to route all traffic for RFC1918 addresses via the VPN. Remote user traffic is proxied by the VPN Agent so that all remote traffic on the LAN has the source IP address of the VPN Agent host. The following *tracert* example shows the routing in the network.

```
C:> tracert srv1.example.com
Tracing route to srv1.example.com [192.168.1.21] over a maximum of 30 hops

1 32 ms 31 ms 32 ms 10.128.0.1          ← Client Access Server
2 34 ms 34 ms 35 ms 10.192.0.3          ← Virtualised Customer Router/Firewall
3 66 ms 67 ms 66 ms 192.168.1.20        ← VPN Agent IP address on LAN
3 69 ms 67 ms 69 ms 192.168.1.21        ← Server address on LAN
```

Figure 4 - VPN Network Routing

Each VPN is assigned a virtualised VPN router/firewall in AccessMyLan which is responsible for enforcing customer configured VPN Access Controls and routing user traffic via connected VPN Agents.

The virtualised VPN router also provides a DNS relay by forwarding any DNS UDP datagrams addressed to the VPN router address to VPN Agents that have a DNS route declared.

Routing to Reserved and Public IP addresses

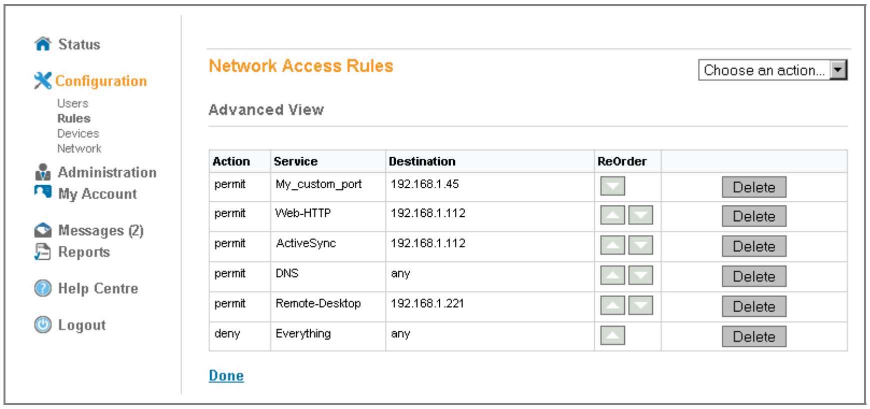
Users connected to the service can only access hosts assigned addresses in the ranges 10.0.0.0/9, 172.16.0.0/12 and 192.168.0.0/16. Where a LAN uses addresses outside these ranges, the service uses Network Address Translation (NAT) to enable remote clients to connect to the LAN.

To access addresses outside this range, each host in the LAN requires a NAT entry on the service. When a remote user issues a DNS request to resolve a hostname that is in the NAT translation table, the VPN agent automatically modifies the DNS response to use the service assigned NAT address rather than the actual public address. Using this approach, AccessMyLan can transparently support networks using public addresses internally.

Access Controls

Access Rules

Network access rules are applied to all remote traffic and control access based on the application protocol and the destination host. The VPN administrator can define custom services in addition to the standard service definitions.



Network Access Rules

Advanced View

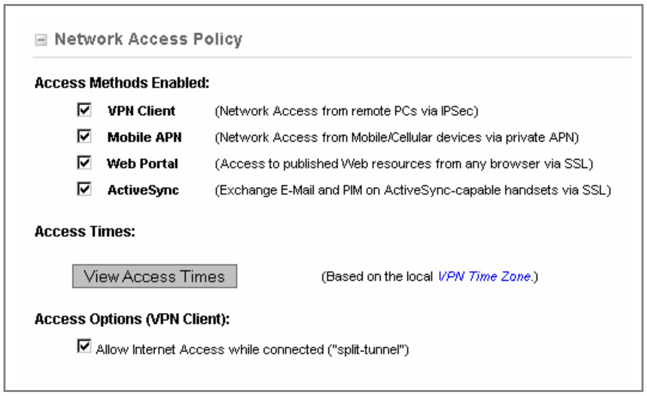
Action	Service	Destination	ReOrder	
permit	My_custom_port	192.168.1.45	▼	Delete
permit	Web-HTTP	192.168.1.112	▲ ▼	Delete
permit	ActiveSync	192.168.1.112	▲ ▼	Delete
permit	DNS	any	▲ ▼	Delete
permit	Remote-Desktop	192.168.1.221	▲ ▼	Delete
deny	Everything	any	▲	Delete

Figure 5 - Network Access Rule Configuration

User access rules are applied on a per-user basis and are defined in the same manner as network access rules.

User Network Access Policy

The user network access policy defines how a remote user can connect to the service, when they can connect and whether they can access the Internet when connected with the VPN Client (split-tunnel).



⊟ Network Access Policy

Access Methods Enabled:

☑	**VPN Client**	(Network Access from remote PCs via IPSec)
☑	**Mobile APN**	(Network Access from Mobile/Cellular devices via private APN)
☑	**Web Portal**	(Access to published Web resources from any browser via SSL)
☑	**ActiveSync**	(Exchange E-Mail and PIM on ActiveSync-capable handsets via SSL)

Access Times:

(Based on the local *VPN Time Zone*.)

Access Options (VPN Client):

☑ Allow Internet Access while connected ("split-tunnel")

Figure 6 - User Access Policy Configuration

Remote user 'Access Times' provides access control based on day of week and time of day.

End-Point Checking and Quarantine

With quarantine enabled, the service checks the characteristics of a VPN Client or Web Portal end-point and determines if full access should be granted or if the connection should be subjected to the quarantine rules. The service can check if the end-point device is a member of the domain and if the machine has a valid service certificate. This provides a consistent and easy method of controlling application access by users who use both corporate controlled and non-corporate devices to access network services.

User Authentication

By default, remote users are authenticated against the integrated AAA service. The service implements a lockout policy which defines how many login failures a user may have before being locked out. The policy also defines the lockout period before the user may attempt to login again.

User passwords are subject to a password policy which defines the minimum length and character set mix.

The service can be configured to authenticate remote users with any RADIUS capable authentication server in the LAN such as Active Directory or SecureID. Authentication requests are proxied via the VPN Agent to the internal RADIUS server defined by the VPN administrator.

Summary

AccessMyLan provides a comprehensive, secure and scalable solution for remote access that is easy to manage and deploy. Along with addressing fundamental remote access requirements the service provides many features beyond competing remote access services including;

- Single solution for VPN Clients, e-mail on handsets, Web browser clients and mobile clients
- Integrated high availability and resilience features
- No inbound ports opened on firewalls
- Service easily scales on-demand
- Reduces infrastructure complexity for Exchange push e-mail deployment
- Delivers mobile device connectivity on-demand via Mobile APN

AccessMyLan is developed and operated by Asavie Technologies Ltd. AccessMyLan and the AccessMyLan logo are registered trademarks of Asavie Technologies Limited. All other trademarks are the property of their respective owners.

Glossary

ActiveSync	A Microsoft developed protocol for synchronising mobile handsets and smartphones with Exchange Servers
APN	Access Point Name - An interconnect on a mobile network to a public network such as the Internet or a corporate LAN
CPE	Customer Premise Equipment - Hardware installed on a customer network
CSV format	A comma separated text file suitable for importing into programs such as Excel
Data Centre	General term for the the service delivery infrastructure
DMZ	Demilitarized Zone - Industry term for a secure network that exposes an organisations services to the Internet
IPSec	Industry standard for securing VPN links
L2TP	Layer 2 Tunneling Protocol - an industry standard for connecting networks usually implemented over an IPSec connection
RADIUS	Remote Authentication Dial In User Service - Industry standard protocol for authentication and authorization of users.
RFC1918	The Internet standard that defines the address ranges for use on private networks (LAN) as 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
Software-as-a-Service (SaaS)	Industry term for delivery of applications and solutions via the Internet
SSO	Single Sign On uses internal servers (e.g. Active Directory) for

remote user authentication. The user credentials used to login to the portal are used to login to portal applications removing the need for the user to authenticate using the same credentials with each application.

VPN Agent Provides connectivity between the customer LAN and the AccessMyLan data centre via SSL

W3C Format An industry standard format for logfiles

WebDAV Web Distributed Authoring and Versioning - an industry standard for accessing content (such as file shares) via HTTP

Appendix 1 – Deployment Scenarios

Remote Access & Disaster Recovery

In a disaster recovery scenario, AccessMyLan can provide rapid failover to the recovery site without any reconfiguration of the remote clients. This is achieved by deploying a VPN Agent at the recovery site and manually stopping the VPN Agent. In the event of a failover to the recovery site, the VPN Agent is manually started as part of the documented recovery process.

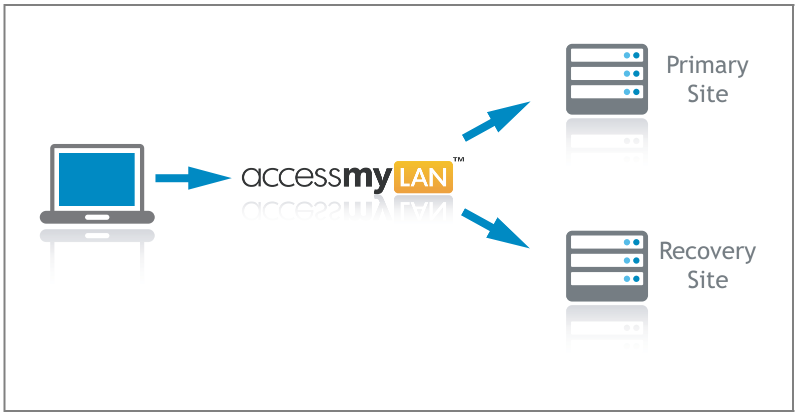


Figure 7 - Disaster Recovery Topology

Once the VPN Agent at the recovery site connects, the service will dynamically route all client traffic through the newly connected VPN Agent. Remote clients do not have to disconnect and reconnect as part of the recovery process. Multiple VPN agents can be deployed in the recovery site for resilience and/or traffic routing.

Concurrent Access to Multiple Sites

Where an organization has multiple sites, VPN Agents can be deployed at each site providing concurrent connectivity to all sites. When a VPN Agent at a site connects to the service, it provides routes to all local subnets and configured static routes. Client traffic is dynamically routed via the appropriate VPN Agent by the service transparently to the client.

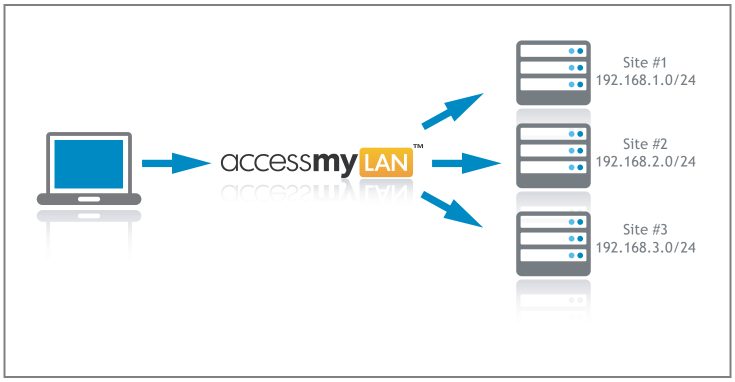


Figure 8 - Concurrent Site Access

Where sites are interconnected by WAN links, each VPN Agent can be configured with static routes to off-site subnets. The routing metric assigned to these static routes ensure that the least-cost route to a subnet is via the VPN Agent on that subnet. If a VPN Agent loses connectivity the service will dynamically re-route traffic via the remaining VPN Agents based on the route metrics. This approach keeps remote access traffic off the WAN and places it on local Internet links.