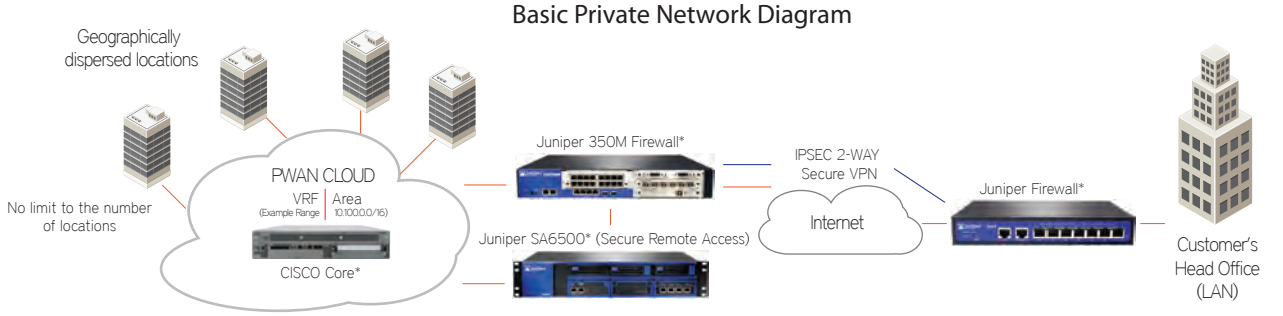
FULLY MANAGED PRIVATE NETWORKS

Basic Private Network Diagram



*example equipment

Technical Product Overview

Blaze Networks' private network is built utilising CISCO core routing equipment and Junipers cutting edge security platforms. The customers routers first authenticate to Blaze Networks radius server, then the connection is passed to the customers Virtual Routing and Forwarding (VRF) area or dedicated equipment. Each router, at each geographical dispersed location, connects in the same way, building a fully routed or 'hub and spoke' network utilizing complete private IP addressing. For example, a customer with two hundred locations is allocated an address range of 10.100.0.0/16 supporting 254 geographical locations with 250 hosts under each individual site location. Unlike traditional VPN technologies the private network does not route information over the public internet. The VRF area is given a default gateway of the enterprise Juniper Firewalls. For hardware dedicated customers, the Cisco equipment is given a default route to dedicated Juniper firewalls. The Firewall controls all internet bound communications offering the very best security approach for large infrastructures. The customer's head office is connected through the public internet over a secure IPSEC VPN tunnel, making head office services available to all geographical dispersed locations. As well as the customer's head office services being made available to the private network, cloud services like Microsoft Azure, Office 365, Google Apps and many more can be made available through firewall security policies on the customer's request. Blaze Networks' core infrastructure uses interconnects or direct peering with leading manufacturers like Microsoft offering the fastest path available to large cloud solutions, reducing the number of physical hops between the private network infrastructure and the customers cloud investment.

For a more complete technical overview, quotation or to see how the private network can be implemented for you, please arrange a meeting by contacting us or visiting our private network pages available on our web site.

What is a Private Network?
A private network is a highly secured wide area network (WAN). The private network links multiple geographically dispersed locations together with no limitations, offering rich, uninterruptable data and application availability within the private network. The private network has a maximum of two entry points into the customer's network from the public internet. These two entry points are secured by leading firewall manufacturer Juniper Networks. Customers who utilise the private network benefit by concentrating their security investment in these two areas. This reduces budget requirements and the customers PCI DSS security scope significantly. Ultimately this offers clients better security than traditional based firewall products which route across the public internet. For example, if a customer links one thousand geographically dispersed locations together with traditional VPN technology then there are one thousand entry points into the customers network from the public internet and all of these locations are in PCI DSS security scope due to this. With the private network there are only two entry points, no matter how many locations the customer brings into the private network solution.

Secure control over internet resource
Due to the private network having two secure entry points to the public internet, internet access policies to things like credit card bureaus and in-cloud services like Mirosoft Azure and Office 365 can be implemented across all locations with ease, reducing administration and PCI DSS penetration testing areas. The private Network can also utilises Blazescreen, a secure content filtering platform that implements the customers internet policies in all areas from one centralised location, again reducing administration and complexity of the network. For more information on Blazescreen please download the Blazescreen brochure or visit the web pages.

Remote access and controlled third party communications
The complication of controlling access into large network infrastructures is solved in all cases by utilising Blaze Networks remote access solution. Remote employees (sales forces, home workers) can access the network through a secure web based remote access portal that enforces the customer's access policies. Third party companies that require access to the system can also gain restricted entry as required by the customer. This type of remote access offers two phased authentication into the private network complying with PCI DSS security standards. For more information on remote access download the brochure or visit the web pages.

Covering all eventualities with a proactive support approach
Blaze Networks help desk teams actively monitor all connectivity and services on the customer's Private network 24/7. Monitoring and reporting is achieved with Ipswitch's 'What's up pro!' MSP edition. Ipswitch is the market leader in infrastructure monitoring and is the key to Blaze Networks proactive support approach. The customer is given full access to the monitoring platform offering feature rich reporting on all elements of the private network infrastructure. When issues arise alerts are automatically triggered and both the help desk team and customer are notified in real time. There is no delay in Blaze Networks help desk team actioning issues that arise offering the customer the best IT support approach available. All technical issues are entered into the help desk ticketing system that automatically notifies line managers of reoccurring issues. The customer has access to the ticketing platform so they can raise technical faults if required and report on Blaze Networks technical activity within the private network.

Tel: 0844 2477747 e-mail: sales@blazenetworks.co.uk Web: www.blazenetworks.co.uk