WHITE PAPER: OPEN.VPN CLOUD

Implementing A Secure OpenVPN Cloud Platform

White Paper: OpenVPN Cloud Platform

Implementing OpenVPN Cloud Platform

Content

OpenVPN Cloud Platform - White Paper

Introduction

The Internet is designed to facilitate point-to-point communications, typically consisting of communications between clients and servers that are either unsecured or layered on top of the Secure Sockets Layer (SSL). However, this architecture presents limitations that arise from the traditional point-to-point communication model of the Internet.

Emerging Web applications require a secure, scalable, and fault-tolerant content distribution infrastructure to fully realize the potential of advanced collaboration and media applications that combine real-time interactive media, broadcast, and secure document exchange.

In addition, the security requirements of modern enterprise applications, the increasing bandwidth needs of rich media Web applications in the enterprise, and the associated high cost and complexity of configuration management require a next-generation approach to network security and scalability that extends the traditional virtual private network (VPN) model to the next level. This level is where the virtualization of the network and its services (e.g., VMware) can be seamlessly managed. A level where dynamically scalable, and highly-available virtual private networks are easily provisioned and mapped to the public Internet.

OpenVPN Cloud is a communications platform offering from OpenVPN Technologies, Inc that rises to the challenge of providing a highly available, web-scalable network solution for a diverse application space, not only fulfilling the requirements of the traditional VPN market, but expanding those to address the demands of real-time media exchange and distribution applications.

The Problems

The Internet today is a collection of computer networks that exchange data packets using the standard Internet Protocol (IP). These data packets can travel over a variety of network and server paths on the way to their destination in a completely unsecure manner.

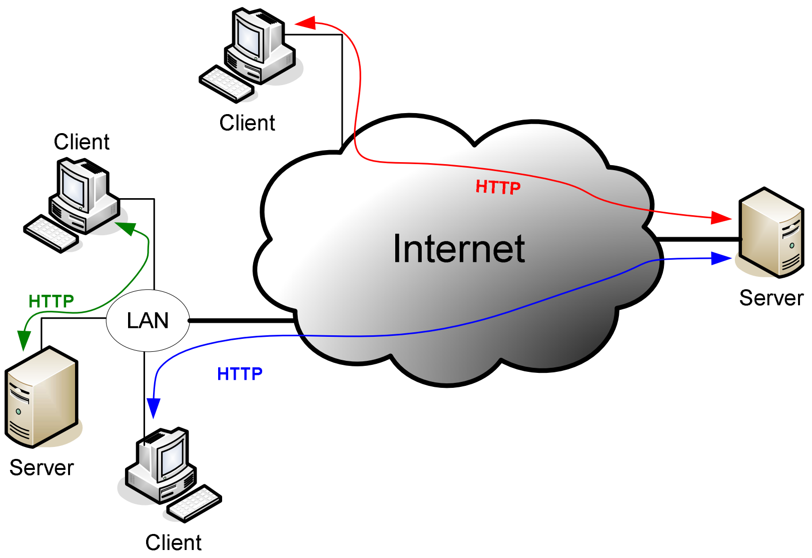

Figure 1: Traditional Internet, client-server architecture.

One solution to fixing the insecurity of the public Internet is by creating a smaller private network called a Virtual Private Network (VPN). VPNs allow connecting remote users together securely over unsecure public networks, but are very limited in the functions they can provide. They can have point-to-point connections (i.e., remote access and site-to-site access), but are inadequate when building a scalable network that requires many different types of communications in order to accommodate true virtualization.

This brings up the issue of how to securely and reliably transfer real-time media content (e.g., audio, video, Virtual Desktop) along with simple data files. There are numerous media formats and delivery methods for the various types of content available, add to this the lack of control over the paths packets take using a public network. There is no way to guarantee that every packet sent will take the exact same path; this can cause varying transmission speeds, dropped packets, and limited service support.

Overcoming some of these drawbacks can be accomplished, but it requires an in-depth knowledge of networking technologies and security techniques. This can dramatically increase the Total Cost of Ownership (TCO) and complicate management, configuration, and complexity of the network.

Limitations of today’s IP networks

Currently, IP is the main protocol of the TCP/IP suite that is used to identify the source and destination hosts for communications performed across a packet-switched network. This presents inherent vulnerabilities.

Unencrypted packet headers – Any host along the path of the communication can read the source and destination addresses within the IP header. This exposes networks to security risks such as: IP spoofing, packet sniffing, and session hijacking. Some solutions for this are to use: the IP security (IPsec) protocol, or a Secure Sockets Layer (SSL) based VPN, however, these solutions require extra effort and cost in the form of configuration, management, and maintenance.

Unreliable packet delivery – IP makes no guarantees about packet delivery. It is a connectionless protocol and therefore doesn't require any setup be performed prior to sending packets to a host, similar to the UDP protocol. There is no inherent quality of service available; data can be corrupted or packets can be lost, dropped, duplicated, or received out of order.

Limited functionality – As the Internet continues to expand at an exponential rate, there is a growing demand for real-time and reliable multicast and broadcast media content delivery. Undoubtedly, the current public network infrastructure based on legacy technologies, will be unable to keep up with mounting demand for multimedia communications. Factoring in the limited ability to control the packet path reveals the limitations of networks to provide scalable solutions that cannot be extended to work wherever and whenever situations demand. Compounding all of this, is the fact that not all routers currently in use today can support multicasting.

Limitations of traditional VPNs

VPNs can be very powerful tools in solving secure point-to-point data communications needs, but there are limitations to the capabilities they can support.

Built on an insecure public network – In order to properly ensure sufficient protection on a public network, a detailed understanding of network security issues is required. Expensive equipment is usually required and this equipment can be incompatible across different vendors.

Administrative challenges – Rolling out VPN services for many users can be very time consuming and costly. Also, after the VPN has been rolled out, there comes the management and maintenance of the client software, which can require considerable effort and cost.

Multi-point communications – Conventional VPNs allow secure remote access and site-to-site connections. However, they typically don't support multicasting or broadcasting connections which are highly dependent on the underlying network and are not within administrative control.

Limited scalability – The VPN client software by itself only connects remote users to the company's private network. It does not enable user's dynamic access to various resources and applications across the network that may be necessary. Simply stated, the current VPN solutions are not scalable.

The Solution

For those looking to employ a solution that can provide a unified and secure communication platform for many different types of services, then the OpenVPN Cloud is the optimal solution.

OpenVPN Cloud technology

OpenVPN Cloud is a web-scaling software overlay/infrastructure that extends the usefulness of the Internet by providing secure communication between hosts across the unsecure public network. This is similar to a VPN, however since OpenVPN Cloud is a unified solution, it allows application developers and service providers the ability to securely and reliably exchange data through corporate firewalls without compromising or bypassing corporate security policies.

The OpenVPN Cloud infrastructure is composed of interconnected OpenVPN servers that are hosted on clustered, redundant machines dispersed across multiple geographical locations. This makes the network resilient to the failure of individual nodes by employing a *self-healing* feature, thereby providing the highest level of uptime and availability.

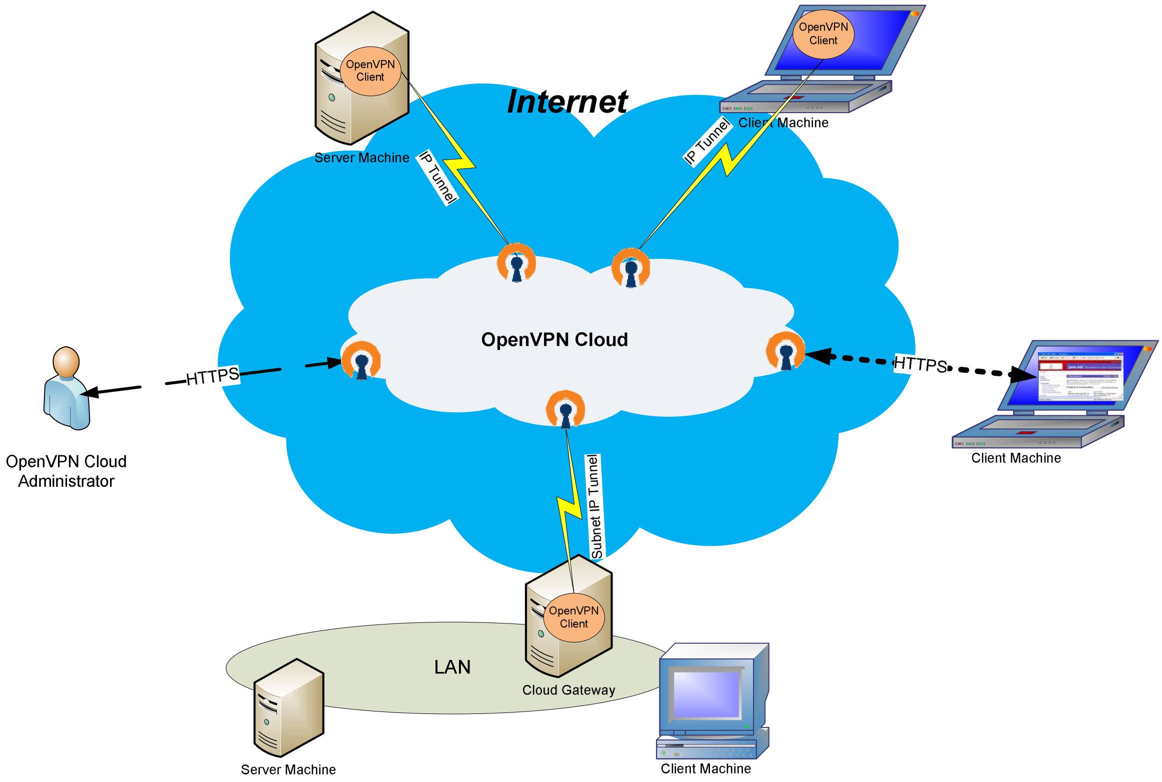

Figure 2: OpenVPN Cloud Architecture

All systems outside the OpenVPN Cloud are treated as endpoints (server machines or client machines). These endpoints access OpenVPN Cloud by connecting to OpenVPN Servers that are located at the edges of the OpenVPN Cloud. This allows for secure data communication between 2 or more endpoints with the only requirements being the OpenVPN Cloud and an Internet connection.

The OpenVPN Cloud is designed to accommodate simple deployment, zero configuration, and simplified management of VPN Secure Clouds, enabling remote access and site-to-site IP-VPN (layer 2 and layer 3) business and enterprise applications.

Application developers can create scalable and secure interactive, multicast, file sharing, and media delivery applications by utilizing OpenVPN Cloud and its capabilities. OpenVPN Cloud supports APIs that provide the necessary tools to create, delete, and share data across the OpenVPN Secure Clouds.

OpenVPN Cloud advantages

OpenVPN Cloud positions its services closer to the edge of the network, bringing all its functionality closer to the end-user. This increases the user experience by circumventing traditional network limitations, such as interruptions in service, and delays in media content delivery due to buffering.

OpenVPN Cloud takes all of the common functionality (security, transport, multicast, and switching) of the network, and combines them to provide a more cost-effective solution. It takes care of all the delivery mechanisms and scalability aspects so that applications can be developed independently. Application developers shouldn't have to deal with the complexities of the underlying network in order to distribute and share content; OpenVPN Cloud allows them to concentrate on building applications by managing all of the backend aspects of the network.

OpenVPN Cloud is the next generation of Web-scaling solutions, virtualizing Internet routers by removing traditional IP network limitations from the picture. OpenVPN Cloud Endpoints can connect to multiple VPN Secure Clouds at the same time, allowing access to all the resources of various networks.

OpenVPN Cloud incorporates the industry standard SSL protocol to provide security, and integrates easily with existing authentication systems, such as Active Directory, Radius, and PAM.

OpenVPN Cloud can be viewed as a platform to support all types of secure communications (unicast, multicast, and broadcast) as universal language for securely deliver content. The increase in Web applications will also help to spur this migration from legacy IP based to OpenVPN Cloud based delivering mechanisms and capabilities that don't exist in IP.

Summary of OpenVPN Cloud features

- No need to deploy any special VPN hardware appliance
- No need to download and install complicated VPN server software
- Enables business users to securely access OpenVPN Cloud resources and applications
- Enables application servers to securely connect to OpenVPN Cloud
- Enables private network or LAN to securely to connect to OpenVPN Cloud
- Enables secure management and monitoring of OpenVPN Cloud

- Works with existing enterprise applications
- Enables Web enterprise applications
- Provides APIs to allow application developers to develop emerging Web applications
- Removes many of the limitations of conventional IP networks and VPNs

Summary

With the OpenVPN Cloud solution, SMBs , enterprises, and web application developers can feel confident they are providing secure, scalable, and reliable data communications over the Internet. Complex configurations are required to setup and maintain the security that is essential when sending information over a public network. Another issue is the scalability needed for next-generation technologies, and the need for expanding the size of a secure private network. OpenVPN Cloud is capable of solving all of these problems and provides many additional features to overcome the inadequacies of IP networks and traditional VPNs.

With OpenVPN Cloud there is no need for expensive, dedicated hardware, a simple Internet connection is all that is required. This lowers TCO by eliminating the necessity of additional hardware, infrastructure to support it, and the extensive knowledge of networking and security techniques needed to configure it. This frees IT staff to devote their valuable resources to other matters and leaves the managing and deploying of a secure and reliable network to the automated OpenVPN Cloud architecture.

OpenVPN open source software tools and OpenVPN Cloud services are provided for application developers, SMB managers, and enterprise managers to use and have access to traditional VPN and on-demand OpenVPN Cloud services. All the tools necessary to create, control, and deliver secure VPN, interactive web collaboration, file sharing, and other types of web applications. This allows IT managers and developers to concentrate fully on building their applications, while not having to worry about the underlying delivery methods.

Where to get more information

For more information about the OpenVPN Cloud solution, contact us at **info@openvpn.net**.You can also visit our website at **www.openvpn.net**.

About OpenVPN Technologies OpenVPN Technologies is the provider of next-generation secure and scalable communication services. OpenVPN Technologiesis is a privately held company based in Pleasanton, California. More information is available at www.openvpn.net.

For more information on specific services offered by OpenVPN Technologies, please visit our website or email us at info@openvpn.net.

OpenVPN Technologies, Inc.
5980 Stoneridge Drive
Suite 103
Pleasanton, CA 94588 USA
www.openvpn.net

July 2010