Columbitech Mobile VPN™

COLUMBITECH

Technical Description

Updated 2013-01-25

Abstract

Not too long ago the workplace was a place where business related communications took place and where decisions were made. Enterprise Mobility has given today's workforce a new level of efficiency not only for telecommuters but also truly transforming areas such as production, logistics and customer relations.

Wireless technologies are finally getting mature enough to be useful for typical mobile enterprise applications, public safety records access or areas such as mobile health. Information Technology in its form of wireless data communication is literally transforming our entire society. Driven by global standards such as GSM 4G LTE and high capacity smart-phones and tablets, we are now entering an hitherto unprecedented opportunity to rapidly scale up innovations, ideas and entire economies.

However, large enterprises and service providers have until today been unable to successfully launch their corporate wireless services. One major showstopper has undoubtedly been the lack of security. Communicating sensitive data in a public wireless environment requires a security framework that is strong enough to resist any unauthorized access to the data or to the corporate network, while still being convenient for end users. The lack of convenience combined with relatively poor wireless performance is another issue that prevents a successful commercial rollout. As most enterprises or agencies today have a wide range of different devices including laptops and smart phones the wireless solution must offer security for all types of devices. There is clearly a demand for secure and robust software designed to deliver on any current and future software platform, flexible enough to fit into the advanced IT infrastructure (today fueled by cloud-based solutions) and optimized to let innovations in the form of mobile applications truly deliver as promised, and yet address important barriers of entry such as regulatory compliance and productivity for the worker.

This white paper presents Columbitech's Mobile VPN solution, a system that enables secure and convenient remote access to the corporate network. The architecture is developed with the assumption that a wireless network environment will inheritably always suffer from limited bandwidth and unstable connections. This solution has been designed to overcome the four main obstacles in wireless communications, namely the lack of security, the poor wireless performance, the low level of transparency to the end user and support for all types of devices.

Contents

Introduction

Columbitech Mobile VPN™ is a client/server based software architecture for secure and remote access to designated corporate data. The architecture enables mobile users to be continuously and securely connected to their corporate intranet, using any public or private network available. The Mobile VPN lets the user work normally, as if connected directly to the office LAN. Data is transferred within an encrypted and authenticated WTLS or DTLS session, over a public network, to the VPN server residing on the corporate network. Columbitech Mobile VPN™ is network-agnostic and transparent to the applications. This means that a remote user can use any network provider to securely access any enterprise service or application.

As the name suggests, Columbitech Mobile VPN™ is a VPN architecture developed for use in a wireless environment. Various mechanisms are used to create a high-quality wireline-like experience over unreliable, low-bandwidth wireless networks. Columbitech's solution protects the secure session in case the wireless network fails. Automatic connection re-establishment mechanisms make sure that the user automatically gets logged back on to the corporate network as soon as any access network is available. The VPN session may be established over one type of network and later resumed over another, depending on current network availability.

Columbitech Mobile VPN™ is not just another VPN solution. By using standards and protocols especially adopted for wireless communication, Columbitech has been able to create a VPN with exceptional reliability. The VPN architecture is implemented as a middleware and can be seen as a wireless communications platform, not only providing a very high level of security, but also providing high performance through efficient adaptive compression and various protocol optimization techniques. Furthermore, the peculiarities of wireless data communication are made transparent by providing the end user with a robust, convenient and hassle-free single sign-on environment.

Columbitech Mobile VPN™ is designed for seamless interoperability with existing corporate solutions. Columbitech Mobile VPN™ can make use of existing services for authentication, authorization and network management. A company that is already using another IP VPN solution may deploy Columbitech's Mobile VPN as a wireless extension and still benefit from their existing IP VPN for wireline services. If a company is not currently operating an IP VPN, the Columbitech Mobile VPN™ solution is able to provide traditional wireline VPN services in addition to the wireless functionality. Many of the wireless optimizations implemented in the Columbitech architecture are just as applicable to wireline environments.

Technology Overview

A Mobile VPN can be defined by a number of characteristics. How they differ from other VPN architectures; How they handle being used on smart phones; How they handle limited bandwidth; What security protocols they use; How they integrate with other vital systems etc.

Mobile VPN vs. other VPN solutions

Virtual Private Networks (VPN) was originally developed because the there was no built-in way to secure data over a public network in TCP/IP. A VPN is basically a way of sending data between two computers that can authenticate each other; the data sent is confidential and reliable (not changed in transit).

A mobile VPN furthermore has to take into account that a user will move from network to network and suspend their devices to preserve battery life. All this without requiring the users to restart their VPNs and devices.

Internet Protocol Security (IPSec)

IPSec is the most commonly used VPN technology today. It was mainly designed for wired networks. It is able to authenticate users, send data confidentially and reliably but suffers from a set of drawbacks in its design. It does not handle coverage gaps or device suspension at all. This is due to the fact that IPSec was designed with the assumption that the address of the device will remain unchanged.
With MOBIKE (RFC 4555) the requirement for the address having to be unchanged has been addressed. MOBIKE does however not add any mobility optimisations to increase the speed and applications still have a hard time surviving coverage gaps and hibernation.

SSL VPNs

SSL VPNs are primarily browser based. This means that you are connecting to a web portal with the built-in security of the web browser. The web portal will then proxy the data traffic to internal web resources. This works for rudimentary access and will require a client to be installed on your device for more advanced applications. When a client has to be installed on the device the SSL VPN basically turns into a Mobile VPN and the benefits of the client-less VPN are long gone.
The SSL VPNs are mainly good for public and kiosk computers. They do however not handle coverage gaps and suspension of devices well.

Mobile VPNs

Mobile VPNs are designed to handle coverage gaps, suspending devices with the same or a higher level of security. A Mobile VPN is also designed with smaller devices and limited bandwidth in mind. This means that a Mobile VPN works equally well on smart phones as laptops using wireless networks spanning from 2G up to 4G-LTE and WIFI or wired networks.
Below a few other very important aspects of a mobile VPN are outlined.

Security Protocols

A very important goal when designing a Mobile VPN is to not sacrifice security when trying to create a convenient security solution for the users. A Mobile VPN must be based on a standardized security protocol that can handle mobility. Examples of standardized security protocols that are designed for mobility are WTLS and DTLS. Both these security protocols contain all the security features that must be there as well as roaming features. The roaming features are used to handle the reestablishment of the secure session when moving from one network to the other; when resuming suspended devices or just recovering from network coverage gaps.

Device support

A Mobile VPN must be able to handle devices of very different characteristics. The different devices span from older handheld devices with limited memory and processing power to laptops and desktops with lots of memory and CPU. We have already touched on the battery aspect of a device when it comes to device suspension and it is also important to point out that Mobile VPN clients have to be implemented in such a way so they do not drain the battery while running.

It is becoming more and more evident that corporations and agencies today have a hard time standardizing on a specific type of device. The pressure from the employees is that they want to use their own devices to access internal resources of their employer. Therefore it is becoming more and more of a challenge to find a single product that can handle all the aspects of wireless and have support for all different devices. A Mobile VPN really has to have a broad device support.

Securing the device

When it comes to securing the device there are a few things to you need to consider. The Mobile VPN will ensure the confidentiality and integrity of your data traffic. What happens if the device itself gets compromised? On a laptop you will have to complement the Mobile VPN client with a personal firewall as well as Anti-virus. You should also have the Mobile VPN server require the Mobile VPN client run an integrity check before being allowed access to the internal resources of the corporate network. This integrity check should check things like if the personal firewall is running; is the anti-virus running and is it up to date; are the latest OS patches installed?

Well, all this sounds good, but what should you do with your smart phones? They have limited battery power so having an anti-virus client running all the time is not optimal.

One solution that mitigates the need for anti-virus and personal firewalls is sandboxing. Sandboxing is the way that applications are run on devices running iOS and Windows phone. Sandboxing means that the application runs in its own isolated space within the OS and cannot communicate with other applications within the smart phone. So, even of you do get a virus on your smart phone, the virus can never get access to your application.

Integration with other systems

A typical corporate network today already has a number of systems in place: an authentication server of sorts and a firewall etc. The last thing a systems administrator wants to do when installing a Mobile VPN is, for instance to setup a new user database. The Mobile VPN must be able to interact with the already existing systems.

Mobility optimizations

A Mobile VPN implements a number of optimizations. The most important ones are compression and multiplexing. The payload of every packet is compressed and also the headers of the data packet are compressed using header compression (e.g. RObust Header Compression – ROHC), which both saves bandwidth and increases transmission speed. This will also have a positive impact on the battery length as many CPU-cycles are saved when less data has to be encrypted.

Every applications communication will go through the same TCP/IP connection. This saves a lot of bandwidth as a TCP/IP is quite chatty (TCP/IP control packets) and the fewer TCP/IP connection you have to have the fewer TCP/IP control packets will be transmitted. This technique is called Multiplexing.

System Overview

Columbitech Mobile VPN™ architecture consists of a client software component, the Columbitech Mobile VPN™ Client, and one or more server components. Columbitech Mobile VPN™ Server is a server software component residing inside the corporate network. Columbitech Mobile VPN™ Server acts as the VPN terminator; it handles encryption, authentication, compression and session management. A second server component, Columbitech Gatekeeper, may be installed in the corporate demilitarized zone (DMZ) to further increase security, to simplify firewall configuration and to enable load balancing. The Gatekeeper is not a mandatory component in the Mobile VPN architecture. However, to meet strict corporate security policies, the Gatekeeper component may be required.

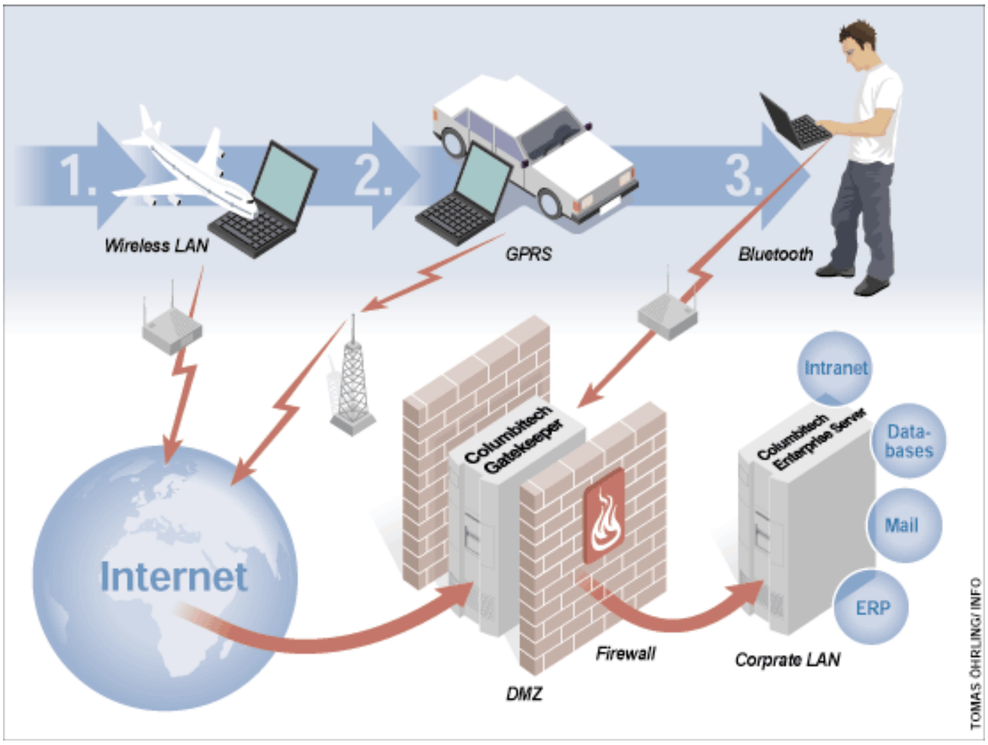


Figure 1: *Imagine a businessman at an airport, connected to his corporate LAN through a hot spot WLAN access point (1). When leaving the airport, the connection will be lost and the VPN client will switch over to a GPRS/3G/4G network (2), making it possible to remain connected, without any new logon procedures. When visiting the customer, the businessman could connect to his corporate server using the customer's Bluetooth network (3). Each network switch is performed automatically, totally transparent to the user.*

Columbitech's Mobile VPN solution is implemented at the session layer, totally transparent to the applications as well as to the underlying network infrastructure. Transparency to network operator or service provider is achieved since no software or hardware needs to be installed outside the corporate domain. However, the mobile VPN architecture includes components that may be installed by an operator or service provider to enable outsourcing of the corporate wireless data services.

Columbitech Mobile VPN™ Server

Columbitech Mobile VPN™ Server consists of several software modules that can be installed either on the same machine or on separate machines. The modules are described below:

Columbitech Mobile VPN™ Server

Columbitech Mobile VPN™ Server is the core component responsible for handling the VPN connections. Columbitech Mobile VPN™ Server is installed on a server residing on the corporate network inside the firewall, as depicted in Figure 2. Mobile VPN Clients may connect directly to Columbitech Mobile VPN™ Server or via a Gatekeeper located outside the firewall, in the DMZ. Regardless of which, the secure tunnel is always terminated by Columbitech Mobile VPN™ Server. No data will ever be revealed outside the firewall.

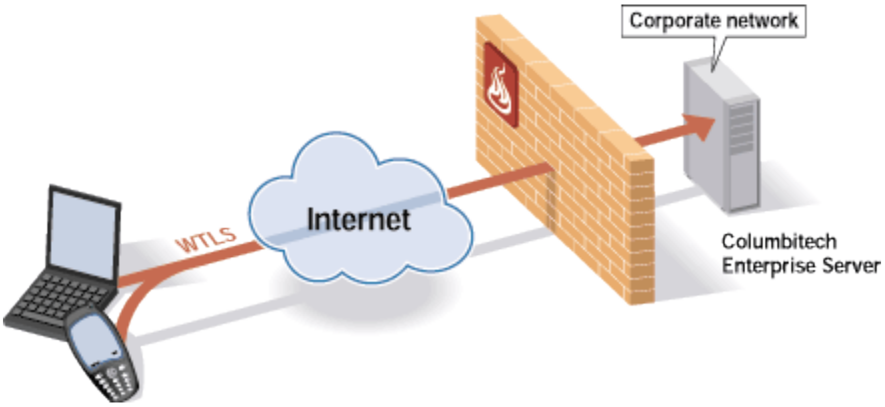


Figure 2: Columbitech Mobile VPN™ Server

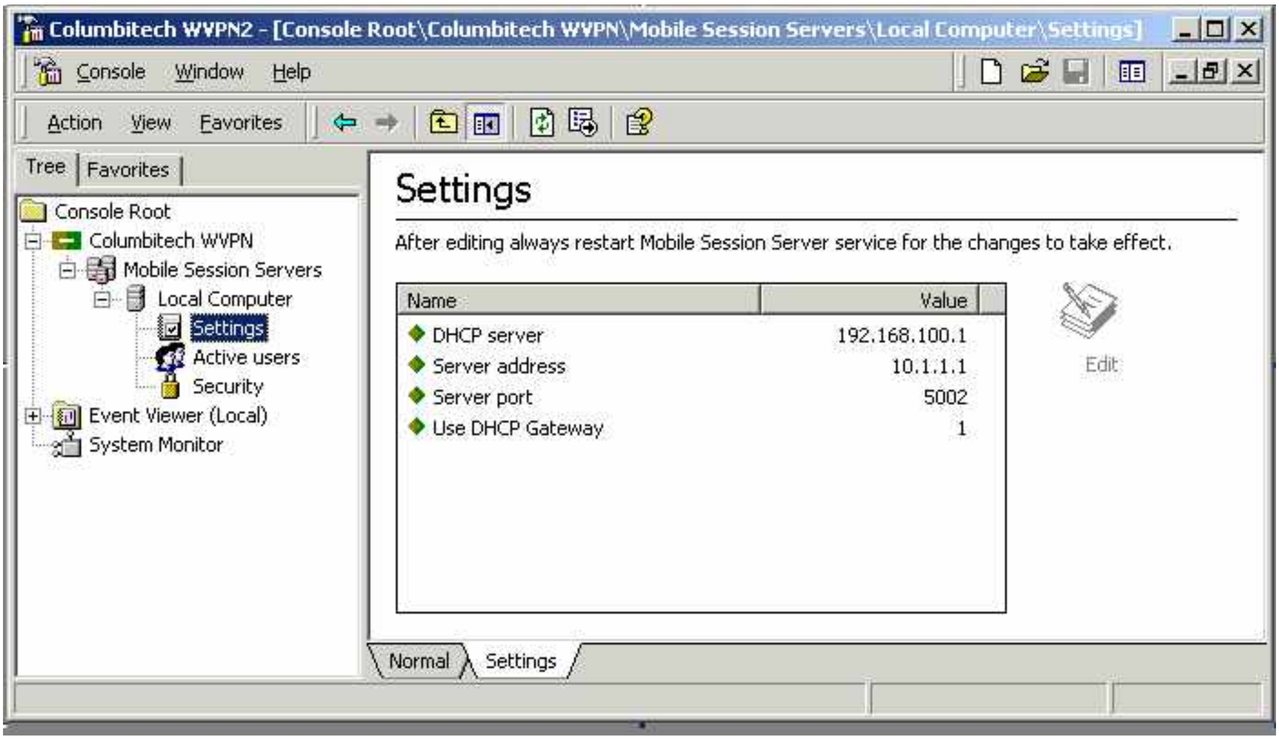
When a client initiates a VPN session, the user is required to authenticate to Columbitech Mobile VPN™ Server. Authentication can be done by using one or a combination of the following authentication mechanisms:

- Client certificate (X.509 and WTLS formats supported)
- Windows username/password.
- RADIUS (challenge/response or username/password)
- RSA SecurID one-time-password
- Smartcard / CAC card
- Biometrics
- Google authentication

When the user has been properly authenticated, the mVPN Server enables the VPN session and assigns a corporate domain IP address to the client. Data to a Mobile VPN client is intercepted by Columbitech Mobile VPN™ Server for compression and encryption before it is sent to the client. For any corresponding host or node, the VPN client appears to be connected directly to the corporate network, the fact that the client may be remotely connected to the mVPN Server is totally transparent.

Administrative Tool

The Columbitech Mobile VPN™ Server Tool is implemented as an MMC (Microsoft Management Console) snap-in. The management console is using Com+ objects for communication with the mVPN Server. This enables the system administrator to install the management console on a different machine for remotely managing the mVPN Server. It is possible to connect to multiple mVPN Servers from the same management console, a useful feature in large installations with distributed servers. As an option, the communication between the management console and the mVPN Server may be encrypted and authenticated.



Settings

After editing always restart Mobile Session Server service for the changes to take effect.

Name	Value
DHCP server	192.168.100.1
Server address	10.1.1.1
Server port	5002
Use DHCP Gateway	1

Figure 3: Columbitech Mobile VPN™ Server management console

Columbitech Certificate Manager

Included in Columbitech Mobile VPN™ Server is an application for creating and managing certificates. An enterprise is thus not dependent on an external PKI solution or provider for enforcing certificate authentication in Columbitech Mobile VPN™ with the Certificate Manager, a system administrator can easily create CA certificates, client certificates and server certificates according to the x.509 or the WTLS standard. Certificate revocation lists can be imported or created in order to revoke invalid certificates.

For large installations, the Columbitech Wireless PKI Portal can be used to automatically create a large number of client certificates. The PKI portal connects to the corporate Windows domain controller and creates a client certificate for each domain user, or for a group of users, as configured in the Certificate Manager. Furthermore, the PKI portal supports automatic distribution and installation of client certificates on the client devices.

Columbitech Gatekeeper

Columbitech Gatekeeper is an additional server component designed to be installed in the corporate DMZ. The main purposes for deploying the Gatekeeper is to:

- Increase the security through strong authentication outside the firewall.
- Simplify firewall configuration.
- Prevent exposure of the mVPN Server on the Internet.

- Enable load balancing and failover.

If the system is configured to use a Gatekeeper, the mVPN Server connects to the Gatekeeper when the server starts. The connection is established from inside the corporate network to the DMZ, something most corporate security policies allow. The VPN clients connect to the Gatekeeper, they do not connect directly to the mVPN Server. The Gatekeeper connection is totally transparent: The VPN client does not explicitly have to be configured to use the Gatekeeper, this is taken care of by the mVPN protocol.

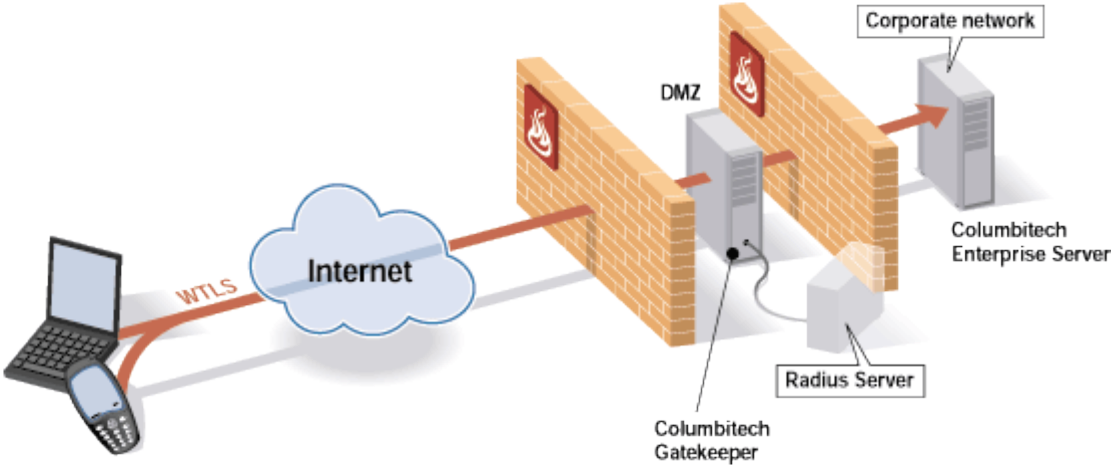


Figure 4: *Gatekeeper deployment*

When an mVPN Client initiates a handshake, the Gatekeeper authenticates the user before allowing the connecting client to continue the handshake with the mVPN Server. Data from mVPN Client is intercepted by the Gatekeeper and multiplexed over the TCP session that was initially created by the mVPN Server. Thus the firewall does not have to be opened for incoming TCP connections. The Gatekeeper supports the following authentication mechanisms:

- Client certificate (x.509 or WTLS format)
- RSA SecurID
- RADIUS (challenge/response or username/password)

By deploying Columbitech Gatekeeper, strong user authentication can be enforced before any traffic is allowed inside the firewall, still without breaking the end-to-end encryption between the VPN client and the VPN server.

Columbitech Gatekeeper can also be used to seamlessly and dynamically scale up the system, while at the same time providing the mVPN Server with load balancing and failover. Several mVPN Server can be grouped into one logical server by using a server group identifier. Large enterprises with different branch offices or isolated departments may deploy a Gatekeeper inside their corporate DMZ and have one mVPN Server group per branch office or department connecting to the same Gatekeeper.

The Gatekeeper is responsible for distributing mVPN Clients evenly on the available mVPN Servers within one server group. If one mVPN Server is going down, only the users connected to that particular mVPN Server would be disconnected. When the mVPN Client reconnects, the Gatekeeper will allocate another mVPN Client from the server group to the client.

Administrative Tool

Using the Gatekeeper Administrative Tool, a system administrator can configure the Gatekeeper service and monitor connected mVPN Servers and users. The functionality is very similar to the mVPN Server Administrative Tool.

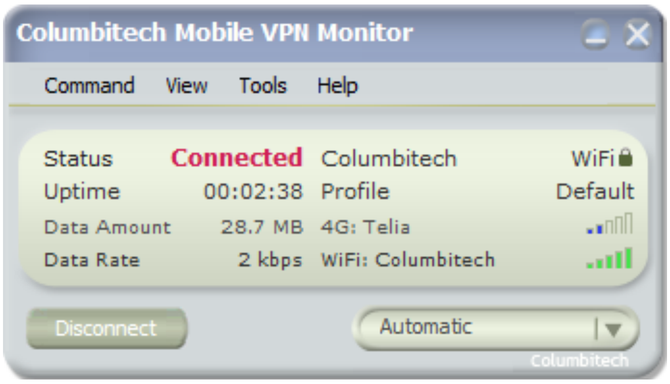
Columbitech Mobile VPN™ Client on Windows

The Columbitech Mobile VPN™ Client is implemented as a virtual network interface. When the client connects to the mVPN Server, the virtual interface gets an IP address allocated from the corporate domain. The mVPN Client reconfigures the routing tables to force all applications to send data through the virtual interface. Functions at the session layer compress and encrypt the data before it is passed down to the virtual interface for address translation. The data is then multiplexed over one of the physical network connections for further transport to the mVPN Server.

The mVPN Client runs as a Windows service and uses the following components to interface the user:

Client Monitor

The client monitor is an icon on the system tray menu. The monitor displays the current connection status, available connections, and the currently used bearer. In expanded mode, the mVPN Client Monitor can be used to change connection state, profile and bearer.



Status	Connected	Columbitech	WiFi
Uptime	00:02:38	Profile	Default
Data Amount	28.7 MB	4G: Telia	
Data Rate	2 kbps	WiFi: Columbitech	

Figure 5: *Mobile VPN Client Monitor (expanded mode)*

mVPN Client Control Panel

The control panel is used to change the settings of the mVPN Client, including connection settings, connection preferences and user profiles. Administrative privileges are required to change the mVPN Client settings or to allow for the personal firewall to be switched off. A normal user can thus not bypass the VPN by disabling the Wireless VPN client or by changing the security configuration.

SSO Module

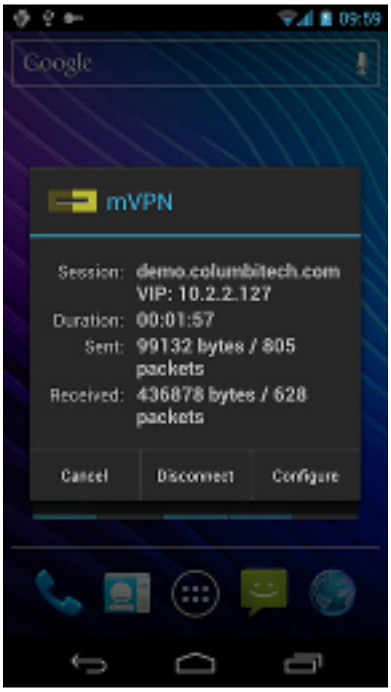
The Columbitech SSO module is a module for integrating the mVPN Client login with the standard Windows login mechanism. When a VPN user logs on to the computer, the Columbitech SSO module intercepts the user’s credentials and the user gets transparently logged on to the mVPN Server before the Windows login logs on to the windows domain.

Client API

Columbitech Mobile VPN™ Client includes a software API with which an application developer can integrate the Mobile VPN functionality into a user application in order to make the Mobile VPN functionality transparent to the end user. By using the client API, an application can connect and disconnect to the mVPN Server, change profile and trigger network roaming. The application can also retrieve status information regarding data rate and the type of bearer through the API. This feature opens up new possibilities for creating adaptive applications where the behaviour and information is adapted according to the currently used bearer type.

Columbitech Mobile VPN™ Client on Android

The Columbitech Mobile VPN client for Android uses the Android VPN API that was introduced in 4.0 (Ice Cream Sandwich). The Android VPN API exposes interfaces to the built in virtual network interface (i.e. TUN adapter) in Android. The Columbitech Mobile VPN client for Android supports all functionality of the Columbitech Mobile VPN including DTLS. It uses the FIPS-validated cryptographic module from OpenSSL.



mVPN

Session: demo.columbitech.com
VIP: 10.2.2.127
Duration: 00:01:57
Sent: 99132 bytes / 805 packets
Received: 436878 bytes / 628 packets

Figure 6: The mVPN client on Android

Columbitech Mobile VPN™ SecureBrowser on iOS

The mVPN client for iOS is a little bit different from the other platforms. It is built-in to a Web browser which means that all HTTP/HTTPS requests and responses are tunnelled through the VPN tunnel instead of using its normal ports. The benefit from this is that no additional ports needs to be opened when allowing access to internal web servers. All applications on iOS are sandboxed which means that the applications cannot communicate to each other. This mitigates the need for anti-virus as the viruses cannot high-jack other applications. The SecureBrowser does not listen for any incoming data traffic which in turn mitigates the need for a personal firewall. The Columbitech Mobile VPN SecureBrowser for iOS supports all functionality of the Columbitech Mobile VPN including DTLS. It uses the FIPS-validated cryptographic module from OpenSSL.

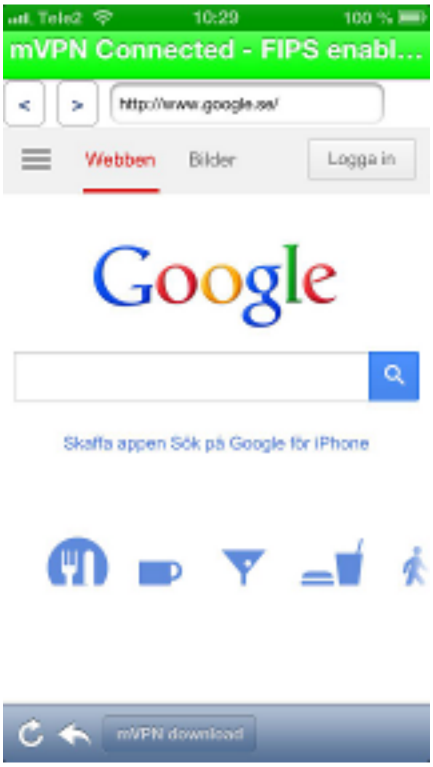


Figure 7: The SecureBrowser for iOS

Columbitech Mobile VPN™ App SDK

Both the SecureBrowser and the mVPN client for Android have been built using the App SDK. The App SDK consists of a number of libraries that are very easily integrated into any iOS, Android or Windows Modern UI Apps (Windows 8 and Windows phone 8).

By integrating the Columbitech Mobile VPN App SDK into an application, the application will be able to use an existing mVPN infrastructure and use all the mVPN functionality. The application will also be using a FIPS-certified cryptographic module.

Functional Description

Security

Many wireless network technologies are using various mechanisms to prevent third parties to eavesdrop and tamper with transmitted data. Examples of such mechanisms are frequency hopping and the WEP link layer encryption system. Although those techniques make eavesdropping more complicated, they are not to be seen as secure solutions. With the appropriate equipment and knowledge it is fully possible to listen in on traffic transmitted over e.g. GSM(2G), DECT, 802.11 W-LAN and Bluetooth. Also, the data is protected only when transmitted over the wireless link. Most wireless network providers are using the Internet to transport data from its backbone to the end customers, thus the data will be transmitted in clear. There is obviously a need for end-to-end secure VPN solutions.

Not only is it important to make the data transmissions impossible to eavesdrop on, it is equally important to protect the corporate network from unauthorized access and a good VPN must be able to handle both requirements. Transmitted data is effectively hidden by the use of encryption and the corporate network is protected by enforcing strong user authentication. Columbitech Mobile VPN™ implements the latest standards and algorithms for securing the transmitted data, the corporate network and the client device, as will be described in the following paragraphs.

Columbitech Mobile VPN™ is FIPS 140-2 certified and uses the FIPS-certified Cryptograhic module from OpenSLL on Android, IOS and applications created with the App SDK.

Securing Traffic

To secure the transmitted data, a virtual encrypted tunnel is created between the mVPN Client and the mVPN Server. Columbitech Mobile VPN™ is using the WTLS [5] or DTLS standard to encrypt, authenticate and validate the transmitted data. WTLS is a wireless implementation of TLS, which is an enhanced version of SSL 3.0. The reason for using WTLS instead of IPSec is mainly that IPSec suffers heavily from sub-optimized performance when applied over wireless, low-bandwidth networks. DTLS (rfc6347) is also a wireless implementation of TLS and uses UDP for its data transfer. The Columbitech Mobile VPN uses DTLS 1.2, which is based on TLS 1.2.

The WTLS and DTLS framework defines a set of protocols and algorithms for encryption, signing and hashing; Columbitech Mobile VPN™ uses DES (56 bit), 3DES (112 bit) and AES (up to 256 bit) for the symmetric encryption of the payload data. RSA (up to 15360 bit) is used for asymmetric encryption during the initial handshake, and MD5 (128 bit) or SHA (up to 512 bit) is used for validating the data integrity. Columbitech Mobile VPN™ can be configured to use a combination of the algorithms mentioned above to achieve a desired level of security.

Securing Network Resources

To protect the corporate network from unauthorized access, Columbitech Mobile VPN™ enforces strong authentication mechanisms. User authentication may be performed by the mVPN Server inside the corporate network, by the Gatekeeper residing outside the firewall, or by both the mVPN Server and the Gatekeeper. Typically, a corporate security policy might state that no unauthorized data is allowed inside the corporate network. In such a scenario, the Gatekeeper could be configured to enforce client certificate authentication or one-time-password authentication before the VPN session is handed over to the mVPN Server. The VPN handshake will then be continued by the mVPN Server, possibly asking the user for a Windows NT or RADIUS password, a client certificate, or a one-time-password.

Columbitech Mobile VPN™ has been designed to interoperate with the existing corporate authentication mechanisms. With the Columbitech SSO module, a user will be transparently logged on to the mVPN Server as soon as he or she logs on to the computer. Furthermore, a system administrator does not have to maintain two different sets of user accounts for each user; existing user databases may be used for Mobile VPN authentication. Columbitech Mobile VPN™ Server and Columbitech Gatekeeper can be configured to utilize any standard RADIUS server, Windows Active Directory server, or RSA ACE server. Columbitech Mobile VPN™ has full PKI support to ensure for maximum scalability and to provide for reliable authentication of servers and clients. Certificates are easily created, maintained and distributed with the included Wireless PKI Portal and the certificate management application.

To further secure the network side, Columbitech Mobile VPN™ Server includes a firewall to enforce packet filtering and inspection. Enabling strong user authentication in combination with firewall protection at the network edge is the most effective defense against intrusion. In most organizations, access to network resources is based on user and group policies. To enforce group based access control, Columbitech Mobile VPN™ can be configured to allocate IP addresses that belong to different IP subnets, depending on which user groups the connecting user belongs to. Access can then be controlled by a firewall or policy router. The Enterprise Server can also be configured to allocate different IP addresses depending on if the user connects directly to the Enterprise Server or via a Columbitech Gatekeeper. This allows the system administrator to set up different access policies depending on whether the user connects remotely or directly from the office.

Securing Clients

Employees often bring their laptops home and connect them to the Internet through their home broadband connections. As soon as the computer is connected to the Internet it is exposed to attacks. The corporate firewall is no longer there to protect the computer from viruses, trojan horses and other exploits. Later, when the computer connects to the internal network, the malicious code could easily spread to the whole network and cause substantial damage.

Columbitech Mobile VPN™ Client on Windows ensures that all data is processed by the virtual VPN interface. The mVPN Client software protects every network interface on the computer, including dial-up connections, by applying IP filters that only accept properly encrypted data that has been sent through the VPN tunnel. This functionality is part of Columbitechs personal firewall and the main goal is to protect the computer from malicious attacks when exposed to public networks as well as to prevent client applications from bypassing the VPN connection.

Managing devices is perhaps one of the biggest challenges with a mobile workforce. It is important that the mobile devices run the latest security patches and other appropriate security software, as specified by the corporate IT policy. To make sure that the connecting device does not compose a security threat, Columbitech Mobile VPN™ contains built-in Network Admission Control (NAC). This means that the client can check the integrity of the client computer before allowing it to connect to the corporate network. When the Mobile VPN Client requests a connection, the Columbitech Mobile VPN™ Server sends an encrypted script, or program, that executes on the client computer. The script can verify that security patches, anti virus programs, personal firewalls and other security software are running and up-to-date. Depending on the return value of the script, the client is accepted by the server, rejected by the server, or as a third option, placed in quarantine. When placed in quarantine, the client gets limited access to the network, just enough to download e.g. virus definition updates or OS patches.

Securing the client when using the Mobile VPN Client on iOS and Android the challenges are a bit different.
On iOS the need for anti-virus and a personal firewall is mitigated due to the architecture of iOS. In iOS every application runs in its own space and cannot communicate with other applications in the OS. This technology is called sandboxing. The need for a personal firewall is further decreased due to the fact that the Mobile VPN client on iOS does not listen on any incoming ports.
On Android the applications are not sandboxed. This means that you will probably need anti-virus and some kind of firewalling.
On both iOS and Android the NAC functionality described above will further strengthen the security of the smart phone devices. Having the security policies checked every time a device connects ensures that the security of the devices does not degrade over time.

Wireless PKI

In order to establish an encrypted WTLS/DTLS tunnel, a shared secret key must be agreed upon by both communicating peers. To exchange the secret key, asymmetric encryption is used. In asymmetric encryption, each party has a key pair consisting of one *public key* and one *private key*. The public key is publicly available to anyone, while the private key remains private. A message encrypted with the public key can only be decrypted using the private key (and *not* using the key that encrypted the message, as is the case in symmetric cryptography). Asymmetric encryption is extremely processor heavy and thus not feasible for encrypting large amounts of data. Instead, symmetric encryption is used for the actual data transfer and asymmetrical encryption is only used to exchange the shared secret key used for the session.

Public Key Infrastructure (PKI) is the infrastructure for managing a trusted matching between public keys and their owners. One of the fundamental components of PKI is the digital certificate. A digital certificate has many similarities with a passport. It contains information about its owner, or subject, and about the entity that issued it. The public key of the subject is also included, as well as a *digital signature* that proves the authenticity of the certificate.

To handle certificates, Columbitech Mobile VPN™ includes a Certificate Manager with which a system administrator can create and manage digital certificates, i.e. it lets you operate a simple certificate authority. A wireless PKI portal included in Columbitech Mobile VPN™ Server allows easy certificate management in large installations. The PKI portal connects to the Windows user account database and automatically creates and distributes client certificates for all users in the corporate domain. Columbitech Mobile VPN™ is fully x.509 compliant, any public certificate authority can be used to create and manage certificates for the Columbitech Mobile VPN™ architecture.

Convenience

Automatic Session Resume

Intermittent connectivity is unfortunately a characteristic closely related to wireless communication. Connections go up and down due to bad radio coverage, shortage of radio resources or due to interference. One of the design goals for the WTLS and the DTLS standard was to address these issues by implementing mechanisms for fast session re-establishment after a network failure. The result, called *Session Resume*, allows for a very fast VPN reconnection without any user interaction. The user does not have to go through any extra logon or authentication procedures. As soon as the radio link is re-established, the client and the server are authenticated and the WTLS/DTLS session is resumed from where it was suspended. This technique of resuming an old session is sometimes referred to as a lightweight handshake. It is done in a background process very efficiently.

The Session Resume functionality in Columbitech Mobile VPN™ also allows for a seamless and automatic activation of the VPN session when a device resumes from hibernation. This is a very important feature, especially when using mobile devices with limited battery power. If the device cannot enter hibernation, the battery power on a standard MOBILE DEVICE will not last longer than a couple of hours. With standard VPN solutions, resuming from hibernation often means that the VPN Session has to be re-established and the user has to log on again to the VPN server.

Data Transaction Recovery

Even though the secure session is re-established automatically, (this may also include automatic dial up of a dial-up connection), it is very frustrating to lose a network connection, especially if data was being transferred. In order to make life easy for the mobile user, *Columbitech Mobile VPN*™ implements a function called *Transaction Recovery*. Transaction Recovery allows a data transfer to pick up from where it was interrupted. The user does not have to restart the transfer, nor the application. All applications will survive a lost connection and all interrupted data transfers will automatically continue from where they were interrupted, as soon as data can be transferred again. Retransmission mechanisms at the session layer make sure that lost data segments get retransmitted before the data transfer resumes. In the eyes of an application, this short re-establishment period will just be viewed as a period of lower-than-usual bandwidth.

Seamless Network Roaming

Seamless network roaming is a delicate task and a great technical challenge. With seamless network roaming we mean the general concept of moving between different networks, possibly of different types, without loosing any open connections. Columbitech Mobile VPN™ uses the session resume functionality implemented in WTLS and DTLS to create a seamless, always-connected experience for the mobile user. During network roaming, the secure session is instantly resumed over the new network and the flow control and transaction resume mechanisms guarantee that no data is lost in the process. The seamless network roaming functionality is totally transparent to the application layer, i.e., the applications believe they are still using the same connection.

Since the roaming functionality is implemented at the session level, the client applications are not dependent on TCP for retransmissions and flow control during the handover. This is particularly important when roaming from a fast network, e.g. 3G/4G, wireless LAN or LAN, to a slow network, e.g. GPRS, GSM or CDPD, since TCP will most likely fail to adapt to the drastic change of bandwidth and delay.

Single Sign-On

The Mobile VPN logon can be made transparent to the user. By integrating the VPN logon into the standard Windows domain logon, the Mobile VPN user gets transparently logged on to the mVPN Server when he or she logs on to the computer. Standard Windows clients are supported as well as Novell Netware clients.

Internet service providers and wireless hotspot providers often require the user to logon before gaining Internet access. The most common way to authenticate a user is to redirect the user's Internet browser to the ISP's authentication server. The users must then enter a username and password before they can be allowed to enter external networks. By defining a network access policy in the Mobile VPN Client, the hotspot login can be performed entirely in the background by the mVPN Client, without any user interaction. A user is thus able to logon to the access network, the mVPN Server, and the corporate Windows domain with one single login.

Performance

Since radio frequencies are a limited natural resource, wireless capacity will always be limited. Therefore, wireless networks will always be significantly slower than wired networks. This motivates the efforts for implementing wireless optimizations.

Adaptive Data Compression

Compression is probably the most widely used optimization technique for data reduction. A characteristic that all types of compression algorithms have in common is that they take advantage of recurring structures or patterns in the data in order to compress it. In contrast, good encryption is designed to distort and remove patterns. Therefore, if both compression and encryption is applied to a data stream, it is vital to compress the data *before* encrypting it, in order for the compression to be efficient. Columbitech Mobile VPN™ implements data compression at the session layer, before the data is encrypted. This way, the compression algorithm may be applied on large blocks of data, ensuring very high compression ratios. IP level compression on the other hand is applied on individual IP datagrams. Therefore, the compression algorithm cannot exploit recurrences in the data flow, since the datagrams are compressed separately.

When using thin clients, such as handheld devices, over fast networks such as wireless LAN or fixed networks, the device's memory and CPU load may be the critical bottleneck, not the bandwidth. Therefore, compression is applied on a per connection basis. When roaming between fast and slow bearers, the Mobile VPN Client can be configured to dynamically switch the compression on and off, according to the current user profile.

Adaptive Encryption (Trusted Zones)

Trusted Zone is the term used for any network where the client can access the mVPN Server directly without going through a Gatekeeper. This is typically the local wired network. It is possible to configure the mVPN Server to allow clients to bypass the VPN if connecting from a Trusted Zone to further increase performance. The user is still subject to full authentication and the client computer will be subject to integrity check prior to bypassing the VPN. The VPN client is still running to detect change of network, from a trusted to a non-trusted network.

Transmission Protocol Optimization

Other schemes for data reduction are also applied; Optimizations at the transport level, such as TCP connection multiplexing, prevent flooding the wireless link with redundant TCP retransmissions during handover. In short, the available bandwidth will be used to transport actual user data instead of redundant TCP retransmissions. If the entire link capacity is utilized for retransmissions, TCP will eventually break down due to lack of new user data on the link. However, if all data were multiplexed over one TCP Session, there would be plenty of room for new data to reach the receiver and the applications would be more likely to survive a bad connection.

When communicating over networks with large delays, such as most cellular wireless networks, the standard TCP flow control mechanism leads to poor link utilization. A TCP sender will not be able to fully utilize the available link bandwidth. This is caused by a combination of a large delay-bandwidth product and a badly configured TCP transmission window size. The standard setting of the TCP buffers causes the TCP connection to stall because it takes to long for the receiver's acknowledgments to return to the sender. A TCP sender is dependent on the returning acknowledgments as well as on the size of the sending window for increasing its sending rate. A small sending window and a long acknowledgment delay will undoubtedly prevent the connection from reaching the maximum link speed. To prevent this from happening, the Columbitech Mobile VPN™ Client continuously monitors the current round-trip time in order to dynamically configure the TCP buffers for optimal transmission performance.

Data Encapsulation

Columbitech Mobile VPN™ Client software uses OS routing mechanisms for capturing, encrypting and forwarding traffic. By creating a virtual network interface card (NIC) and forcing all application data to be routed through it, the VPN client is able to encrypt all outgoing traffic without requiring any changes to existing applications. The virtual NIC intercepts the data and sends it to the VPN client software for processing. After compression, encryption and address translation, the data is sent to the currently used physical interface. By using address translation mechanisms rather than standard tunnelling, Columbitech Mobile VPN™ is able to reduce the data overhead to less than 10%, as compared to over 25% for standard IPSec. Session based data compression and transport optimization reduces the overhead to a minimum.

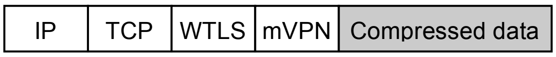


Figure 8: Data transport in Columbitech Mobile VPN™

The local termination of connection-oriented traffic makes the client resistant against temporary loss of network connections. Even though the real network connection may go up and down, the virtual NIC is always enabled and is always accepting traffic. The effect of the virtual NIC being constantly enabled is that if a network connection goes down, the locally terminated application connections will not be affected and the applications will still believe that they are online. A network failure immediately triggers the VPN client software to start reconnecting to the VPN server. The client software starts scanning for available networks and connects through the best available network, according to a defined user profile. When the client succeeds to connect to the VPN server, the WTLS/DTLS session is instantly resumed and all data transfers are synchronized and continued.

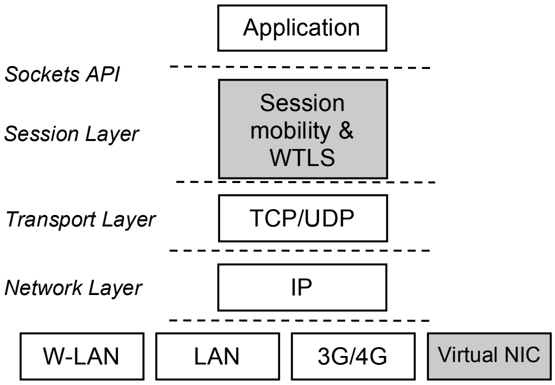


Figure 9: *The mobile VPN client protocol stack*

When a VPN client connects to the corporate network, the mVPN Server allocates an IP address from the corporate domain to the virtual VPN interface. The mVPN Server allocates the IP address by making a DHCP request to an existing DHCP server on behalf of the client. If there is no DHCP server on the network, the mVPN Server may be configured to allocate IP addresses from a specified IP address range. In practice this means that each VPN client actually has two IP addresses; one on the physical interface, allocated from the access network provider and one on the virtual interface, allocated by the corporate domain. The IP address on the physical interface will change when the client moves between different networks. The IP address on the virtual NIC will however remain constant during the whole session.

The fact that the client keeps the same IP address on the virtual interface enables seamless roaming with continuation of services. All applications and communicating peers use the corporate IP address on the virtual interface when communicating with the client. The IP address on the physical interface is hidden from the applications and is only used for transporting the data between the client and the VPN server. Inside the corporate network, the mVPN Server translates all incoming and outgoing traffic to hide the physical interface's IP address from the applications.

A connection between a VPN client and a server application is terminated locally inside the Mobile VPN client. In order to establish the connection all the way to the application server, the client requests the mVPN Server to establish a connection on its behalf. Once the connection has been properly established, the client and the server may start forwarding traffic between each other. The client application as well as the server application is totally unaware of the mVPN Server, they believe that they are connected directly to each other.

A server application connects to a remote VPN client exactly the same way as if the client had actually been physically connected to the corporate network. The connection request is intercepted by the VPN Server and forwarded to the VPN client through the WTLS tunnel. If the client has an active application listening on the specified port, a connect message is reported back to the mVPN Server and the mVPN Server accepts the connection to the application server and data can be sent to the client. However, if the client was not listening on the specific port, the VPN client software sends a reject message to the mVPN Server, which in turn sends the appropriate ICMP message to the connecting application.

Connectionless data is handled the same way; a UDP datagram sent from a corresponding node is intercepted, encrypted and re-encapsulated by the mVPN Server for further transport to the client.

The use of split TCP connections adds robustness and flexibility to the system. If the TCP connection between the client and the mVPN Server would break down for any reason, the application connections will be maintained and the communication may continue as soon as a new physical connection is established. The split TCP connection approach also allows for further optimization of the communication between the VPN client and the mVPN Server, since the applications are actually unaware of this connection. TCP may be re-implemented or replaced by another protocol that is optimized for wireless communication.

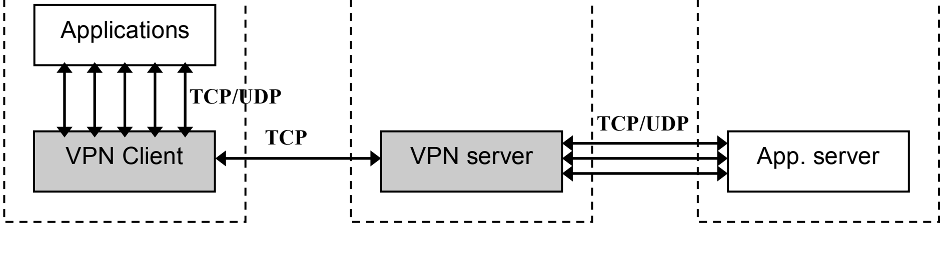


Figure 10: Data transport overview. The application connections are terminated locally on the client and the data is tunneled to the mVPN Server over one single TCP connection. The mVPN Server performs address translation and forwards the data to the destination.

However, since the TCP end-to-end semantic is violated, it is vital that the architecture implements mechanisms for end-to-end flow control and retransmission. To prevent data loss in case the connection between the VPN client and the mVPN Server would fail, the Columbitech architecture uses standard TCP mechanisms to stop the sending application from transmitting more data. In case of network failure, the mVPN Server will immediately send a TCP control message to the sender, stating that the mVPN Server has no more receiving buffers available. When the connection to the VPN client is re-established, the mVPN Server commands the TCP sender to continue transmitting. This approach is to be preferred before a solution where the VPN server buffers data in memory. Eventually the server will run out of memory and start dropping packets. The former of these two TCP flow control mechanisms is implemented in both the mVPN Server, the Gatekeeper and in the Mobile VPN client.

To avoid loosing packets that were being transmitted when the connection broke down, the mVPN Server stores the few last transmitted packets for each client connection. When the VPN client reconnects, the mVPN Server and the VPN client synchronize their data flows and if any packets were lost in transit, they are retransmitted.

Scalability

Columbitech Mobile VPN™ includes support for server load balancing and fail over. Expensive third-party solutions are thus not required to provide server redundancy. By using Columbitech Gatekeeper, several mVPN Servers can be clustered into one mVPN Server group, as depicted in Figure 11. When a user connects to the corporate network, the Mobile VPN Client will establish a connection to the Gatekeeper. After initial user authentication, the Gatekeeper will hand over the client to one of the mVPN Servers belonging to the server group specified by the client. It is possible to cluster as many as 255 mVPN Servers in one server group and one Gatekeeper can handle a large number of server groups. A large enterprise with different branch offices or departments in separate administrative domains may deploy a Columbitech Gatekeeper in the corporate DMZ to centrally manage the remote access. When a client connects to the Gatekeeper, the Mobile VPN session will be handed over to one of the mVPN Servers belonging to the accessing user's administrative domain.

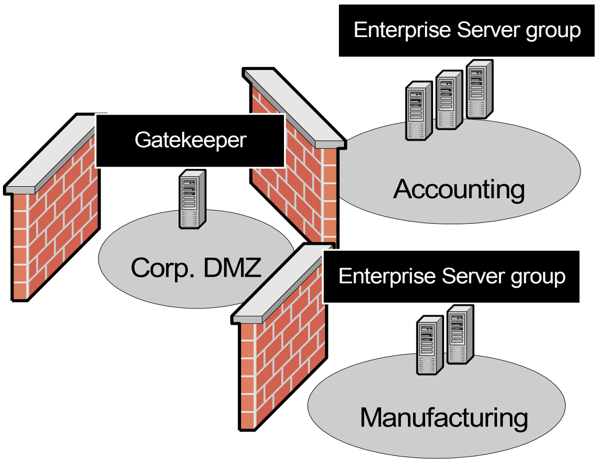


Figure 11: Example of mVPN Server clustering

If one mVPN Server within the server group were to fail, only the users connected to that particular server would be disconnected. In this case, the Mobile VPN Client will prompt the user to log in again and the Gatekeeper will now allocate another mVPN Server from the client's server group. A server failure will thus only cause a limited and temporary disruption of the Mobile VPN service.

The server group functionality allows for seamless system up-scaling; mVPN Servers and server groups may be added without any interruption of the service. New mVPN Servers will automatically connect to a Gatekeeper and send information about the server group they belong to. The mVPN Server also sends information to the Gatekeeper regarding its processing capabilities to ensure for efficient load balancing

Technical Data

Authentication Mechanisms

Columbitech Mobile VPN™ solution can be configured to use one or more of the following authentication methods:

- Windows AD username/password
- Radius (username/password or challenge/response)
- X.509 certificates
- WTLS certificates
- RSA SecurID
- Smartcard
- Biometrics
- Google

* Some authentication mechanisms are not supported by the embedded client.

Encryption Algorithms

Columbitech follows the WTLS and DTLS standard and supports the following algorithms:

Encryption:

- DES (56 bit)
- Triple DES (112 bit)
- AES (up to 256 bit)

Key exchange:

- RSA (512-15000 bit)

Hashing and signing:

- MD5 (40-128 bit)
- SHA-1 (40-512 bit)

Software Requirements

Columbitech Mobile VPN™ Client

Windows 2000 professional + SP4
Windows XP
Windows Vista
Windows 7
Windows 8
Pocket PC 2002
Windows Mobile 2003, Mobile 5, Mobile 6, Mobile 6.1, Mobile 6.5
Windows CE 3.0*
Windows .Net*
Windows CE 5.0/6.0

App SDK – support for building apps with built-in mVPN functionality for Android, iOS and Windows Modern UI apps.
Android – supported for Android 4.0 (Ice Cream Sandwich)
iOS – implemented as a Web browser with a built-in mVPN client.

Columbitech Mobile VPN™ Server
Windows 2000 Professional + SP4
Windows 2000 Server + SP4
Windows 2003 Server
Windows 2008 Server
Windows 2012 Server
Wireless Switch (customized installations)
Linux (different distributions)

Columbitech Gatekeeper
Windows 2000 Professional + SP4
Windows 2000 Server + SP4
Windows 2003 Server
Windows 2008 Server
Windows 2012 Server

* Special restrictions apply. Contact Columbitech for more information

Hardware Requirements

Columbitech Mobile VPN™ Client **for Windows**

CPU	Any CPU capable of running Windows 2000/XP/Vista/7/8
Memory	128 MB required

Columbitech Mobile VPN™ Client **for Windows Mobile**

CPU	StrongARM

Columbitech Mobile VPN™ Server for Windows and Columbitech Gatekeeper

CPU	Any CPU capable of running Windows 2000/2003/2008/2012
Memory	256 MB required, 512 MB recommended

Conclusions

Columbitech Mobile VPN™ has been created with the mobile user in mind. By enabling secure data access over any wireless IP network, Columbitech's Mobile VPN solution brings remote access to a new level. With inherent support for seamless roaming between different networks and subnets, the mobile user gets the final say about when to disconnect. If networks go down or become unavailable, the software will automatically and smoothly re-establish live connections, without any need for cumbersome login procedures.

In this white paper we have argued that wireless communication is so vastly different from wireline communication that VPN solutions built on wireline technology will fail to provide a seamless end user experience when used in a wireless environment. This we believe is mainly due to:

- **Lack of mobility** – the traditional VPNs does not have the capability to survive the challenges of mobility. Battery preservation, coverage gaps and broad device support must be addressed in a mobility solution.
- **Lack of performance -** due to extensive protocol and processing overhead introduced by IPSec
- **Lack of robustness** - IPSec does not cope well with low-bandwidth, large-delay networks. Although some instability issues are not directly related to IPSec protocols, they make no effort to protect the user from these shortcomings.

Columbitech Mobile VPN™ is developed especially for mobile devices and wireless networks. Large effort has been made to reduce the processing and data transport overhead to a minimum as well as to create a robust communications platform on which any wireless-unaware application can operate. By only using standards and protocols developed and optimized for wireless communication, Columbitech has been able to provide a VPN architecture with exceptional robustness, end user experience and the flexibility of building mVPN apps, still maintaining the highest possible level of security.

References

[1] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

[2] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[3] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[4] Perkins, C., “IP Mobility Support”, RFC 2002, October 1996.

[5] Wireless Application Protocol Wireless Transport Layer Security Specification, February 2000. (http://www.wapforum.org.)