Seamless Roaming in a Remote Access VPN Environment

Always on

If we look just a few years into the future, the "office warrior" who works exclusively onsite will be a scarce phenomenon. Instead, these busy professionals will use PCs, smartphones, and tablets to answer their emails and access data on the company network, whether from a home office, at a coffee shop, from their hotel room, or while on the road. As globalization continues to drive the growth of mobile office workers, we'll see an increase in the global mobile workforce: **from 1.26 billion in 2013**, accounting for 36.4% of the global workforce, **to 1.67 billion in 2018**, accounting for 41.8% of the global workforce.[1]

The mobile workforce is not limited to large enterprises. According to IDC, small and midsize companies from every geography and size category are making active use of mobile technology, with employees often leading their companies to adopt new technology.[2] In particular, CEOs and sales and service employees use mobile devices to access company data over a VPN (Virtual Private Network) during business trips.

All these mobile workers avail themselves of the best-possible communication medium at any location, at any point in time. They'll use a Wi-Fi network at the airport or hotel, a 4G cellular network in a coffee shop, and the LAN at the company offices. And they'll move amongst them, from the airport Wi-Fi to 4G as they're boarding the plane.

A remote access VPN solution has to guarantee seamless roaming between those different networks—without compromising security.

The Demands of Seamless Roaming

Most business laptops are equipped with a Wi-Fi module, a cellular network chip, and an Ethernet card. However, the network type that corresponds to each of these communication mediums isn't always available to the user. Maintaining a continuous VPN connection isn't a simple matter when switching between networks.

Changing between various types of networks and communication media—known as seamless roaming—has become the expectation, not the exception. However, the

There are three ways for mobile devices to set up a secure VPN tunnel to the company network:

1. The traditional wired Ethernet LAN
2. Wireless LAN (Wi-Fi) at public hotspots, hotels, or companies
3. Cellular network connections

For cellular network connections, the system must support the GSM network, 3G connections, and high-speed connections via 4G (LTE, or Long Term Evolution) networks.

flexibility to move among communication media poses significant challenges to a remote access solution. To maintain a continuous VPN connection, the solution must:

- Automatically support any change of communication medium;
- Dynamically redirect an existing VPN tunnel during a change; and
- Prevent session loss.

The Risk of Unstable Applications

When the communication medium changes—for example, from Wi-Fi to 4G or vice versa—many remote access solutions and VPN clients react by disconnecting the VPN tunnel. The same thing happens when a connection is temporarily unavailable, for example, if the user passes through an area with poor cellular network reception. In such cases, the user must set up a new connection and authenticate again—a time-consuming and often aggravating process.

A bigger problem is that most network applications “dislike” changing communication media and result in short-term interruptions. If the system loses its physical connection to the server, network applications can enter an unstable mode—which might lead to data loss.

An important requirement for seamless roaming applications is to ensure application persistence, restoring the state of the application prior to connection loss. Application persistence is also required when a connection changes from a faster to a slower communication mode—for example, from a Wi-Fi network with a bandwidth of 50 Mbit/s to a HSPA (High Speed Packet Access) cellular network connection with 3.6 or 7.2 Mbit/s during download. “In such a case, it is necessary to calm down the application in order to prevent data loss," says Jörg Hirschmann, CTO of NCP. It is also essential to keep the interruption time during the change of communication medium as short as possible.

Redirecting the VPN Tunnel

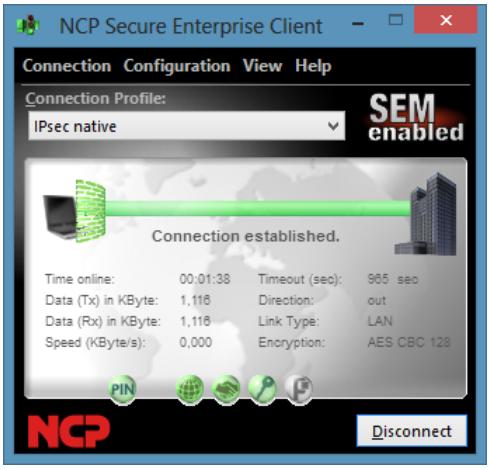
To maintain the VPN tunnel during a change in communication medium, the system must retain its IP configuration. As soon as the IP address changes, the system has to renew the VPN connection. In addition, roaming of VPN connections requires IKE (Internet Key Exchange) protocols 1 and 2 to support redirection of VPN tunnels. IKE protocols are responsible for negotiating the encryption mechanisms and exchanging the keys in IPsec VPNs. With IKEv2, MOBIKE—an expansion that allows changing IP addresses of the host system, for example, during a network interface change—ensures redirection of the VPN tunnel.

Seamless Roaming in a Remote Access VPN Environment

With MOBIKE, a user can establish a VPN connection over a wired LAN in the office, remove the network cable, and continue to use the same VPN connection via a Wi-Fi network in a different room or building. The applications remain untouched by this change, the user experiences no productivity interruption, and network security is never compromised.

Seamless Roaming with NCP

NCP's IPsec VPN client is one of the first client software solutions to support seamless roaming of VPN connections across various media. Working in conjunction with NCP's Secure Enterprise VPN Server, this robust solution ensures that in the event of a network interruption the VPN tunnel remains in place until a physical connection can be reestablished. The logical connection also remains in place, even if the VPN client does not have access to the VPN server. The client software notifies the user of the temporary interruption of the physical connection by changing the state of the VPN tunnel from green to yellow.



NCP's Secure Entry Client supports seamless roaming.

DPD (Dead Peer Detection) is a process that recognizes when an endpoint becomes unavailable, or a session is terminated, and subsequently allows a reconnection of the tunnel and/or creation of a new session. During seamless roaming, the software automatically controls the handling of DPD so that neither the gateway nor client terminates the VPN connection during an interruption of the physical connection.

Connection at the Touch of a Button

For VPN access via a cellular network, it's important that the VPN solution automatically reestablish the connection as soon as the network becomes available again. This process must be transparent to the user, both to increase user productivity and to decrease the risk of user-side errors. With the NCP solution, user productivity is further increased, since the VPN client can automatically select the best, appropriate communication medium as specified by the network manager's policies. Ideally, the user only needs to click the Connect button.

Conclusion

In today's mobile business world, seamless roaming is not a luxury. VPN solutions that do not support seamless roaming significantly restrict the work and efficiency of the company's employees—an increasingly obsolete restriction that any organization cannot afford to impose on its workforce.

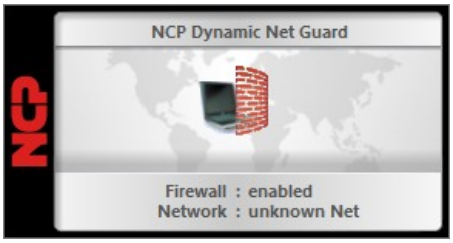
Seamless Roaming in a Remote Access VPN Environment

Checklist for a VPN Client Solution

In addition to support for seamless roaming between networks, you'll want to look for the following features in your VPN solution:

Support for all kinds of networks.
Make sure your VPN solution supports LANs, Wireless LANs, and the largest-possible range of cellular network types, such as GSM, 3G, High Speed Packet Access (HSPA), as well as 4G technologies like Long Term Evolution (LTE).

Adaptive Personal Firewall.
The VPN client's firewall must automatically adapt to the appropriate security settings, depending on the communication medium, such as an insecure Wi-Fi network, a cellular network connection, or a company network. The system automatically adapts the rules after it recognizes the IP address range of the network, the Mac address of the DHCP server, or an NCP FND server. Important note: The firewall must support IPv6.



Essential for any VPN client software, a dynamic firewall automatically adapts the security settings to the available connection medium.

Support for Windows 7 Mobile Broadband.
The mobile broadband interface of Windows 7 allows the use of 3G and 4G cellular network technologies like LTE (Long Term Evolution).

Cooperation with leading security gateways.
A VPN solution should be able to operate with the IPsec or SSL gateways of various third-party vendors (like Cisco, Juniper, Check Point, and WatchGuard).

Support for IPsec and SSL (Secure Socket Layer).
Support for robust industry-standard protocols provides the highest degree of user flexibility.

Fallback option from IPsec to HTTPS.
Firewalls frequently block IPsec VPN connections—which requires the VPN solution to tunnel the IPsec connection via an SSL connection.

Cost transparency and control.
A VPN solution can provide users with an overview of accruing communication costs and enforce limits so they cannot exceed their budgets.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com

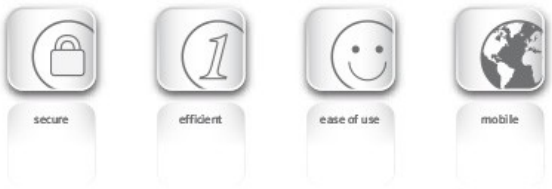
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

Seamless Roaming in a Remote Access VPN Environment

Sources

[1] Strategy Analytics, https://www.strategyanalytics.com/access-services/enterprise/mobile-workforce/market-data/report-detail/global-mobile-workforce-forecast-update-2012-2018?Related#.VVocXmDTabJ

[1] IDC, http://mwaintel.com/wp-content/uploads/2013/11/How_Small_and_Midsize_Firms_Worldwide_Can_Capitalize_on_New_Mobile_Resources.pdf



Next Generation Network Access Technology

www.ncp-e.com