4 Easy Ways to Protect Public Wi-Fi Sessions

Securing anywhere-anytime connections without limiting the freedom of your users.

At the airport, at the coffee shop, or in the comfort of a five-star hotel, Wi-Fi has changed the way people work. Now your organization's employees can be available and productive wherever they are—providing greater benefit to the business. But at what cost?

More than ever, public hotspots put your corporate network and your users' data at risk. And don't think for a second that a password-protected hotspot is safer. Anyone with access to the same network is a potential attacker. Do a search on "hotspot hacking tools," and you'll see just how easy it is for that guy in the corner to be monitoring the area's network traffic.

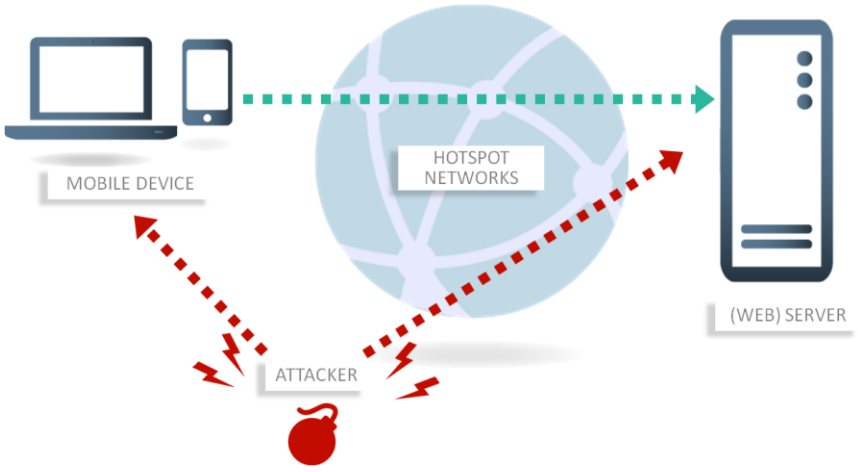
With a VPN, all of the traffic from your device is encrypted—that's an excellent step in the right direction. But there's a moment of vulnerability between jumping on the Wi-Fi connection and connecting to the VPN. And a moment is all it takes for an interloper to listen to traffic to and from the user's device, modify it maliciously, or even harm the device itself—which can ultimately cause serious harm to your corporate network.

Three Degrees of Danger

Although all intrusions can be plenty serious, let's group these threats in three escalating categories.

Listening to network traffic

Without users ever becoming aware of the intrusion, a fellow traveler or a fellow coffee-drinker could be listening to the traffic sent and received by their devices—capturing corporate data and confidential information as well as user credentials or personal information. Even if such data is encrypted, the attacker can save and store the traffic for more laborious decryption measures at a later time.



Modifying the network traffic

Commonly known as a man-in-the-middle attack, interlopers may hack the public hotspot to redirect network traffic—so that the device is actually connected to the attacker's network rather than the public hotspot. (The user typically will not be aware of the intrusion.) Once connected to the user, the interloper is able to intercept all traffic and make changes to network packets, sending modified information to the end device. For example, they can create an e-commerce website that resembles a trusted site and collect confidential company or personal data. Or they can redirect the user to a page for downloading a PDF, which turns out to be a piece of malware.

Attackers have it even easier if they create a "fake" hotspot, calling it something like "Guest Network" or a similar name as the official Wi-Fi network. No hacking is required and no specialized hardware—they can set up the network from a mobile phone. Users on the go may choose this network, especially if they see that it's easy to join and doesn't require a password. As a security professional, make sure your users are aware of this risk and suggest that they always confirm the network name with a representative of the business that's providing the network access.

Of course, network interlopers will look first for unencrypted data, so VPN protection—which provides end-to-end encryption—may almost entirely eliminate the threats of traffic interception.

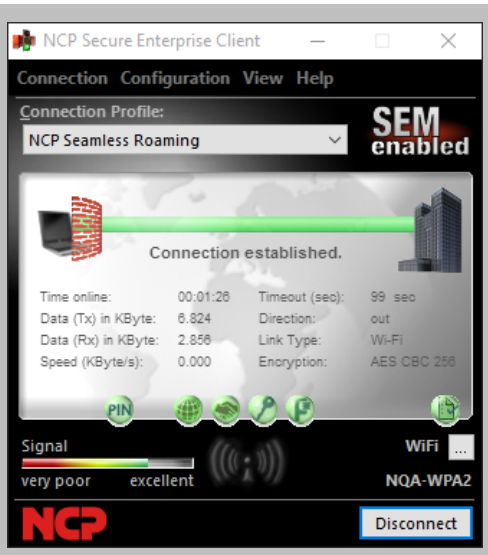
Attacking the end device

In most cases, a personal firewall and additional security controls will prevent attackers from tampering with an end device that's connected to a public hotspot. However, if the Wi-Fi network connection is compromised, attackers may be able to access the end device, adding malware to the network traffic—and ultimately opening a door to your corporate network. Even if your organization's employees are using a VPN (and therefore their network traffic is encrypted), attackers may be able to use the VPN as a tunnel to insert malware onto your servers, threatening the confidentiality of corporate data and the security of corporate hardware.

4 Easy Ways to Protect Public Wi-Fi Sessions

First, the Fundamentals

All solutions for addressing the threats at public hotspots involve two important practices: the use of a personal firewall and the use of a VPN. Whether you're a security manager or an IT administrator, your job is to ensure that your company's employees are using a VPN client that safeguards communication between the end device and the corporate network. To mitigate the risk of attacks, you'll also need to make sure that the personal firewall on end devices restricts network communication on public hotspots, permitting only communication via VPN.



A properly configured personal firewall and VPN client work together to:

- Safeguard confidential information
- Protect both sent and received traffic
- Shield the end device from attacks

Four Additional Measures That Make All the Difference

A VPN and a private firewall go a long way to mitigate the risk of listeners and attackers, but your company's data and your network will be far safer when you add the following measures to your public hotspot security practices.

1. Friendly Network Detection

A robust personal firewall must be able to differentiate secure, or "friendly," networks—such as at the office, at your data center, or in the user's own home—from unsecure, public networks. As the administrator, you can define rule sets that provide the right level of security for each type of network and/or location. To adhere to mobile computing best practices, you'll want to configure the firewall to block all traffic except VPN communications on public hotspots. But when users are at their office or on company premises, there's no need to burden them with the extra steps or the latency of a VPN, so you can configure the firewall to automatically permit unencrypted traffic at those locations.

2. Secure Hotspot Logon

When your users want to hop on a Wi-Fi network, they typically need to open a browser and agree to the terms and conditions of the hotspot provider. But with a properly configured personal firewall that detects an unsecure network, the device will only permit traffic over VPN—so the hotspot logon will be blocked.

NCP has created a secure and easy way for users to log on to public hotspots, without opening up their communications to interlopers.

Here's how:

- The user selects the public Wi-Fi network.
- The NCP VPN client determines if the network requires a logon.
- If a logon via browser is required, the NCP client opens a restricted browser window, and the NCP client's firewall only permits access for this specific browser. During the logon process, users are prohibited from specifying a different URL or changing options, and any configured proxy is ignored.
- As soon the logon is successful, the NCP client detects the Internet connection, establishes a VPN connection, and—once again—blocks all other network traffic.

3. Network Access Control (NAC), or Endpoint Protection

As soon as the VPN client establishes a connection to your organization's network, it's important to confirm that the end device is healthy. With the NCP Secure Enterprise Solution, the NCP client can check the operating system, assess the status of the device's security tools and protections, and integrate with anti-virus/malware-detection software to determine if your network could be compromised by a connection to the end device.

In the event of any abnormality, the client will restrict access to the VPN. For example, if an update to the device's anti-virus utility is required, the NCP client will limit access only between the anti-virus update server and the end device. If malware is detected, or if other threats exist, the NCP client will disable the entire VPN connection immediately, preventing infected devices from causing harm to your network.

4. NCP VPN Path Finder Technology

Some hotspot providers only allow browsing on the public network—typically DNS, HTTP, and HTTPS. And they often block ports that are used by native VPN protocols, such as IPsec and L2TP, thwarting user efforts to access their company network over a VPN.

With the help of VPN Path Finder technology, available with the NCP Secure Enterprise Solution, the NCP client easily overcomes this obstacle. If it detects that the hotspot has blocked native VPN protocols, the VPN client automatically switches to a modified mode (emulating HTTPS) and sets up an end-to-site tunnel to the company network—creating a holistic IPsec-based implementation of your organization's security policy, without requiring any action on the part of the user.

Conclusion

As the employees in your organization enjoy the freedom and efficiencies of working wherever they happen to be, it's crucial that they understand the risks of connecting over public Wi-Fi networks—particularly when they're connecting to your corporate network. Make sure that they know to confirm the network name and access steps before joining a hotspot. Make sure they've activated a personal firewall that prevents hotspot network access except over the VPN. And make sure that they're equipped with a VPN client—such as the one from NCP (which includes a firewall)—that provides easy and secure hotspot logon, robust endpoint protection, and automatic switching when a hotspot blocks native VPN protocols.

To learn more about the best balance between corporate security and mobile user productivity, contact **www.ncp-e.com**.

About the Author

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has ten years of experience in the networking and security industry, as well as expertise in SSL-VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP. He also provides the company's key accounts with pre- and post-sales technical support for their remote access security solutions.

About NCP engineering

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their secure remote access and to overcome the complexities of creating, managing, and maintaining network access for their staff.

Headquartered in the San Francisco Bay Area, NCP serves 35,000+ customers worldwide throughout the healthcare, financial, education, and government markets, as well as many Fortune 500 companies. In addition, the company has established a network of national and regional technology, channel, and OEM partners to serve its customers.

For more information about NCP's remote access VPN solutions, visit www.ncp-e.com.
You can also reach us on our blog, VPN Haus, or on Twitter at @NCP_engineering.

Next Generation Network
Access Technology

www.ncp-e.com