WHITE PAPER

Work from Home: Secure and Scalable Connectivity Strategies

Table of Contents

WHITE PAPER

Work from Home: Secure and Scalable Connectivity Strategies

By Jeff Ebeling CISSP, CCSP

Most security conscious organizations have traditionally handled remote workers with full tunnel virtual private networks (VPNs). Widely considered as the most secure method to provide remote user access to sensitive internal data and systems, VPNs are a practical and popular solution when less than 20% of the workforce requires such access. In this traditional use case, most of the traffic on the VPN was destined for internal systems.

The positives of the full tunnel VPN approach are obvious:

- Highly private and secure, complete control of dedicated infrastructure is possible
- Centralized visibility and control of all remote client traffic
- Support of all ports and protocols[1]

However, with the rapid transition to heavy reliance on cloud-based services like Zoom, Teams, WebEx, Exchange Online, SharePoint/OneDrive, Box, Slack, Salesforce, Workday, GitHub, G Suite, and others, these traffic patterns have dramatically changed. Work from home and use of Software-as-a-Service (SaaS) are extremely common practices that continue to increase.

The COVID-19 pandemic forced most organizations to quickly adjust to having anywhere from 50% to 100% of their employees working remotely. Many of these employees may never, or only infrequently, return to local offices. In today's environments, the practicality of the full-tunnel VPN approach needs to be reexamined and alternative architectures should be seriously considered.

Option 1: Expand Existing Full-Tunnel VPN

One approach to addressing increased user traffic is to maintain the current architecture with its associated benefits and simply purchase massively increased VPN infrastructure.

Here is a summary of the downsides to maintaining this approach in today's world.

- **High infrastructure cost:** Dedicated, highly available VPN infrastructure is costly to maintain.
- **Greatly increased bandwidth costs:** Depending on the business and their cloud service adoption rates, anywhere from 50% to 95% of the traffic traversing the VPN is HTTPS traffic destined for external resources. Internet bandwidth capacity will need to be increased at the data centers where the VPN concentrators reside because most traffic will traverse the corporate border twice rather than not at all.
- **Poor performance:** End users experience poor performance for this traffic, as most corporations do not maintain globally distributed, highly available VPN networks and even if they do, they are likely not collocated at internet exchange points with peering support.
- **Reduced security:** If the VPN networks are provided by a third party (possibly improving performance and resilience), it will likely be multi-tenant, thereby reducing some of the perceived security benefits of the full tunnel approach.
- **Inbound firewall rules still needed:** This approach still requires admittance of arbitrary source addresses, making inbound VPN connections and possibly HTTPS connections to and through the firewall.

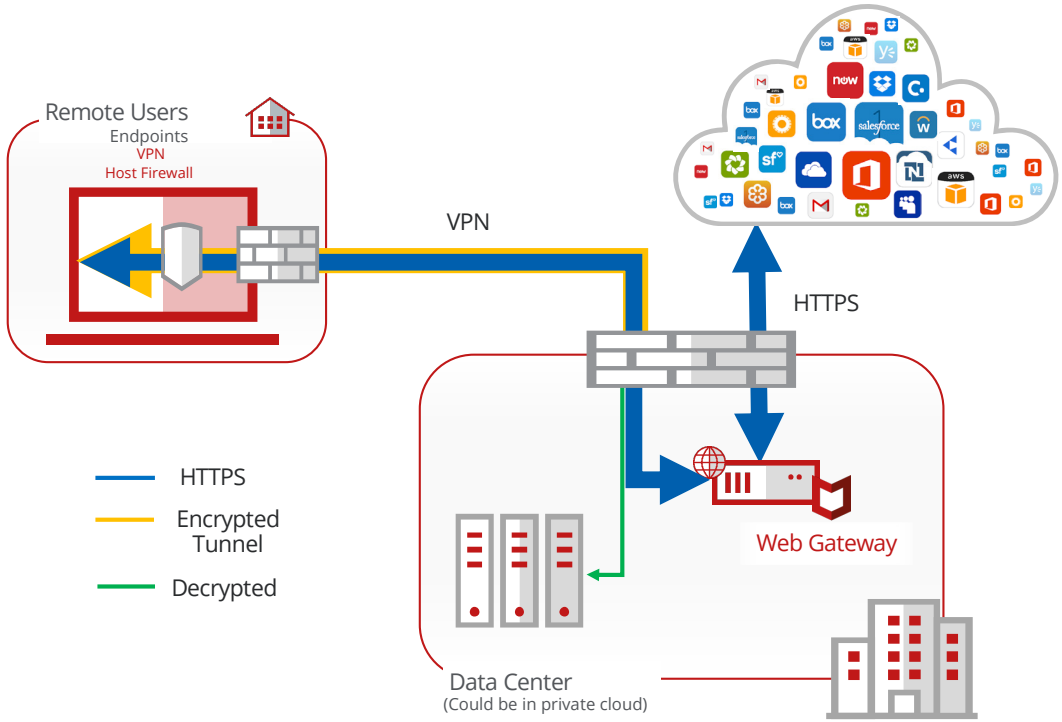

Figure 1. Full-tunnel VPN traffic flow.

Option 2: Use "VPN Alternative"

Another approach that is currently being heavily promoted is to use an additional agent to direct most, if not all, traffic to a globally distributed cloud service that provides multiprotocol support and potentially some next-generation firewall capabilities. The solution eliminates the need to massively increase VPN capacity and internet bandwidth. The approach potentially can simplify firewall inbound rule requirements and possibly permit the replacement of one agent for another. It also allows for the use of corporate egress IPs for selected traffic. However, in most cases, the existing VPN agent needs to be retained.

While this approach is certainly viable, it adds significant additional concerns:

- **VPN often needs to be retained:** If all protocols are not supported, the VPN agent, infrastructure, and its management cannot be eliminated.
- **Additional infrastructure required:** Secure connections from the cloud service now must be terminated on a system (often managed by the provider) in the data centers and/or clouds hosting the customer applications.
- **Reduced performance for internal applications:** Performance of internal applications is significantly worse than it would be with a direct client-to-site VPN connection due to more hops, longer routes, and multiple additional layers of otherwise unnecessary encryption and decryption.

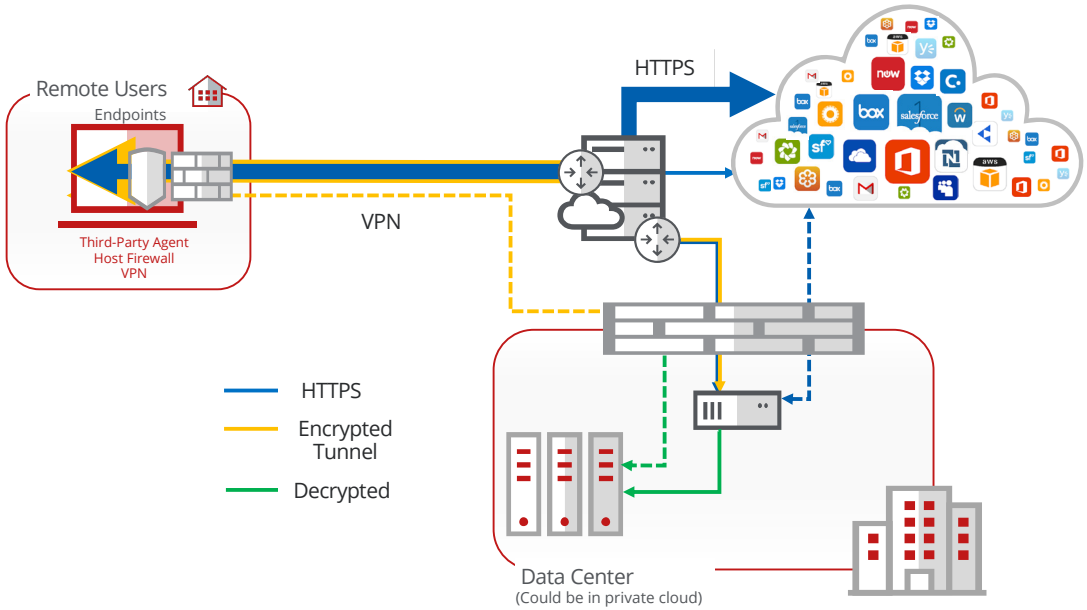

Figure 2. VPN alternative traffic flow.

- **Reduced performance for HTTPS to the public cloud:** In this case, performance is worse due to added encryption/decryption on traffic that is already more than sufficiently protected with Transfer Layer Security (TLS) from client to server.
- **Authentication challenges:** While authentication can be client to service based on certificates or Security Assertion Markup Language (SAML), certificates may be associated with the machine rather than the user.

SAML, against a shared service, from an unknown IP, requires a prompt and was not designed for accurate authentication to a gateway handling multiple protocols and server destinations.

- **Increased reliance on service provider availability:** This solution adds more reliance on the availability of the service for all traffic. If the service becomes unavailable, not only are users cut off from corporate resources, they are also either cut off from accessing external resources or permitted unfettered access to these services. As such, the vendor's historical availability metrics and service level agreement (SLA) should be closely examined, as should their ability to detect and stop distributed denial-of-service (DDoS) attacks to the service.
- **Increased reliance on service provider protection and inspection capabilities:** Most cloud services provide little more than signature antivirus and reputation services for real-time threat protection. Out-of-band sandboxing and remote browser isolation are often offered to compensate for a weak level of protection that is no better, and frequently less effective, than what modern endpoint antivirus can provide. These solutions are expensive and/or ineffective for stopping zero-day and rapidly morphing threats in real time.

Option 3: Split HTTP/S to Cloud Service

Another more practical option is available today from McAfee. The solution uses an agent to direct most, if not all, HTTP and HTTPS traffic to a robust (99.999% availability SLA), globally distributed cloud web gateway service. The small remainder of the traffic can be split at the client and continue to be handled via the existing VPN infrastructure. The solution eliminates the need to massively increase VPN capacity and internet bandwidth while potentially improving the security posture for all public cloud traffic.

There are many benefits to this approach, as opposed to splitting the traffic in the cloud or at the data center.

- **Improved performance:** There are shorter routes to internal resources and no added layers of encryption. The service is globally distributed and enables organizations to take advantage of peering capabilities.
- **Added context:** The client provides additional context about the web request for use in making filtering decisions. This valuable context can be transparently added to any application using standard HTTP/S protocols even if the application is not proxy aware.
- **Full VPN compatibility:** A centrally managed client can be compatible with existing VPN technology for handling non-web traffic. Web traffic can still be adequately controlled through centrally managed, host-based firewalls provided by the client operating system (OS) vendor or the endpoint security vendor.

- **Improved security:** McAfee offers industry leading real-time protection with its proprietary Gateway Anti-Malware engine. The engine uses emulation-based sandboxing and machine learning-enabled behavioral code analysis to detect and block in real time, not only 95% of what other vendors require out-of-band sandboxing to detect, but also 95% of the browser-based exploits that sandboxing has no possibility of detecting or blocking. McAfee competitors require add-on browser isolation technology to stop these browser-based exploits. More information on the Gateway Anti-Malware engine can be found here: https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-gateway-anti-malware.pdf
- **Egress IP control:** The McAfee client also provides the ability to direct a portion of the web traffic back through a cloud-based or on-premises gateway that can provide a corporate-owned egress address for compatibility with services that use egress address as an admittance factor. This traffic could be sent inside the VPN tunnel or outside of it.

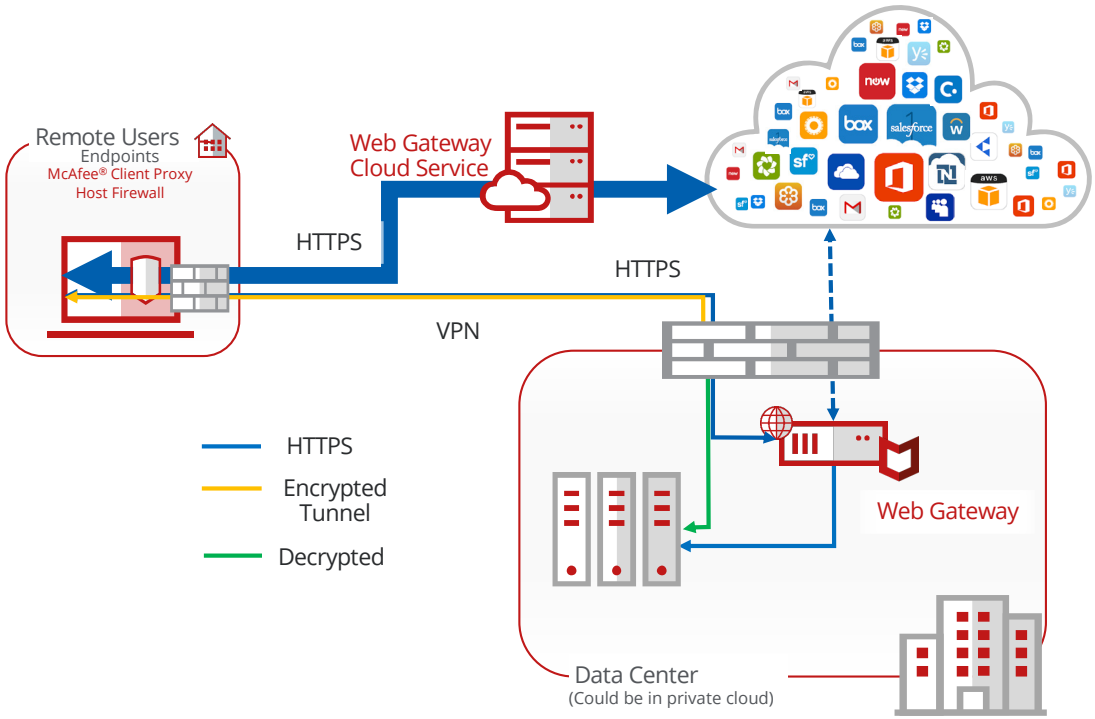

Figure 3. Split HTTP/S traffic flow.

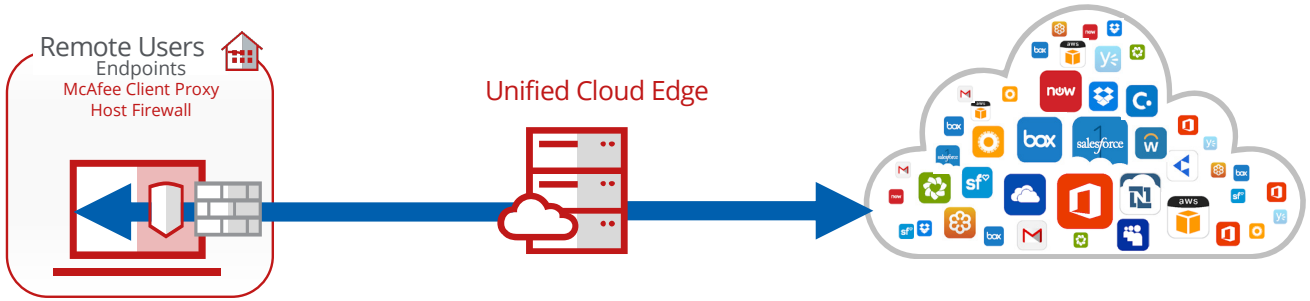

Figure 4. No VPN traffic flow.

There is still the downside of infrastructure to support corporate egress IP and client admittance, but this is true with any complete solution. Also, the infrastructure only needs to support a small portion of the traffic, and all HTTP/S traffic is tightly controlled.

A variation on this option is to dramatically reduce dependence on the VPN and make all commonly used applications directly available. This eliminates the need to expand VPN capacity, and the VPN can remain full tunnel (Option 1) when internal access is needed. Most of the time, users would access the web directly through the cloud service as restricted by the service and, potentially, a host-based firewall, as seen in Figure 4.

Other Scenarios and Considerations

Exclusively On Premises

For those entities that would prefer to maintain an architecture that relies solely on dedicated services, the solution also can work with customer managed on-premises or private cloud infrastructure. While this maintains full, centralized traffic visibility and control at the firewall, the customer does not get the benefit of a robust service provider managed and updated service.

The client can support providing context about the user, their directory groups, the system, the OS, and the process making the web request to the service for use in making filtering decisions. Furthermore, the client can run as a network shim and add this valuable information while transparently proxying traffic from any application using standard HTTP/S protocols.

The client can still be fully compatible with existing VPN technology for handling non-web traffic, and non-web traffic can be adequately controlled through centrally managed host-based firewalls provided by the client OS vendor or the endpoint security vendor.

Bandwidth costs are not significantly reduced, though VPN capacity would not need to be expanded. This approach is also less attractive due to the many of the same performance issues mentioned with current solutions relying solely on VPN backhaul.

Service Infrastructure

A cloud service is only as useful as the robustness of the infrastructure providing the service. McAfee offers a 99.999% availability SLA. Even with recent massive surges in demand, McAfee has maintained over 99.99% availability while our primary competitors have not even been able to consistently maintain 95% in all regions. In addition, a cloud service should be designed to provide low latency using primary globally distributed peering points of presence (PoPs) located at internet exchanges. See: How Peering PoPs Make Negative Latency Possible. An excerpt from that paper demonstrates the value of "bigger pipes" with peering versus going through a generic route or even a more proximal PoP without peering.

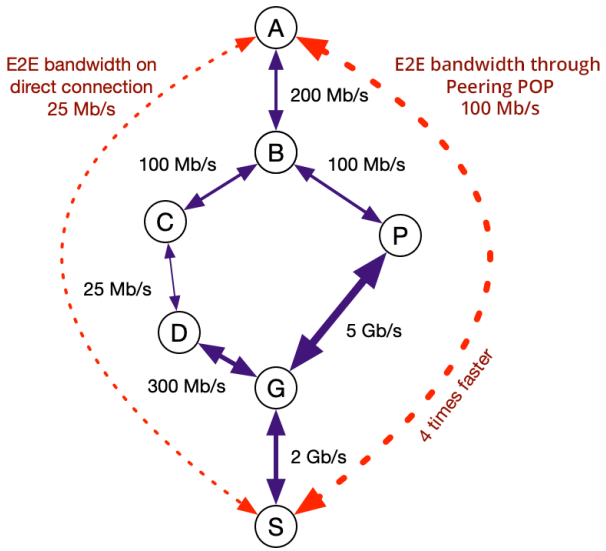

Figure 5. Peering PoP latency advantage.

Service Capabilities

It is important to consider the comprehensive features and functions that are required for filtering the redirected HTTP/S and how they will be managed. Secure Access Service Edge (SASE), as defined by Gartner, is a security framework for enabling secure and fast cloud adoption. This framework ensures that both users and devices have secure access to cloud applications, data, and services anywhere, any time.

As organizations seek to accelerate growth through use of the cloud, more data, users, devices, applications, and services are used outside the traditional enterprise, which means the enterprise perimeter is no longer a location. It is now a set of dynamic edge capabilities delivered when needed, as a service from the cloud. See: What is SASE?

In the context of SASE, with endpoints accessing the public internet from uncontrolled networks, there are three important, interrelated, security functions for an HTTP/S web filtering service:

- **Secure web gateway:** Authentication with HTTPS decrypt, real-time content filtering, activity control, application control, and web threat prevention.
- **Cloud access security broker (CASB):** Visibility and control of sanctioned and unsanctioned third-party applications and corporate specific applications and services. For sanctioned applications, the solution should be fully capable of handling traffic from any device (managed or unmanaged) from anywhere, using a combination of application programming interfaces (API), forward proxy, and reverse proxy capabilities (all are needed). In many cases, the CASB will also be used for configuration and monitoring of security controls for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).
- **Data loss protection:** Inspection of traffic to identify and control uploads and downloads of sensitive data.

A unified console should be available to manage these capabilities, and it should not be necessary to compromise functionality in any area. McAfee offers a cloud-native solution comprised of industry-leading, full-function technologies covering all three areas. This provides for effective and converged, cross-functional, policy creation, policy enforcement, and incident management using a single login to a single console.

Client Capabilities

All solutions require the use of a client agent of some form, and the capabilities and limitations of the agent should be carefully considered. Important features to assess:

- **Application agnostic:** Redirect traffic from any HTTP/S application and supply authentication and context for that traffic even if the application is not proxy aware.
- **Network aware:** Adjust to network surroundings allowing for captive portals and proxied environments and operating accordingly.

- **Highly tamper-resistant:** Client and its redirection capabilities cannot be independently altered or disabled, even temporarily, by an end user. Administrator controlled temporary bypass is available for simple issue identification.
- **Provide additional context:** Process name, system name, operating system, and original IP are transparently available with all transactions from all web applications for use in filtering decisions.
- **Completely transparent user identification:** Accurate and consistent, per transaction, user, and group identification, that is independent of application or the application's ability to authenticate to a proxy or service.
- **Selective redirection:** Simultaneous traffic redirection to multiple proxy locations, allowing for bypass, localization, and use of corporate egress IPs as needed.
- **Central management:** Client should be centrally managed with simple deployment and cloud-based dynamic policy update options.

Conclusion

Enabling remote worker productivity while maintaining information security is a challenge for many organizations. Secure and cost-effective alternatives to expanding the cost and complexity of VPN infrastructure are available today from McAfee. The current solution provides superior protection from web threats and data loss, with industry-leading high availability and a greatly improved user experience.

Key Takeaways

- Cost reduction is possible while simultaneously improving security posture.
- Better network performance, reliability, and user experience can be delivered.
- VPNs are still practical and useful for providing secure access to internal systems.

1. Most of the traffic on a full tunnel VPN is now destined for the internet using the HTTPS protocol. SaaS traffic that is not HTTPS is mostly UDP for audio and video-based collaboration tools. This traffic should be allowed to route direct in order to maintain performance, and therefore is not a focus of this paper.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com