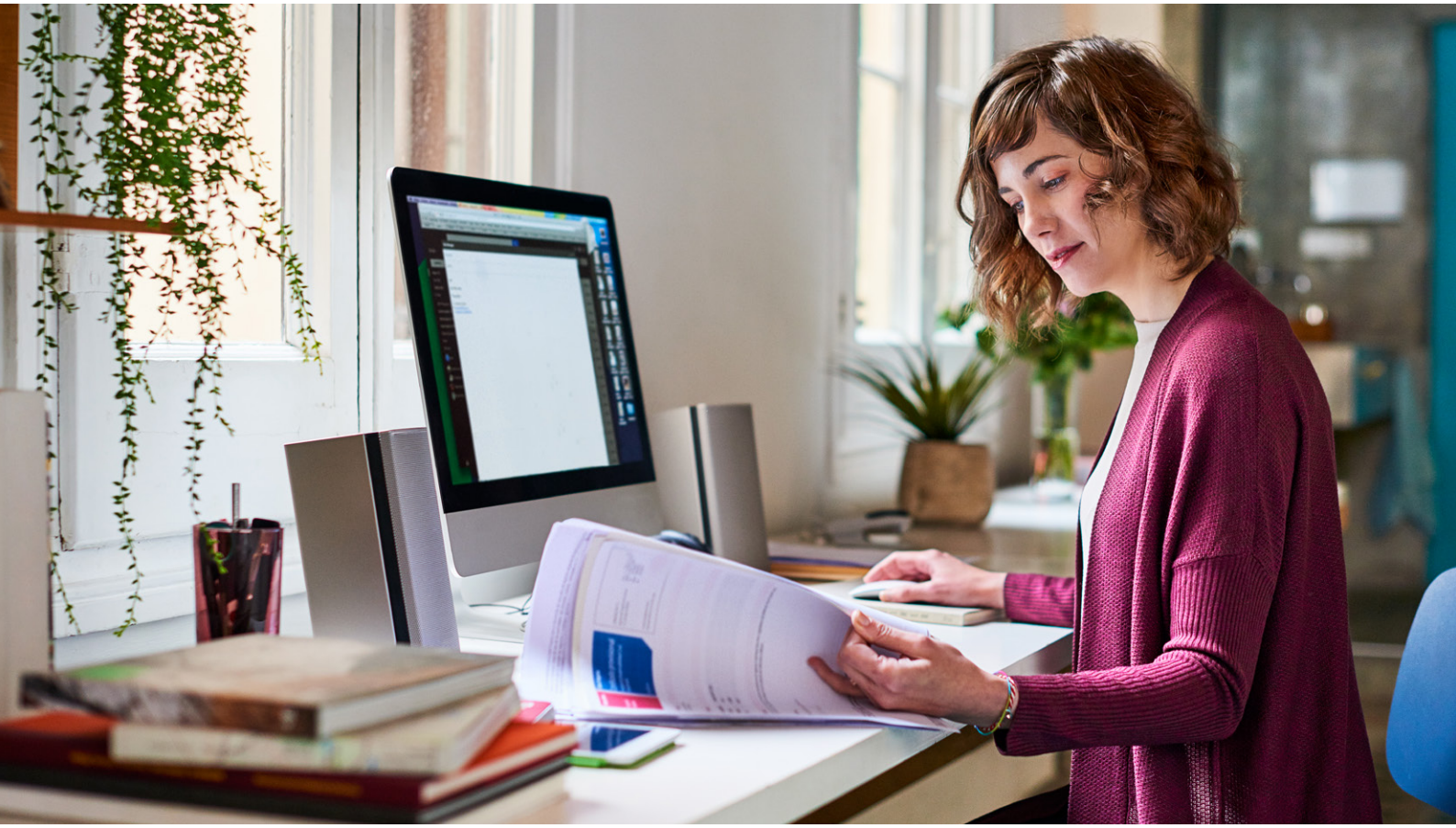
NOKIA



Solution brief

Working from home via a secured network connection

Secured access to business and cloud hosted applications for the teleworker

NOKIA

Contents

NOKIA

Teleworking is a growing phenomenon as exemplified by its growth over the last decade. The COVID-19 pandemic has dramatically increased home-based teleworking putting an unexpected strain on enterprise networks and driving the growth of cloud-hosted applications such as Unified Communications (UC).

Concerns about security, performance, productivity, and cost efficiency all come up when enterprises are asked about their strategy to enable teleworking across their employee base and all can be mitigated by a managed SD-WAN based teleworking solution.

The shift toward home teleworking

The percentage of remote workers has increased dramatically over the last five years and continues to rise. Enabling teleworking has shown to increase employee's morale, productivity, and well-being, while also reducing the costs to the enterprise of maintaining many branches.

With the COVID-19 pandemic, teleworking has accelerated dramatically which has forced enterprises to act quickly, to enable teleworking for a large number of their employees in their home environments whist maintaining security and cost.

This shift to home teleworking has also put a strain on the network itself as the use of collaborative cloud-hosted SaaS and UCaaS applications have grown beyond expectations.

In addition, other cloud-hosted applications, such as Contact Center as a Service (CCaaS), have also shown tremendous growth as home-based contact center agents represent a growing segment in this new environment.

Enterprises need to act swiftly to address these changing business requirements, including:

- Using simple, secure, and cost-effective solutions to enable home teleworking
- Enabling home teleworking without compromising network and business security
- Providing home-based IT policies that define access entitlements to any cloud-hosted applications (e.g. UCaaS, CCaaS, IaaS/PaaS) each teleworker needs to be productive
- Providing access to their legacy data center and private cloud-hosted IT applications
- Ensuring that the network can scale to accommodate the massive increase in network endpoints and the increased consumption of cloud native SaaS, UCaaS, and CCaaS applications

Benefits of managed SD-WAN services for home-based workers
Assured UCaaS, CCaaS performance (Zoom, Teams, WebEx, etc.)
Extend corporate security policies to the home environment
Seamlessly access SaaS and private IT services
Compatible in any home environment
Limited network disruption or process change
Quick and easy to connect and authenticate at home with zero-touch provisioning (ZTP)
Support for both Wi-Fi and wired LAN
No impact to home-based connectivity

Nokia Cloud Managed SD-WAN Service

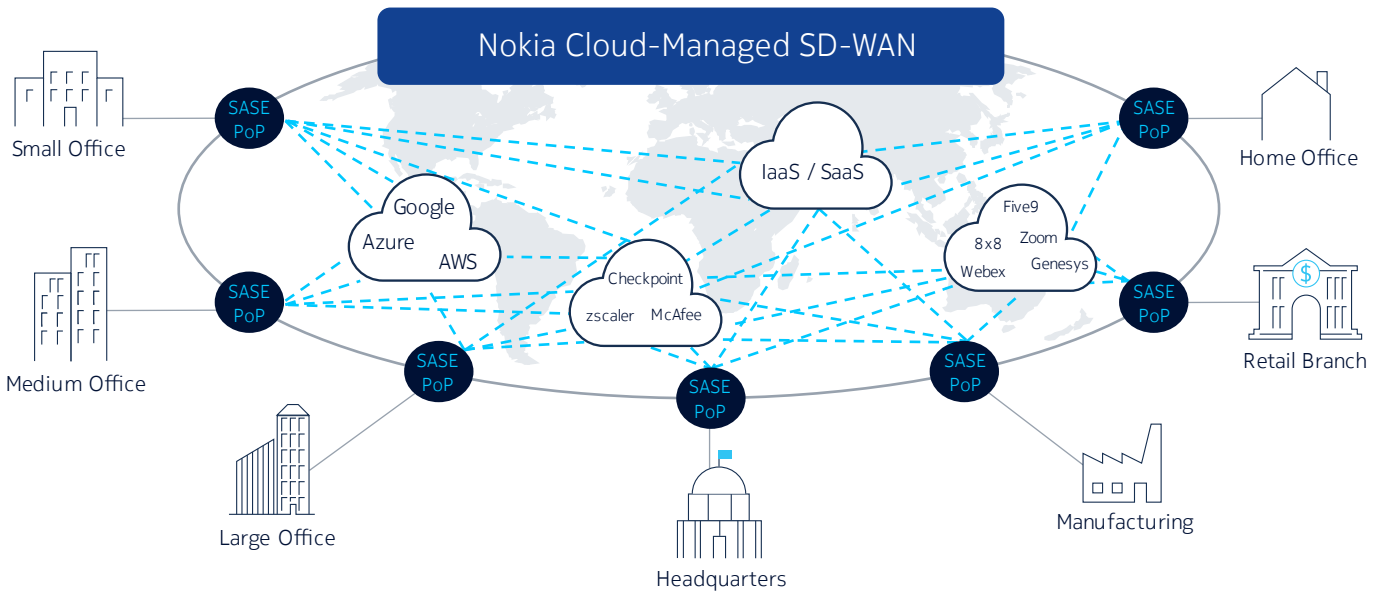
The Nokia Cloud-Managed SD-WAN Service (Nokia managed SD-WAN) is ideally suited to meet the demands of enterprise networking for both in-office and home working employees due to its ability to deliver boundaryless networking across the traditional branch locations, deep into the public cloud where IT applications reside and to any homeworking sites via an encrypted and fully managed Internet or mobile broadband connection.

As a managed service offering delivered to enterprises from their trusted Managed Service Provider (MSP) or System Integrator (SI), it fits with the market trend across all enterprise verticals of their preference for SD-WAN to be provided 'as a service.' This trend is acknowledged by leading analysts' companies, including IDC and Appledore, whom both see the market shifting to managed solutions.

With this 'managed network-aaS' trend, a more collaborative operating model, co-manage, has emerged. With co-manage, it's the responsibility of the MSP/SI to operate the SD-WAN platform (a task Nokia works alongside them with), ensuring the that network service platform is maintained and hosted with capacity for growth, etc. and the enterprise maintains a level of control over the day to day management of their WAN. At its simplest form, this could be limited to visibility into the running conditions of the WAN and the applications or could be more hands-on with shared responsibility for moves, adds, changes and deletions on the WAN.

This allows the enterprise to set a responsibility matrix that meets their need, such as having the visibility and control to affect network or application performance on a location by location basis, and to let the MSP/SI own the changes that affect overall WAN performance and/or maintenance tasks such as network-wide software upgrades.

Figure 1: Nokia Cloud-Managed SD-WAN Service with SASE PoP for cloud and SaaS



NOKIA

Application-aware networking

As an application-aware solution the Nokia managed SD-WAN service delivers full visibility and control of each of the enterprise applications traversing the WAN, with equal visibility of traffic at the traditional branch locations and the emerging teleworking home office deployments. This creates a single IT management domain that reduces the complexity of managing branch and home working locations. This is more efficient than traditional remote access (IPsec VPN) solutions which are managed today via separate IT management toolsets.

The service operates with layer 7 visibility into the enterprise application via an inbuilt Deep Packet Inspection (DPI) engine enabled at each WAN branch and home location. This allows the MSP/SI and enterprise to create network and application policies that set the priority, security and reachability of any application or network user. An example of this is the enterprise Customer Relationship Management (CRM) application. A policy can be created that that prioritizes CRM over and above general office traffic. This prioritization can be extended into groups of applications, for instance, an application policy group called "priority-business" could be set up with the enterprises CRM and Unified Communications suite prioritized as a group over traffic such as office365 or general Internet.

This application-aware networking capability can also be extended further to segment or isolate certain application traffic into secured network slices. For instance, the finance applications could be policy managed to only be available (network reachable) by members of the finance team, or the same with HR, engineering or sales applications and user groups.

Depending on the priority and sensitivity of this traffic (or of any other), the SD-WAN service can encrypt the application flows using IPsec and forward over the available WAN uplinks, be they private MPLS or public Internet.

Reaching deep into the cloud

With digital transformation most enterprises are moving from a purely private data center IT environment to a cloud first approach with a preference for Software as a Service for any new application purchases and a migration strategy for existing applications to be rehomed to either one or more public clouds.

As with any relocation offsite, it's critical that information security is viewed holistically, and that includes the network. With the Nokia Cloud-Managed SD-WAN Service this is inherently provided through the deployment of SASE-PoP locations at the cloud edge.

SASE or Secure Access Service Edge[1] was coined by Gartner as the delivery of both SD-WAN and Security functions as a managed service, and Nokia has adopted this framework for connections to the public cloud for both virtual compute and application (SaaS) use cases.

Gartner predicts that by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at the end of 2018.

40%

As part of the service, Nokia has invested in SASE-PoPs (Points of Presence) in key locations that facilitate the secure interworking of the enterprise WAN to the cloud and SaaS applications. The feature provides flexibility to utilize either public Internet or private connection services (express links) to the major cloud providers and either direct to SaaS or via Cloud Service Access Brokers (CASB) services such as Zscaler or Checkpoint CloudGuard.

1 https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/

The benefit to the enterprise is that any connections to the cloud or SaaS applications inherit the same application-aware network and security policies that are implemented by the enterprise on their SD-WAN service.

So, for cloud-based deployments, the business/information security rules are identical to those implemented at the traditional branch locations, this means a single IT management domain at all the enterprises physical and virtual wide area network endpoints.

Secured corporate access at the employees' home

The MSP/SI partner can empower their enterprise customers to enable home teleworking across the corporate network by deploying an SD-WAN gateway (Nokia 7850 NSG) in their home. The deployment leverages an easy zero touch provisioning (ZTP) process that simplifies the onboarding of the employees' home to the corporate network utilizing their existing broadband service.

With a range of 7850 NSG models available, the MSP/SI can right size the installation to the bandwidth and functional needs of the home environment. Deployment of the 7850 NSG is compatible with any home environment and is agnostic to the home broadband access technology used (e.g. Cable, DSL, GPON) as it's deployed directly behind the Internet residential gateway/modem and connected to a LAN port. Some 7850 NSG variants also support Wi-Fi enabled devices and can create a private 'business' Wi-Fi network in-home for the employee that is physically separated from any existing residential Wi-Fi networks.

Once deployed in the home, the 7850 NSG appears on the enterprise SD-WAN, via the customer portal, and has the same visibility and control of enterprise application traffic as what's available at the traditional branch. This connection from the home-office LAN to the corporate SD-WAN is fully secured and hardware encrypted and is dedicated to the teleworker's IT-sanctioned devices and applications; it becomes a "Branch at Home".

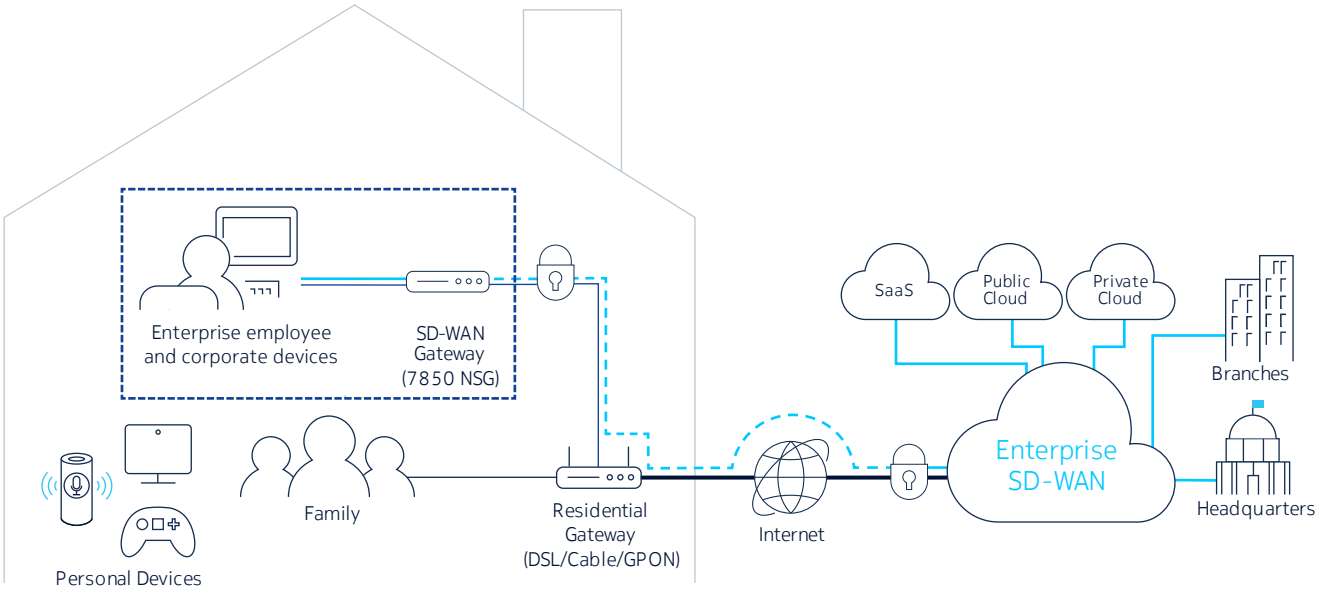
Steps to prepare the 7850 NSG in the home for service activation are:

- Unbox the 7850 NSG and place in work environment
- Connect and turn on the power
- Connect the 7850 NSG's WAN uplink Ethernet port to the Internet modem LAN port
- Connect the IT sanctioned business devices to the 7850 NSG LAN ports or Wi-Fi network.

The teleworker can initiate the secure activation of the service at home with zero touch provisioning (ZTP) using zero, one, or two factor authentication schemes. Two-factor authentication is very common with the secured authentication approach and operating as follows:

- The employee will receive a corporate email on their device (laptop) which they have connected to a LAN port on the SD-WAN gateway. This email will provide a link to the SD-WAN activation page that will generate a challenge activation code (factor 1)
- The activation code is sent via text to the employees' mobile phone and once input (factor 2), the activation of the service commences.
- The 7850 NSG is authenticated, the employees' home location profile is downloaded, and the Branch at Home is connected to the enterprise WAN.

Figure 2: Secured corporate LAN at the employees' home; "Branch at Home"



Branch at Home vs. Remote Access VPN

The traditional way to connect remote employees on the move has been to implement a remote access VPN service. This is provided by a VPN terminator installed at one or more centralized corporate locations, and a software VPN client installed on the employee's device. When required, the employee starts the VPN client, connects to the VPN terminator and authenticates an encrypted path over the Internet to the corporate WAN.

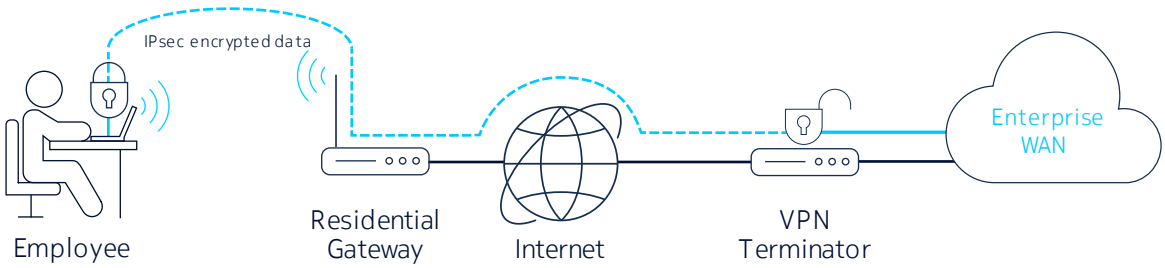
For employees on the move, frequent travelers etc. this has been a workable solution when they stop off at hotels, the airport or at customer sites and with the COVID-19 pandemic this has been a method for connecting home-based employees to the network.

Although well-established there are drawbacks to this remote-access approach that the Nokia Managed SD-WAN powered Branch at Home features mitigate.

Client based remote access

Deploying an enterprise solution based on remote access VPN using a client to initiate an encrypted network tunnel back to the corporate WAN is commonplace. This has been the go-to technology for employees on the move and has seen expansion as businesses needed a solution to the new normal business environment where the majority of the office workforce is working from home.

Figure 3: Traditional remote access VPN deployment



For the employee the process is simple; they start the VPN client on their device, authenticate to the VPN terminator and an encrypted tunnel between the device and the terminator is created that hides the business data from the local Wi-Fi and public Internet. However, there are complexities with the solution though which we will breakdown into IT management and employee domains.

IT Domain

On the corporate side there is expense in both procuring VPN terminator hardware and licensing capacity with a balancing act to purchase only what's needed, as in, the number of employees that can connect simultaneously. With on the move 'road warriors' using the solution intermittently it was manageable and cost effective with dimensioning rules of say 30% (peak active connections across the employee pool).

But with the pandemic, businesses have had to significantly invest in both increased licensing and VPN terminator capacity as the business environment now calls for a greater number of employees connected for longer, in some cases a whole working day, forcing dimension rules up to 90%.

Other complexities and cost of this solution relate to the IT management of the environment. There are the authentication costs including another challenge password application (probably on the employee phone) and the active directory/LDAP integration costs.

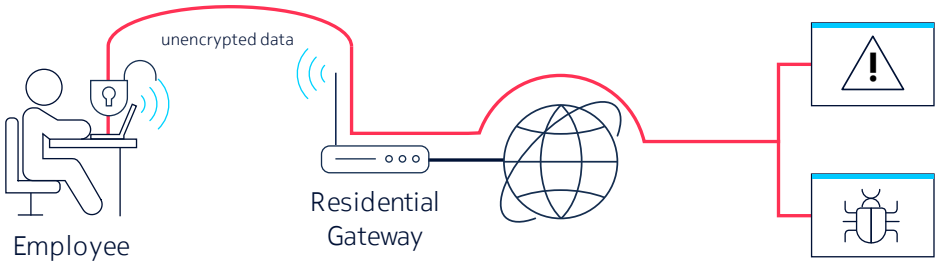
Additionally, there is the complexity of matching the IT based network and security policies between users connecting remotely and those in the office on the LAN. These include rules on what can and can't be done remotely, what extra application level authentications are needed for business sensitive system access, and how general Internet and business SaaS applications accesses are managed.

Employee

For the employee the solution provides access to their business applications whilst the VPN client is enabled, however when the client is inactive, they and their business device are directly connected to the public Internet.

Taking the same example in figure 3 above, the employee is now connected to their home/consumer Wi-Fi network with any Internet bound traffic exposed to online threats. To mitigate this the business needs to invest in a suite of device endpoint protection services, be that anti-virus, safe web surfing browser extensions and on device firewall functions. And more importantly a robust and consistent process that ensures that the endpoint protection suite is up to date.

Figure 4: Employee at home with an inactive remote access VPN client.



These additional protections assist in reducing the risk of the business device being vulnerable to the Internet however they come at a cost; be that additional licenses, IT overhead in management and an impact on the device performance.

Another operational complexity relating to the pandemic enforced working from home environment is the blurring of the line between personal Internet use and that of business use.

In the office it's easy to implement strict rules on what can and can't be accessed on the Internet via proxy servers and commercial firewalls. This might mean that certain Internet websites, be that shopping, cloud storage or gambling etc. are blocked.

That's not the case with business devices at home that are, by factor of using consumer Internet services, on the public Internet before they are on the private business WAN. This can blur the line between work and business in the home, and by human nature, can extend to using the business device for personal Internet tasks. Say the employee has been working for several hours, they stop for a coffee at their desk and with the downtime connect to their fantasy football website, on the VPN this is blocked, so they drop the VPN connection visit the site, then check social media etc. When they are finished, they enable the VPN and delve back into their work.

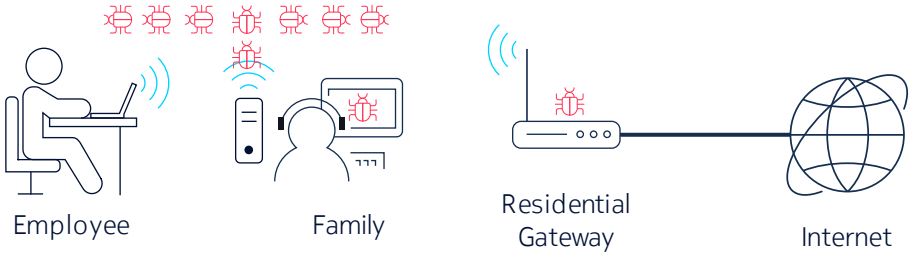
Without going to the HR implications of these actions, for a period of time the business device was exposed to some level of threat, be that visibility to the Internet, cookie tracking or potential infection. It's an extremely disciplined home worker that can completely separate business use from personal use and so there is an increased business risk of client based remote access for home workers.

Another area of risk with remote access via VPN clients is the home networking environment. The quality of equipment used, how up to date it is with firmware and the security levels implemented on the consumer Wi-Fi are not under the control of the business's IT department.

These are shared consumer environments, many with a mix of user, operating systems and device types, and each with their own levels of risk.

For many people their knowledge of Internet threats is focused on what is outside of the home, be that the types of Internet sites they visit or trust levels around any software or files they download. Many don't think about the in-house environment which includes both the implementation of network layer security features and an ongoing process to ensure that they are maintaining the software/firmware levels on their residential gateway and across all devices on their in-home network.

Figure 5: The home network environment



Threats can exist with the consumer Wi-Fi network, be that ensuring that robust Wi-Fi protection/ encryption is enabled and that all devices are running the latest operating system patches and have anti-virus/malware software enabled.

Often overlooked is the residential gateway device. Its installed day-one and runs without maintenance. However, as the main Internet facing device (with the households public IP address) it carries a high risk. There have been malware attacks on residential gateways targeting UPnP or remote access via default ports and passwords that can allow a hacker to silently manipulate the household traffic so its imperative to perform regular updates and ensure best practices on its installation (changing the default passwords etc.) are followed; which is a hard task for business IT team to enforce.

SD-WAN based Branch at Home

By deploying an SD-WAN based home office environment all of the operational complexity issues, the employee usage, and any risks posed by the home network environment are mitigated.

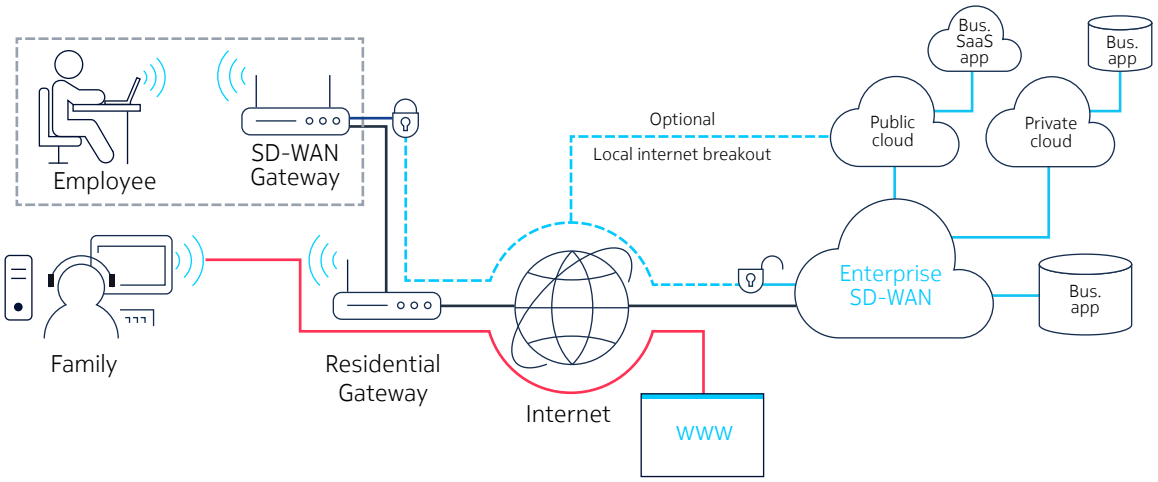
A key difference from client-based VPNs is the network processing. Being the authentication, the encryption and the corporate policy enforcements which with SD-WAN are moved from the employees' device to a dedicated network appliance fully under IT control; the SD-WAN gateway.

This gateway provides a hardware demarcation point where the business traffic and devices are physically isolated away from the consumer Wi-Fi network, home devices and Internet traffic.

Physical connection to the Internet service is provided by a wired Ethernet connection from the WAN port of the SD-WAN gateway to an available LAN port on the residential gateway. The SD-WAN gateway also supports a direct Internet connection, for instance with GPON (fiber broadband) many access service providers deploy a network access device (Optical Network Terminator, or ONT) that is separate from the retail Internet Service Provider (ISP) and their provided residential gateway.

Depending on the local market it may be possible to connect the SD-WAN gateway directly into a separate port on the ONT and purchase a completely separate retail ISP service into the home just for business use but in the example below we depict a shared Internet service.

Figure 6: Nokia managed SD-WAN service; ‘Branch at Home’ with isolation between business and consumer networks



Once installed, the business device(s) are connected to the SD-WAN gateway and are provided with a completely private network segment from the consumer users. These business devices can be hard wired to the gateway via Ethernet or (depending on 7850 NSG gateway model) be connected over a private/ business Wi-Fi network.

The Branch at Home deployment appears on the enterprise WAN exactly the same as a traditional office branch; it can be thought of as a micro-branch.

This means there is a single IT management domain that covers both traditional branch and home locations; the same network control, application visibility, and business and security policies. This results in the employees having an identical networking experience regardless of working in the office or at home. Advanced IT policies based on Zero Trust Network Access (ZTNA) architectures are easily deployed on SD-WAN networks and with Nokia these policies will be implemented at any Branch at Home deployment.

As the business devices are connected to the SD-WAN gateway all decisions on where traffic can go are managed via the central SD-WAN policy portal under the control of the enterprise IT team. This puts control directly into the domain of the IT team and minimizes the opportunity for the employee to bypass business and network policies.

As the business devices are always connected to the Branch at Home network there is no opportunity to bypass the ZTNA and corporate policies that there was with the remote-access scenario above and to use the work device for personal Internet (fantasy football etc.). The coffee break now involves stepping away from the work device, going to a family PC on the consumer network and getting work/life downtime completely separated from the Branch at Home environment.

Network functionality provided by the SD-WAN gateway can, depending on licensing applied, be as rich as that of the larger offices. Functions such as stateful firewall, IDS/IPS, application aware prioritization and routing etc. can be added to the inbuilt hardware-based encryption capabilities resulting in a home network environment that is as secured as a branch location.

An example of this functionality, and depicted in figure 6, is a network policy to allow the employee to connect to public cloud hosted business SaaS applications (office365 as an example) via a local Internet breakout at the Branch at Home. The connection will still be secured via the stateful firewall and security policies however the cloud hosted application use by the employee is more efficient as their path to the application is shortened.

Comparison of Branch at Home and Remote Access VPN technologies

Access type	Device support	Session duration	Internet security	Security framework	Home network	Employee type	Network topology	Cloud-hosted application support
Remote access VPN	Single	Timed based on VPN terminator support. Generally, 8-12 hrs max.	Only when VPN is active. Device is vulnerable when VPN client inactive	Client-based, requires separate endpoint security suite and process for updating	Shared. Member of residential wired/wireless networks	Primarily road warrior and part-time home workers	Hub/Spoke forcing all traffic to VPN terminator before entering WAN	Forced to trombone through terminator before exiting WAN to cloud
Branch at home	Multiple: Laptop + IP phone +VC suite + printer/ scanner	Always on	Always on Comprehensive firewall, IDS/ IPS, and hardware-based encryption	Embedded based on ZTNA model with centralized policy enforcement and localized security functions	Dedicated. Runs in isolation from residential wired/wireless networks	Home-based workers needing always on connections	Full or partial mesh with direct access to all locations on the WAN	Option to locally breakout (local firewall) to nearest Internet instance of cloud application

As the table above highlights, there are different core functions that remote access VPN and Branch at Home provide. For the home-based employee who needs a secure and isolated working space in the home then Branch at Home can't be beaten with its multi-device support, secured and isolated environment and always on availability. However, there is still a place for remote access VPN technologies, be that for more ad hoc home working or for those on the move as part of their business roles.

The technologies can be implemented together on the enterprise WAN to provide a full set of remote working options that fit with the needs of the business.

Conclusion

The Nokia Cloud-Managed SD-WAN Service provides the functionality enterprises require as the pandemic has forced new working conditions that include both in-office and teleworker environments.

With Nokia Cloud-Managed SD-WAN and its Branch at Home feature set, MSP/SI partners can offer their enterprise customers a viable alternative to the remote-access VPN solution that's more fit for purpose to home teleworking where business connections are needed for an extended period of time and where a consistent IT management environment can be administered.

The Branch at Home solution gives business leaders confidence that any critical staff are working in an environment at home that is as secure as they would have in the office. This means confidence that business sensitive workflows are being securely completed, be that:

- Working with client sensitive information
- Working on critical business research and development
- Providing a 'branch quality' remote working environment for front line call center and customer care representatives
- A secured at home working environment for members of their senior leadership team.

The use cases for Branch at Home are as varied as the industry verticals and market segments that need home based business network access and with the future business environment having a strong teleworking culture the need for robust home-based teleworking will continue to grow.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID210137 (November)