BEST PRACTICES FOR REMOTE ACCESS IN DISASTER MITIGATION AND RECOVERY SCENARIOS

How to accelerate the design and implementation of secure remote access during times of crisis

Abstract

In times of crisis organizations can excel in quick resource mobilization but not necessarily rational decision-making. Quick choices are made that seemingly address an immediate challenge but also lead to long-term unforeseen consequences.

This Check Point white paper provides guidance for network security administrators on the capabilities of, and methods of implementing secure access for remote employees. The document highlights the Check Point's remote access solutions and their applicability to different use cases. Also covered are network design considerations and high-level implementation methods.

Audience

This is an introductory-level technical document. It is intended for network and security administrators who are looking for an initial and high-level explanation of remote access options and capabilities. When appropriate, the document provides links to user and administration guides, where detailed instructions are available. This is not a data sheet or marketing white paper.

TABLE OF CONTENTS

Introduction ____ 4
Remote Access Considerations ____ 5
Architecture ____ 7
Use cases and configuration ____ 9
- Use case #1: SSL VPN Portal – Clientless Remote Access ____ 11
- Use case #2: Light client access using - SNX (SSL Network Extender) ____ 13
- Use case #3: Secure Connect with Endpoint VPN Agents ____ 15
- Use Case #4: Large Scale Remote Access ____ 17
- Use case #5: Secure access from SmartPhones ____ 18

Performance and Sizing ____ 20
Rapid licensing in a time of need ____ 20
Summary ____ 23

Introduction

In exceptional circumstances, it might become necessary to prevent employees from working in the office. When such situations arise teleworking and remote access solutions become critical to ensuring continued business operation.

Gone are the days when companies maintained modem banks to which users would dial-in to company systems without leveraging untrusted public network connections. Instead, many workers have their own broadband connections at home with WiFi networks capable of supporting network speeds similar to those found in the office. This makes it possible for employers to leverage their workers' home networks for connectivity to the edges of corporate resources. But, home networks are often shared with family members, fully rely on untrusted public backbones and can be entirely unprotected. Connecting remote employees to corporate systems therefore requires additional layers of security to ensure the confidentiality, integrity and availability of corporate data and systems.

It is important to note that remote access can be achieved through multiple technology types. Some applications, such as video conferencing tools, can be cloud-based and allow employees to communicate and share files together through a SmartPhone, tablet or computer app. In addition, web-based email can make it possible for employees to read and write messages with colleagues, customers, vendors and partners. However, such tools do not connect users to internal systems and services, and they introduce the very real possibility that employees might save confidential company and customer data on unprotected private computers and phones.

In order to overcome these security challenges, organizations need to implement multiple levels of security when opening corporate systems to employees working from home.

This document explains at an introductory technical level the different remote access offerings included in the Check Point product family. The text below also provides guidance on architectural considerations and configuration methods.

Readers interested in more detailed technical guidelines can reference Secure Knowledge documentation available via the Check Point Support Center.

Remote Access Considerations

As a general rule, all Check Point security gateways are equipped with Remote Access VPN capabilities that can be enabled to operate immediately by activating certain licenses. The activation and configuration of Remote Access is very simple and intuitive and does not require a significant level of technical knowledge from the administrator. To improve the user experience, Check Point also provides different types and methods of access; from the clientless to client-based remote access VPN solutions, depending on the required level of access and types of applications in use.

There are several factors to consider when choosing remote access solutions for your organization:

Client-Based vs. Clientless – Installing a full software client enables the provisioning of multiple security features in a single solution: remote access, personal firewall, zero-day attack prevention, malware scanning, disk encryption, port protection, content security and many other capabilities. A full client also provides support for more complex encryption and authentication methods as well as a rich set of network configuration options, such as the allocation of internal-to-the-corporate-network IP addresses to remote machines. However, installing a full client requires administrators to validate configuration settings, define policies and conduct user acceptance testing. Client-less solutions provide far less features and often leverage functionality delivered by other desktop solutions, such as browsers and operating system components.

Device security requirements – In general, the rule of least privilege applies in all security scenarios. Namely, only those people who require access should receive such access, and only those machines that should connect to systems should be allowed to do so. Once a decision is taken to enable remote access, the next step in the security process is to determine the trust, privilege and risk levels of the users and devices that will access internal resources. When the combination of risk and privilege are high, a stringent set of controls needs to be applied. These can be delivered at the network level, meaning the employees' computers at home should not be trusted at all and any access should be contained within company controlled workspaces on the employees' machines. This type of model can be supported by remote desktop like solutions that leverage SSL connections. Users remotely connect to their desktops in the office, and any and all work is performed on the corporate machine located within corporate boundaries. Alternatively, companies can also take-over employee computers at home and install a full set of security controls on those machines. In so doing, they effectively turn the employee's computer into a corporate asset and apply full personal firewall, anti-malware, APT inspection, disk encryption and also IPSec VPN to the device. Of course, there are multiple alternatives within these two extremes, and the different remote access options are intended to support such alternatives.

Secure Connectivity – When considering remote access options, administrators should determine if users will require the ability to work on their home machines (corporate or personal) with the same user experience as when in the office, or will it be acceptable to provide limited access to specific applications. In general, IPSec VPN solutions are best at replicating an in-office experience for employees working from home. In IPSec scenarios, the VPN inserts itself at the IP stack level and encrypts all network communications between the user's machine and the corporate network. SSL tends to be more application specific and ensures the privacy of the communications channels between the applications running on the user's machines and the back-end systems to which they communicate. In essence, with IPSec, administrators focus on building the secure communications path for the machine to the corporate network, while with SSL, IT teams ensure that the applications hosted on corporate resources are designed for SSL connections to employee devices.

The following section summarizes highlights on the architectural considerations for implementing different remote access options.

Architecture

All remote access connections terminate at a gateway. The location of the VPN concentration solution carries with it security administrative implications that should be understood prior to implementing access to connecting machines.

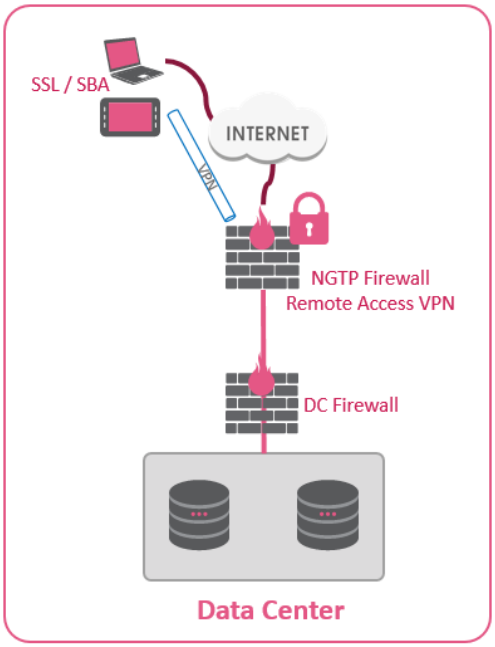
The following section highlights a number of options for designing VPN gateways in the network.

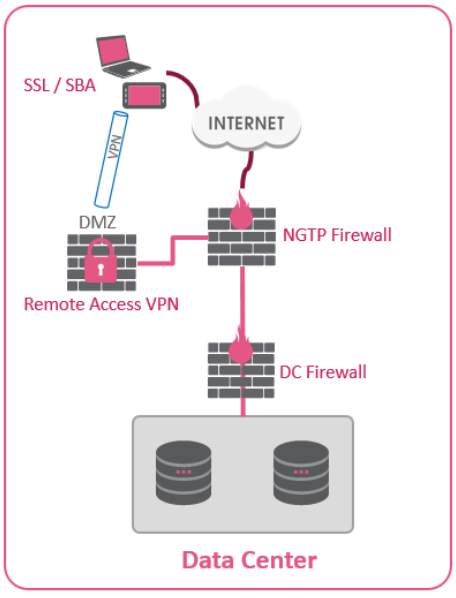
Scenario 1: Simple perimeter gateway deployment for smaller companies

In the simplest remote access deployment, a single gateway, or cluster, inspects all traffic, including sessions with remote access clients.

The gateway runs a full stack of security protections, including firewall, VPN, intrusion prevention, application control and content security, advanced threat prevention and others. The gateway would be configured on the network perimeter.

This configuration is the simplest and is relevant for smaller organizations who do not need to support multiple network segments and in-house hosted applications.





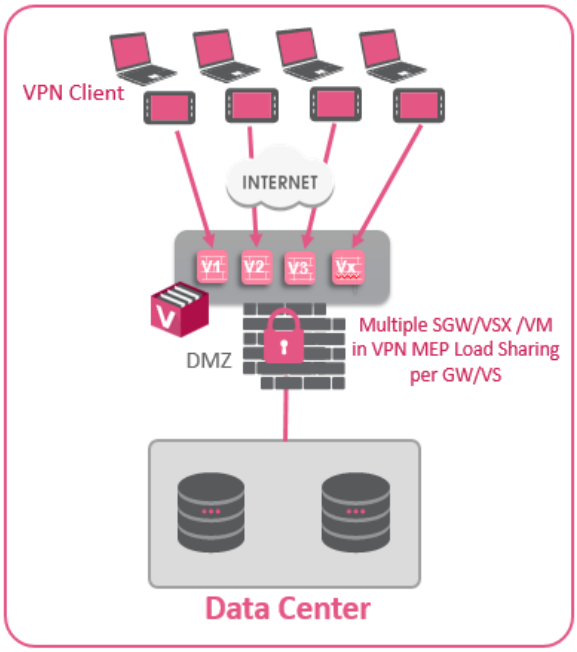
Scenario 2: VPN gateway as a dedicated security gateway in DMZ

When a remote access enabled Security Gateway is placed in the DMZ, traffic initiated both from the Internet and from the LAN to mobile users is subject to firewall restrictions.

In addition, by deploying the remote access gateway in the DMZ, the need to enable direct access from the Internet to the LAN is avoided. Instead, remote users initiate a VPN connection to the remote access gateway.

In this configuration, external gateway policy forwards VPN traffic to the VPN concentrator, where encryption terminates, and threat prevention, authentication, and authorization take place. The VPN gateway forwards requests to the internal servers.

Scenario 3: VPN termination as a dedicated single or multiple Security Gateways (appliances), or virtual instances running in VSX mode or as a Virtual Machine (VM)



Administrators can use multiple appliances or virtual versions of Check Point gateways to support remote access connections.

In VSX deployments, each Virtual System can have a Mobile Access portal with different applications, access policies, authentication requirements, and mobile clients. The same cloud be achieved by deploying several security appliances as physical gateways.

For example, in the picture to the right, a VSX Gateway has four Virtual Systems with remote access VPN enabled. Each Virtual System is configured with different settings to meet the company's needs for different users.

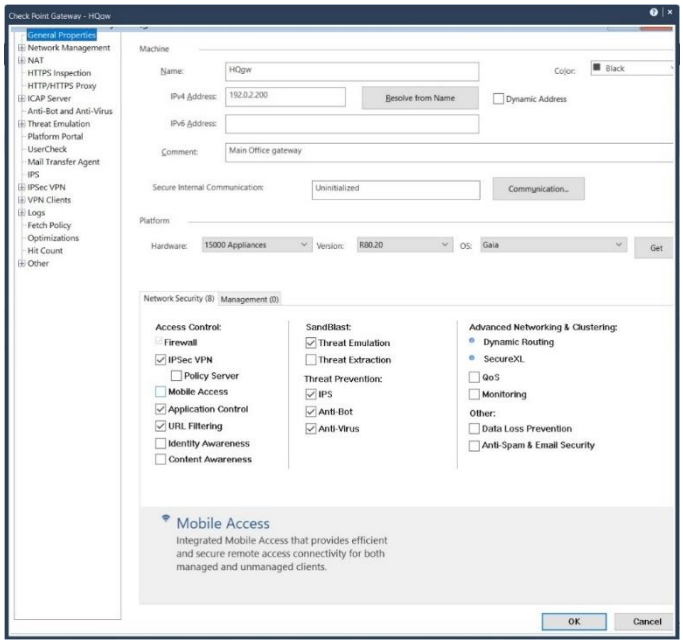
This scenario also fits well when there is a demand to significantly increase the number of remote access users in the existing setup or a new configuration in order to ensure proper performance and scalability of security gateways responsible for remote access VPN.

With IPSec VPN scenarios, the recommendation is to leverage several security gateways or Virtual Systems to enable Multiple Entry Points (MEP) with load sharing among the virtual gateways. The remote users with a pre-installed client will automatically choose the virtual system to which they will connect in random distribution, thus reducing the load on a single gateway.

Use cases and configuration

In disaster recovery scenarios and use cases where SSL VPN is the desired remote access method, Check Point recommends the following sequence to activate Remote Access VPN to critical applications and resources in the corporate environment:

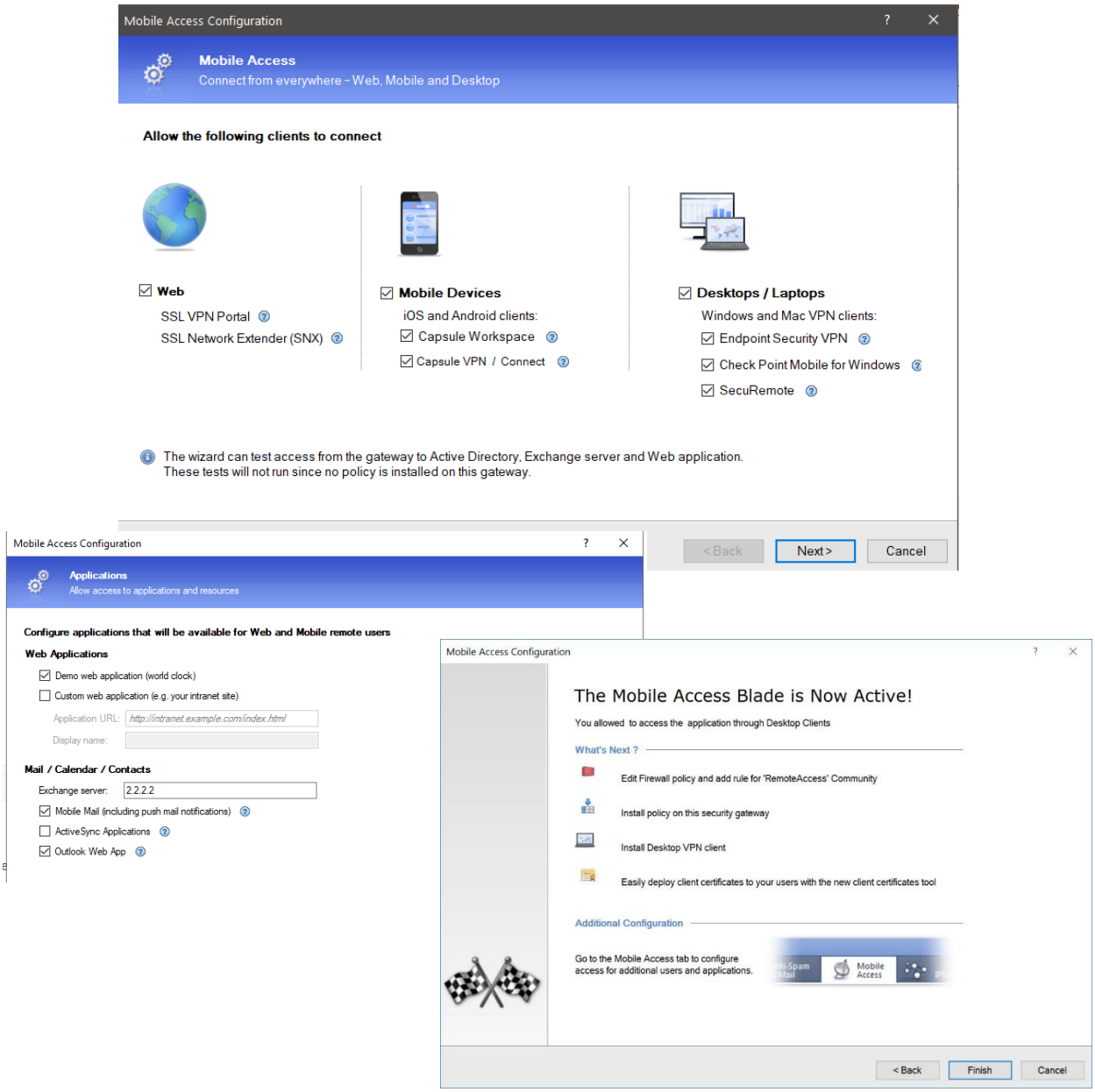
- Activate Check Point's Mobile Access Blade (MAB) on the gateway with all possible features and clients enabled
- Configure SSL VPN portal access and define important web applications to be reached by remote users using their Web browser, such as Web-Based Outlook, and hosts on your Intranet such as SharePoint and file shares
- Allow certain users based on need, to activate and use SSL VPN clients, such as the SNX client from the Check Point SSL VPN portal to connect to resources using native applications, using full L3 VPN tunnel connectivity
- Create a template for smart phone users in the Check Point Mobile Access Blade configuration pane; with instructions of how to download mobile clients from Apple and Google Play stores and connect securely to your Web applications and Email
- Select one of the VPN clients and provide installation guidelines for remote users that require secure access to corporate assets. Additionally, this includes features such as Endpoint local security to ensure that the device is secured even when not connected to VPN, leaving all data on the device encrypted and protected



To begin using Check Point Remote Access capabilities on the security gateway, you will need activate and configure MAB in the SmartConsole of the security gateway.

The majority of Check Point security gateways are pre-licensed for 5 mobile access users. This helps with the initial set-up of connecting devices and to run tests before production enrollment and activation of endpoint or device licenses. Check Point small-to-medium (SMB) appliances are pre-licensed as follows: 700 series: 100 mobile users; 900 series: 300 users; 1500 series: 100 users.

After enablement, the SSL VPN Mobile Access Blade will pop up a first time wizard to proceed with the configuration of all relevant access methods and clients. Follow the wizard and complete the setup to start defining the access methods for remote users, configures authentication and access policies.

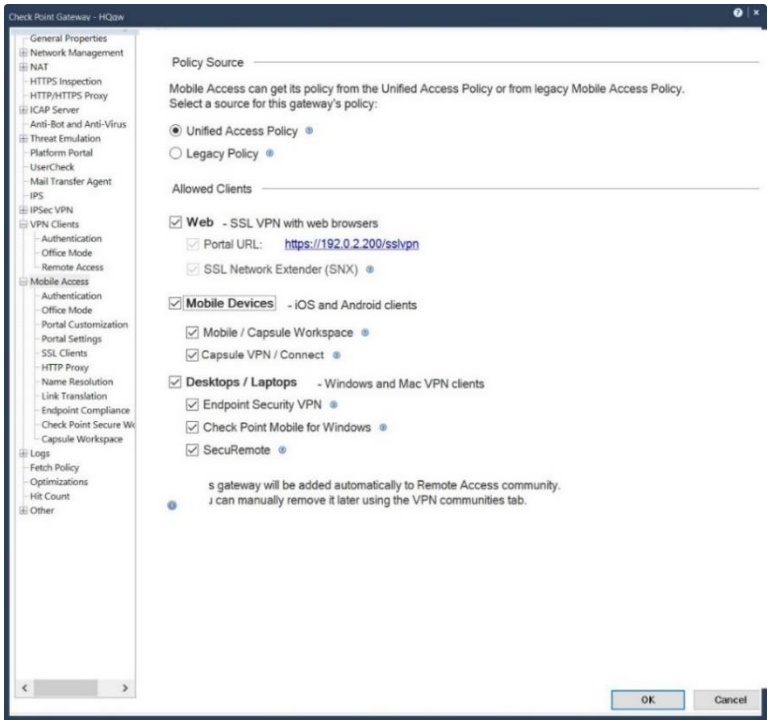


For more detail on how to accomplish the setup of MAB, please refer to the admin guide at: https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_MobileAccess_AdminGuide/Content/Topics-MABG/137084.htm

Use case #1: SSL VPN Portal – Clientless Remote Access

SSL VPN Portal Access enables the rapid deployment of user devices to business services without changing endpoint machines.

SSL VPN Portal Access is a clientless SSL VPN solution. It is recommended for users who require fast, secure access to corporate resources from home, an internet kiosk, or another unmanaged computer.

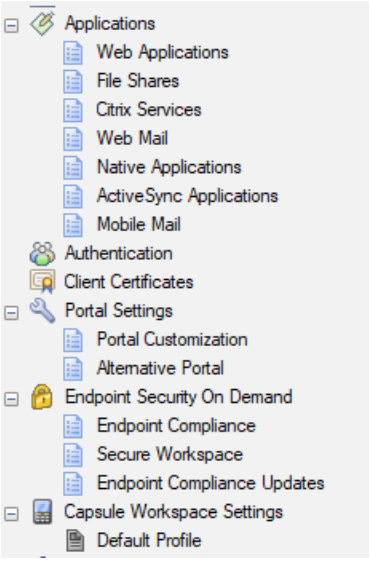


Authentication capabilities include a Check Point password, Personal Certificate, RADIUS, or SecureID.

For mobile devices, the solution includes support for mobile device management and root detection. In addition, SSL VPN Portal supports Secure Configuration Verification (SCV), ,and OS verification.

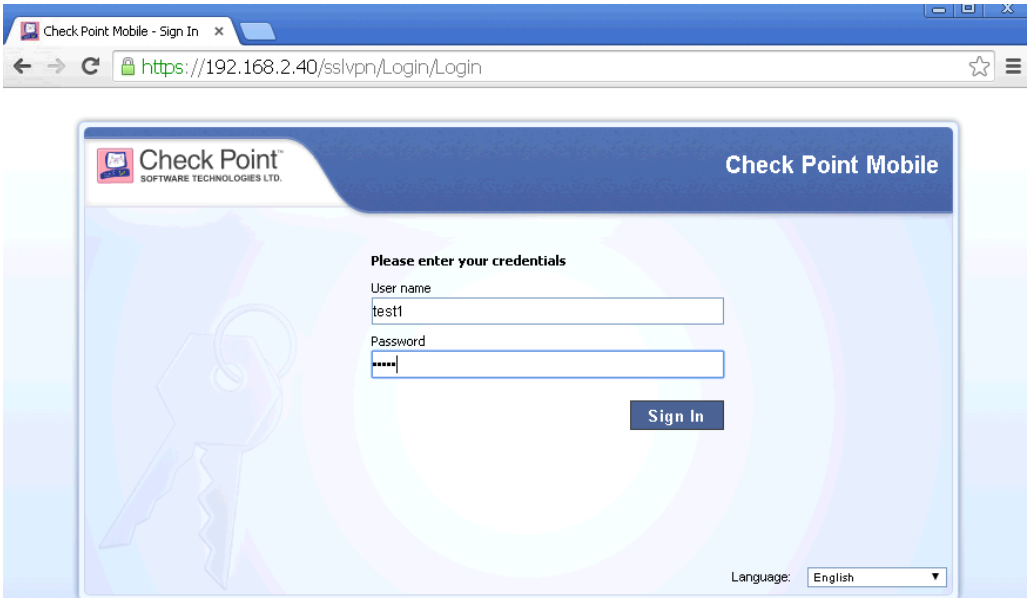
The types of apps that can be remotely accessed include Outlook Web Access (OWA), SAP, Internal Web applications and Web servers and many other commercial tools.

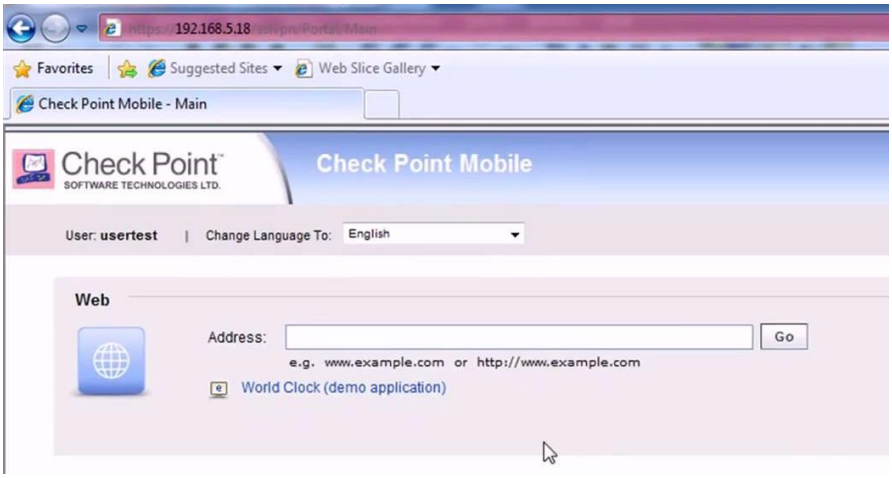
As part of the MAB setup, you have already selected SSL VPN Portal as part of the selected items. The final configuration is to make sure you select the SSL Portal Options, as defined in Gateway Configuration > Mobile Access shown in the image to the right.



A successful VPN setup is displayed after connecting to the portal at https://IP_address/sslvpn

The remote user can connect to the portal, pass the authentication phase and reach the home page with the pre-defined URL (links) to the web applications to which access was enabled.





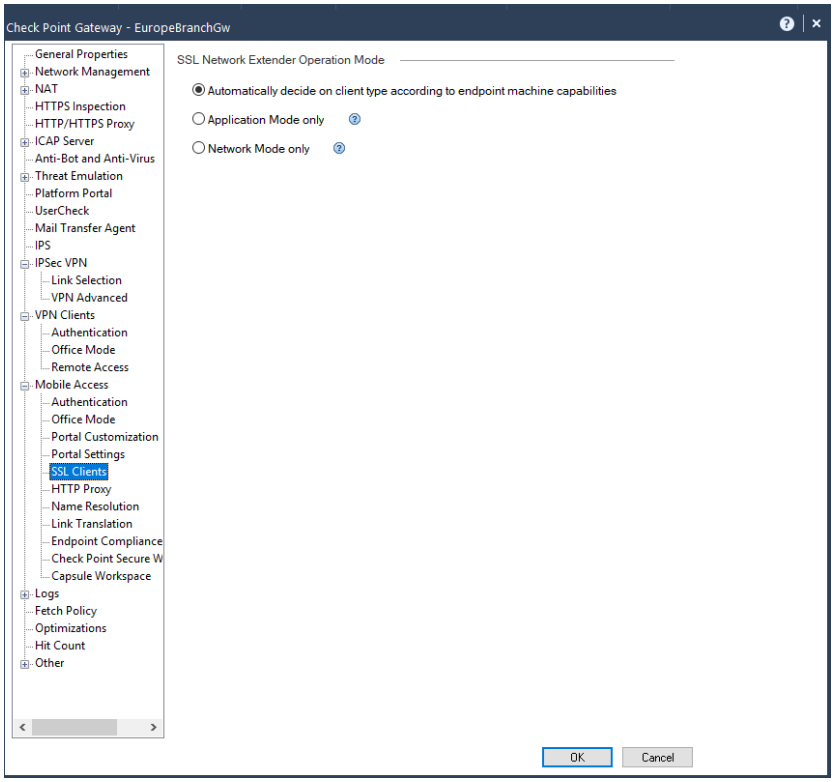
For more detail on how to accomplish the setup of the SSL VPN Portal, please refer to the admin guide at: https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_MobileAccess_AdminGuide/Content/Topics-MABG/137084.htm

Use case #2: Light client access using - SNX (SSL Network Extender)

The SSL (Secure Socket Layer) Network Extender is a simple-to-implement remote access client-based solution.

A thin client is installed on the user's machine. It is connected to an SSL enabled web server that is part of the Enforcement Module. By default, the SSL enabled web server is disabled. It is activated by using the SmartConsole, thus enabling full secure IP connectivity over SSL.

The SSL Network Extender requires server side configuration only. Once the end user has connected to a server, the thin client is downloaded as an ActiveX component or Java, installed, and then used to connect to the corporate network using the SSL protocol.



Note – SSL Network Extender must be configured through the Mobile Access blade; this is also true if SSL Network Extender is configured on an IPsec VPN Security Gateway.

The SNX client-side pre-requisites for remote clients are:

- A supported Windows or Mac operating system
- ActiveX or Java 8 Applet allowed on target machines for installation
- First time client installation, uninstallation, and upgrade require administrator privileges on the client computer

The SSL Network Extender client provides secure remote access for most application types (both Native (IP-based and Web-based) in the internal network via SSL L3 tunneling.

Most TCP applications can be accessed in Application mode. The user does not require administrator privileges on the endpoint machine.

After the client is installed, the user can access any internal resource defined on Mobile Access as a native application. The application must be launched from the Mobile Access portal and not from the user's desktop.

Important SNX features include:

- Easy installation and deployment with an intuitive and easy interface for configuration and use and small size client (650kb)
- Support of Visitor Mode and Office Mode
- Automatic proxy detection
- All Security Gateway authentication schemes are supported
- Authentication can be performed using a certificate, Check Point password or external user databases, such as SecurID, LDAP, RADIUS and other methods
- High Availability Clusters and Failover are supported
- User authentication using certificates issued by any trusted CA that is defined as such by the system administrator in SmartConsole
- Endpoint Security on Demand, which prevents threats posed by Malware types, such as worms, trojan horses, key loggers, browser plug-ins, adware, third party cookies and others
- Hub Mode, in which all VPN traffic is forwarded to a central network entity

For more detail please refer to the mobile access admin guide at:

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_MobileAccess_AdminGuide/Content/Topics-MABG/131215.htm?Highlight=SNX

Use case #3: Secure Connect with Endpoint VPN Agents

Check Point offers a variety of Endpoint VPN clients. Each support full IPSec VPN connectivity for endpoints connecting to a corporate gateway. Unlike client-less and lightweight remote access solutions, endpoint agents provide robust performance, reliability and advanced security and connectivity capabilities.

The below table describes features and licensing of some of Check Point's endpoint VPN solutions:

Solution	OS	Threat Prevention	Additional Features	SKU
Unified Endpoint Security Advanced	Windows, Mac, iOS and Android	YES	Full Endpoint suite & zero-day protection	CPEP-SBA-ADVANCED-MTP
SandBlast Agent	Windows / Mac	YES	Full Endpoint suite & zero-day protection	CPEP-SBA-COMPLETE
Endpoint Security VPN for Windows and Mac	Client-based	YES (Windows) NO (Mac)	Full Endpoint suite	CPEP-SBA-BASIC (and ADVANCED)
SecuRemote	Windows	NO		
Check Point Mobile for Windows	Windows	YES	Endpoint compliance check	CPSB-MOB

Further enhancing the capabilities of Check Point's endpoint solutions are the advanced threat prevention capabilities of Check Point's SandBlast family. This is especially important during emergency scenarios when employees might be confined to their homes, and by definition outside the boundaries of the corporate network, for extended periods of time.

Check Point SandBlast Agent protects laptops and computers from cyber-attacks, both known and unknown, through a rich set of advanced features, including:

- Threat Emulation: evasion-resistant sandbox technology that detects malicious behavior and prevents potential attacks
- Threat Extraction: a unique capability that strips malware and other attack methods from attachments and downloads
- Anti-exploit: protections for vulnerable applications
- Anti-bot: indicator and heuristic capabilities that identify and prevent botnet and C&C communications
- Zero-phishing: real-time blocking of phishing sites and attempts to use corporate passwords in non-company sites
- Behavioral guard: forensics-based detection and mitigation of evasive attack types
- Anti-ransomware: real-time identification of ransomware attacks and backup of data to

prevent file loss

- Forensics: recording and analysis of endpoint events for rapid incident response

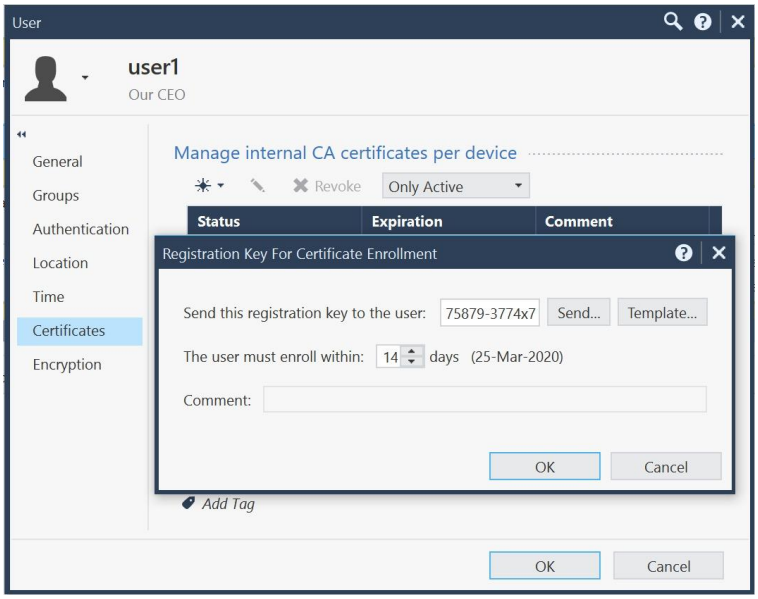
Selecting VPN clients is an intuitive process enabled within Check Point's SmartConsole.

Administrators check the boxes associated with the different VPN client types that employees will use to connect to corporate systems:

Defining authentication methods is equally simple.

Check Point provides fast ways to enroll users in a trusted relationship with the VPN gateway. Among many certification methods is an internal certificate authority that operates within the Check Point management server.

When using this method, administrators define certificate attributes and then distribute certificate details to the employee population.

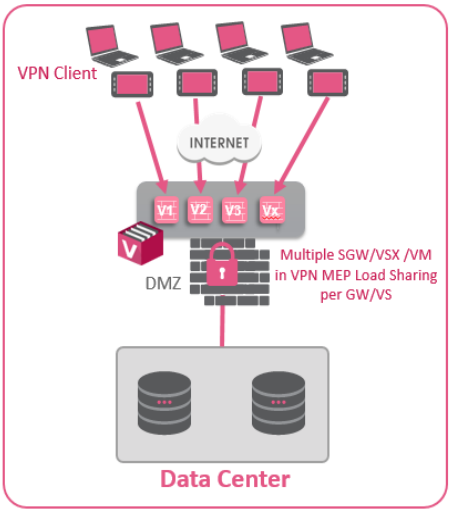


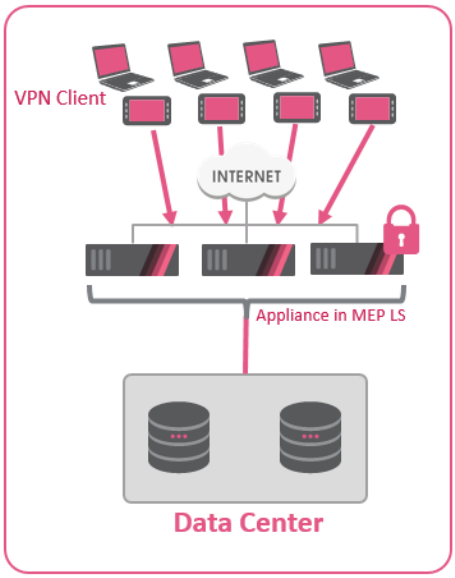
The employee receives a registration key and then activates the certificate. Once this is done, the user enters their credentials via the client prompt, and the agent initiates the connection process.

More information about regarding endpoint configuration is available at: https://sc1.checkpoint.com/documents/R80.40/SmartEndpoint_OLH/EN/Content/Topics-EPSG/Intro-to-Endpoint_Security.htm

Use Case #4: Large Scale Remote Access VPN

In the Large Scale Remote Access VPN scenarios, where there is a request to terminate enterprise-scale numbers of VPN clients with high numbers of concurrent sessions and high rates of new sessions-per-second, Check Point recommends the following best practices guidelines for new and existing deployments:





- As shown in the suggested architecture to the right, multiple VPN termination gateways are configured as Virtual Systems in a VSX/VSLS cluster or using VMWare environment with Check Point GloudGuard IaaS solution
- The same could be accomplished using multiple physical gateways (appliances) as shown in the right bottom figure
- In such scenarios, it is advisable to limit each MEP VS / gateway to up to 3,000 users
- Consider using a high-end appliance, such as the 23000 or 26000 series, with 5-8 VS instances in VSX mode
- When VSLS mode is used, more VSs could be deployed based on the amount of the VSLS members in the cluster setup
- When using multiple physical security gateways it is recommended to utilize medium size appliances, such as 6000-series, in order to distribute groups of users evenly across the gateways and to ensure reliability during fail-overs
- Leverage Multiple Entry Point (MEP) Remote Access VPN technology, which balances and distributes connectivity loads across multiple security VPN gateways
- Activate MEP Load Sharing for load distribution
- When distributing load across different geographies, use Manual MEP to define target gateways based on closest user proximity to gateway
- When dedicating a gateway for remote access, assign more cores to secure network distributor (SND) functions
- Select fast encryption algorithms, such as AES-128, to optimize security and performance
- Turn on NAT-T (NAT Traversal) for users who must pass through systems that block IPSec protocols, and, when possible, avoid Visitor Mode configurations
- As a general rule, use the latest available version an jumbo hotfix

For more information about MEP in RA setup refer to this admin guide:
http://downloads.checkpoint.com/dc/download.htm?ID=60345

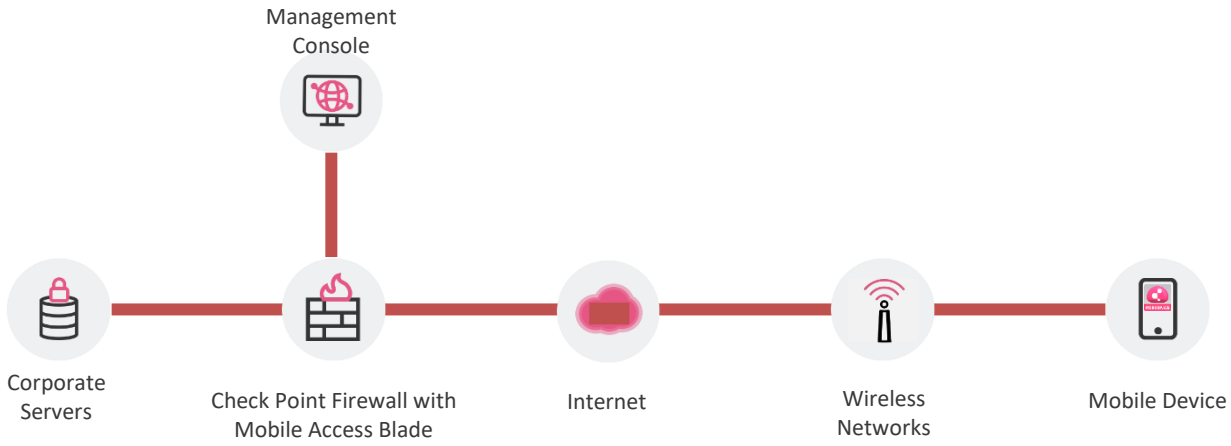
Use case #5: Secure access from SmartPhones

Check Point Capsule Mobile Secure Workspace is a mobile security container that creates an isolated corporate workspace on personal devices, making it simple to secure corporate data and assets both inside and outside the corporate network.

Check Point Capsule Workspace protects and manages enterprise apps and data on iOS and Android devices without needing to manage Mobile Device Management (MDM) profiles.

Capsule Workspace is easy to deploy and manage, helping to reduce the time, effort, and cost of keeping mobile devices and data secure. Once deployed, it creates an AES256-bit encrypted container for enterprise apps and data that puts you in control of the sensitive enterprise information you need to protect. Capsule Workspace never touches personal apps, media, or content, on a device which helps improve end user adoption, even on personally-owned devices.

Users will also appreciate the native experience and one-touch access Capsule Workspace provides to the critical enterprise apps they need to stay in touch on the go. It supports Microsoft Exchange Server and Office 365 email, calendar, and contacts, and includes secure enterprise instant messaging and document access



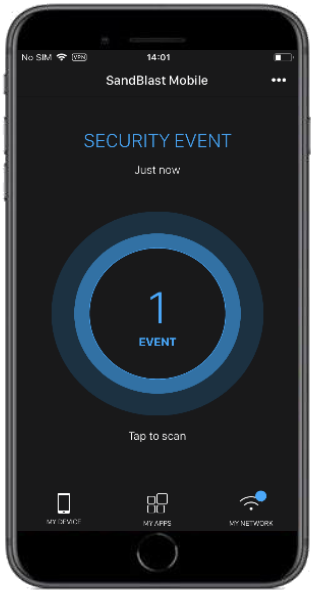
Check Point Mobile enterprise client connects to the Check Point security gateway that is running Mobile Access Blade over a SSL tunnel. The gateway then establishes a connection to the Exchange server using EWS protocol to provide access to the certain user's mailbox, calendar and contacts.

Check Point Capsule Workspace provides the following key value propositions:

1. Segregate business data from personal data and applications
    a. Use business data within a secure application
    b. Manage only business related data
    c. Maintain personal data and applications independently

2. Securely use business applications in a seamless way
    a. One touch access to corporate email, calendar, contacts ,documents and applications
    b. Enable secure remote access to internal corporate resources from devices running IOS / Android.
    c. Encrypt business data and applications to ensure seamless access only to authorized users
3. Prevent business data loss from mobile devices
    a. Define authentication settings to manage access to the business application
    b. Protect sensitive corporate information with remote wipe capabilities
    c. Detect and prevent access on devices that have been rooted, jail broken or modified

As employees leverage SmartPhones for corporate work-related activities, it then becomes crucial to protect the security of those phones. This applies to corporate owned and employee bring-your-own-device (BYOD) scenarios. Check Point address this need with its SandBlast Mobile solution.



SandBlast Mobile provides the following threat prevention capabilities:

- Advanced app analysis: runs apps downloaded to mobile devices in a virtual, cloud-based environment to analyze behavior then approves or flags them as malicious.
- Network-based attacks: detects malicious network behavior and automatically disables suspicious networks to help keep mobile devices and data safe. On-device Network Protection, inspects and controls network traffic to and from the device, blocking phishing attacks on all apps and browsers, and communications with malicious command and control servers.
- Device vulnerability assessments: analyzes devices to uncover vulnerabilities that cyber criminals exploit to attack mobile devices and steal valuable, sensitive information.

Performance and Sizing

When employees work from home they expect that their user experience will be the same as when they are in the office. Their experience connecting to streaming media and gaming services from home teaches that corporate applications should operate with the same level of performance and stability.

To help achieve optimal performance levels it is especially relevant to understand the remote user VPN termination capacity of various security gateways.

Often times, companies request generic VPN performance statistics. This is intended to provide a view towards maximum capacity and to compare marketing data sheet statistics of multiple vendor solutions.

The following table shows an example of certain Check Point appliance **lab testing results** for number of users remotely connecting to gateways. It is shown in this document in order to show capacity and is not a recommendation appliance selection in production environments:

Table 1: Lab Results at 100% Utilization

Business size	Appliance	Number of users at maximum capacity
SMB	3600	2,000
Medium	6600	4,000-9,000
Large	16000	Greater than 10,000
Enterprise	26000	Greater than 10,000

It is important to remember that all customer scenarios are different and individual company engineering teams should assess the current performance levels of their production gateways and their internally defined limits for CPU and memory utilization. An additional element to consider is the average bandwidth of connecting users.

Therefore, when implementing remote access in production networks, is it always advisable, even in emergencies, to limit gateway CPU utilization to acceptable levels. Many customers use 50% as the maximum average CPU utilization benchmark.

Thus, when adding VPN functionality to an existing device, or expanding the number of remote users connecting to it, review current maximum CPU utilization guidelines, and then consider adding remote users in 10% bunches of the total number of people who will be added as remote access users to an individual gateway or cluster.

In production environments, the throughput of individual user connections and application behavior can vary widely from those used in lab test beds. Further, some elements of VPN connections are more resource intensive than others, for example: initial tunnel establishment involves multiple handshakes and authentication processes. In addition, gateway rule-basis and configuration settings can impact over-all VPN performance.

Considering this variance, Check Point recommends that customers take a more conservative approach to VPN gateway sizing. The following table shows **best practices** for assigning remote users types while ensuring sufficient device headroom for activating advance protections, enabling stable communications during peak traffic scenarios and other real-world experiences.

Table 2: Real-World Recommendations

Business size	Appliance	Number of users: real-world recommendations
SMB	3600	300
Medium	6200	600
	6600	1000
	6900	3,000
Large	16000	5,000
Enterprise	26000	10,000+ (VSX / VSLS MEP scenario)

Rapid licensing in a time of need

In times of true crisis, such as global pandemics, national security events and extreme weather, organization might not have the ability to complete their budget approval and procurement processes in time to implement the remote access capabilities that they need to ensure business continuity.

Check Point understands that such scenarios do happen and enables its sales field to request evaluation licenses for the above outlined solutions.

In order to take advantage of this ability, Check Point sales representatives and SEs should leverage Check Point's standard product evaluation resource on PartnerMap, at: https://usercenter.checkpoint.com/usercenter/portal/media-type/html/role/usercenterUser/page/default.psml/js_pane/ProductsTabId,ProductEvaluationId.

And, finally, special requests can be made via an account team's sales leadership, Check Point's Support and Account Services teams and the Solution Center.

Summary

Telecommuting and remote access are standard for many members of the workforce. The rise of the Internet as a reliable and cost-effective communications medium made this possible, and as home broadband speeds have increased and Internet-based technologies have evolved, working from home has only grown in popularity and effectiveness.

During times of crisis, organizations can leverage telecommuting and remote access technologies for business continuity programs.

Check Point offers a wide array of products that enable the rapid roll-out of remote access capabilities. The company's solutions provide easy-to-use tools for administrators and users alike. These technologies include advanced capabilities that intuitively connect remote users to company resources, and, equally important, protect employee computers, phones, tablets and company data from advanced threats.

Check Point is singularly focused on ensuring the highest levels of cyber security. Our teams across the globe are available in times of need and are backed by corporate functions that will rapidly support critical challenges.

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com