Check Point Small-Medium-Business (SMB) Technology Guide

October 2018; Last Updated: May 13, 2019

Mark Sanchez, Security Engineer

EXECUTIVE SUMMARY

The purpose of this document is to provide an in-depth review of the capabilities within Check Point's SMB platform and highlight the key areas that bring both value and the very best in cyber security to the end user.

INTRODUCTION

The main concepts we will cover in this document

- Target Audience for SMB
- Hardware Overview
- Management Options
    - Local Web Portal
        - First Time Wizard (Initial Setup)
        - Access (Firewall) Policy
        - Threat Prevention Policy
        - VPN Policy
        - SMB Relay for Gateways Behind NAT
    - SMP (Security Management Portal)
        - On-Premise Capability
    - SmartProvisioning
- Large-Scale Deployment Options
    - ZeroTouch Provisioning
    - Rapid Deployment with USB Drive
- Technology Roadmap
    - Virtual SMB, Mobile App, Flexiport, SSLi Email Expansion (IMAPS/POP3S)
- Additional Resources

TARGET AUDIENCE FOR SMB

The SMB (Small-Medium Business) product line is targeted for organizations with 300 users or less. Check Point has been the leader in Cyber Security for many years. SMB combines the best security technology with simple deployment and administration. Dedicated network and security staff are no longer required.

Why Do Small Business Need A Solution Like This?

- 81% of SMB businesses do not have a Dedicated IT person
- 86% of SMB businesses do not have a Dedicated Security person

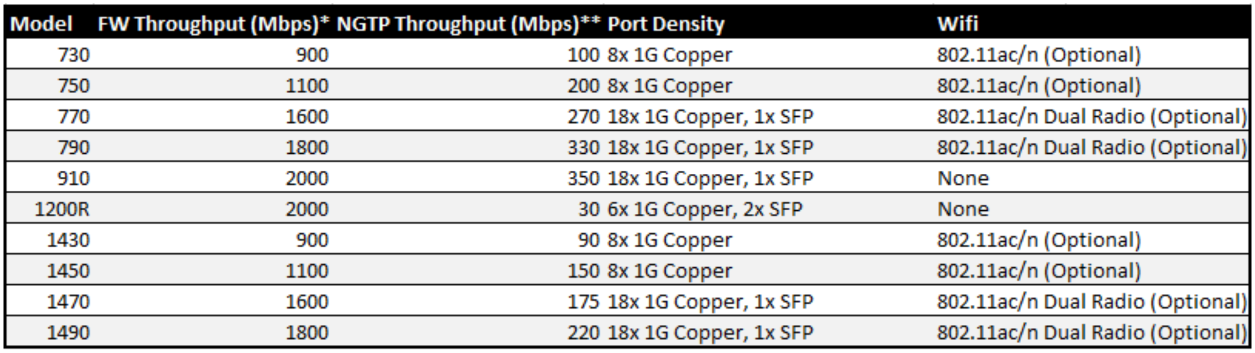
Understanding The Need for SMB Gateways

- 90% of US businesses have fewer than 250 employees.
- 83% attack success ratio on SMBs compared to 0.7% with large enterprises.

- 1 in 5 small businesses falls victim to cybercrime every year.
- 60% of small businesses that suffer a breach go out of business within 6 months.

HARDWARE OVERVIEW

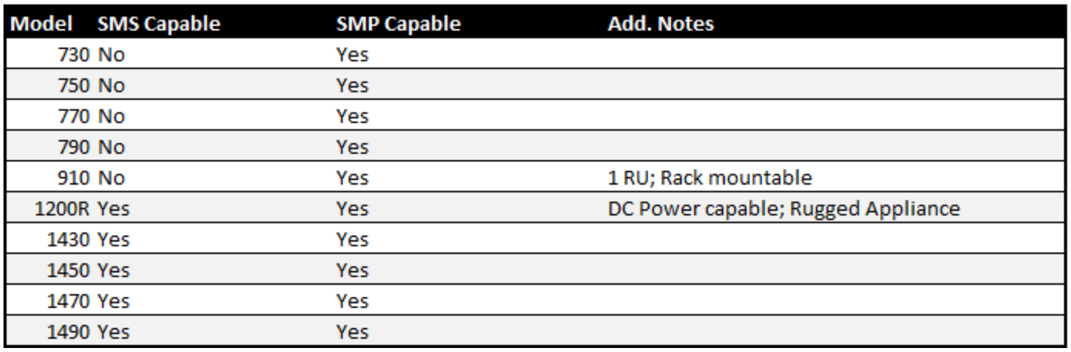
The SMB lineup currently includes 10 devices, but they vary in their capabilities. The charts below highlight their differences



Model	FW Throughput (Mbps)*	NGTP Throughput (Mbps)**	Port Density	Wifi
730	900	100	8x 1G Copper	802.11ac/n (Optional)
750	1100	200	8x 1G Copper	802.11ac/n (Optional)
770	1600	270	18x 1G Copper, 1x SFP	802.11ac/n Dual Radio (Optional)
790	1800	330	18x 1G Copper, 1x SFP	802.11ac/n Dual Radio (Optional)
910	2000	350	18x 1G Copper, 1x SFP	None
1200R	2000	30	6x 1G Copper, 2x SFP	None
1430	900	90	8x 1G Copper	802.11ac/n (Optional)
1450	1100	150	8x 1G Copper	802.11ac/n (Optional)
1470	1600	175	18x 1G Copper, 1x SFP	802.11ac/n Dual Radio (Optional)
1490	1800	220	18x 1G Copper, 1x SFP	802.11ac/n Dual Radio (Optional)

* Including Blades: Firewall Only

** Including Blades: Firewall, Anti-Bot, Anti-Virus, Application Control, IPS, URL Filtering. SSL inspection not included.



Model	SMS Capable	SMP Capable	Add. Notes
730	No	Yes	
750	No	Yes	
770	No	Yes	
790	No	Yes	
910	No	Yes	1 RU; Rack mountable
1200R	Yes	Yes	DC Power capable; Rugged Appliance
1430	Yes	Yes	
1450	Yes	Yes	
1470	Yes	Yes	
1490	Yes	Yes	

Additional SMB Tidbits

- White models (730-910) cannot be managed with SMS, Black models (1200R-1490) can.
- SMB gateways support 3G/4G/LTE models for WAN connectivity via USB port (sk92809).
- SD-card slot can be used for up to 2TB additional local logging capacity (sk111586).
- External logging to SMP (WebUI), Check Point SMS & syslog, are also supported.

MANAGEMENT OPTIONS

Whether you manage a single SMB gateway or hundreds, Check Point has several tools to make deployment & management, as simple as possible. We will walk through the process of managing a gateway locally, and expand upon that with SMB relay, which is helpful for gateway's behind a NAT and the Security Management Portal (SMP), which is a central management platform hosted by Check Point.

While not covered in-depth here, it is important to note that the 1000+ SMB gateways can be managed by the traditional enterprise Management Server and be treated like any other enterprise level gateway.

LOCAL MANAGEMENT

Before we can configure a policy, the first time wizard must be completed.

How To Complete The First Time Wizard

1. Connect your PC to LAN1 and set your NIC to obtain an IP address via DHCP.
2. Open a web browser and navigate to https://192.168.1.1:4434.
3. Accept the certificate warning (Self-signed) and complete the first-time wizard.

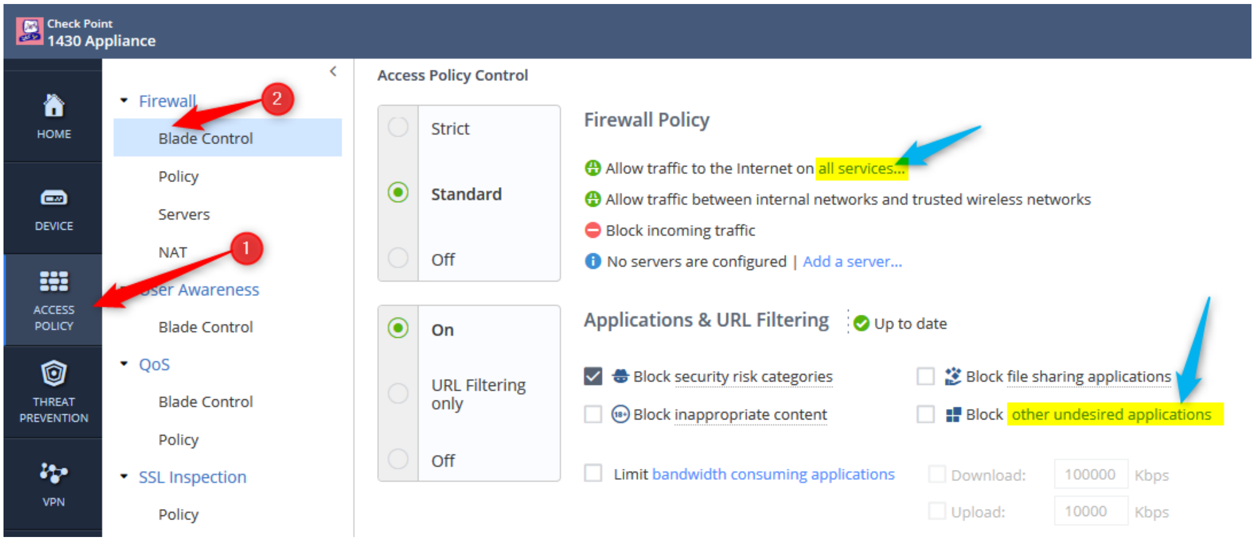
** https://192.168.1.1:4434 will be the URL to locally manage the gateway (WebUI) from here on out, unless the IP addresses are changed – however the default port will remain 4434.

Need console connectivity? Use the following settings for your serial connection.

```
Baud rate = 115200 bps
Data bits = 8
Parity = None
Stop bits = 1
Flow Control = None
```

How To Configure An Access Policy

1. To login the WebUI, navigate to Access Policy > Blade Control.
2. Here you can accept the default Standard policy or make changes as you wish.



Access Policy Control

○ Strict
● Standard
○ Off

Firewall Policy

Allow traffic to the Internet on all services...

Allow traffic between internal networks and trusted wireless networks

Block incoming traffic

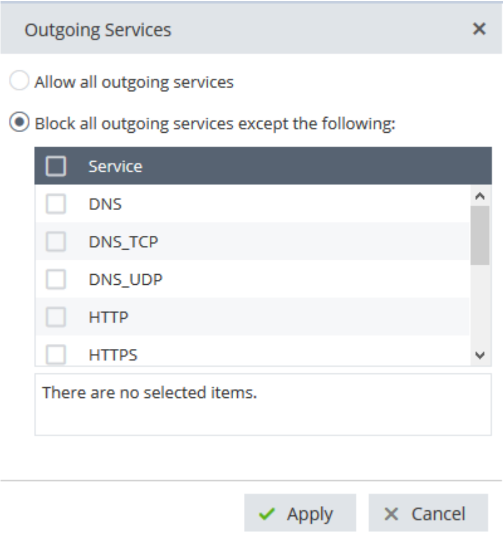
No servers are configured | Add a server...

● On
○ URL Filtering only
○ Off

Applications & URL Filtering ✓ Up to date

☑ Block security risk categories
☐ Block file sharing applications
☐ Block inappropriate content
☐ Block other undesired applications
☐ Limit bandwidth consuming applications
☐ Download: 100000 Kbps
☐ Upload: 10000 Kbps

3. You can get quite granular with the policy using the ‘all service…’ and ‘other undesired applications’ hyperlinks which can leverage not only URLs but also identified applications via deep packet inspection.

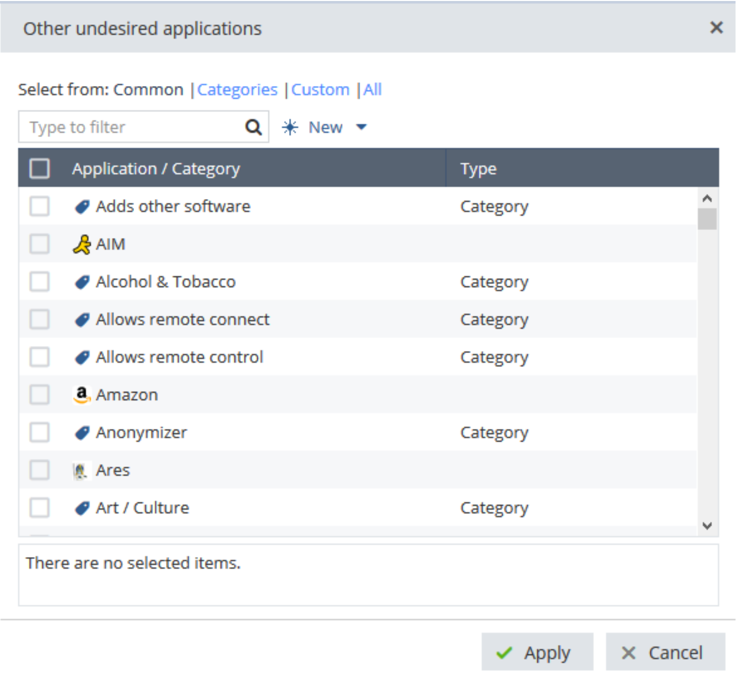


Outgoing Services ×

○ Allow all outgoing services
● Block all outgoing services except the following:

☐ Service
☐ DNS
☐ DNS_TCP
☐ DNS_UDP
☐ HTTP
☐ HTTPS

There are no selected items.



Other undesired applications ×

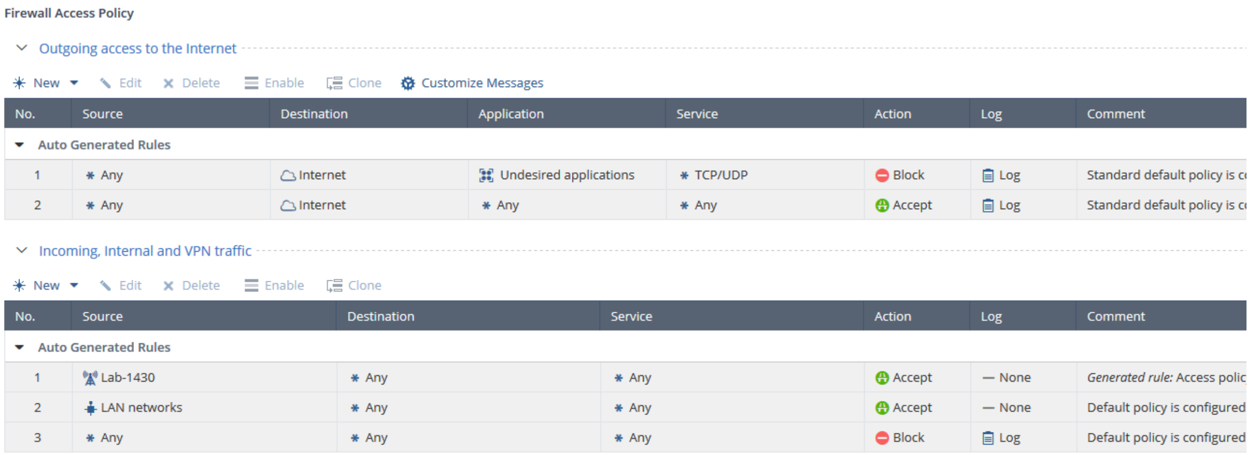
Select from: Common | Categories | Custom | All

Type to filter

☐ Application / Category	Type
☐ Adds other software	Category
☐ AIM	
☐ Alcohol & Tobacco	Category
☐ Allows remote connect	Category
☐ Allows remote control	Category
☐ Amazon	
☐ Anonymizer	Category
☐ Ares	
☐ Art / Culture	Category

There are no selected items.

4. Lastly you can navigate to Access Policy > Policy, to see the full firewall access policy that has been created for you based on your inputs thus far. You can manage the policy directly for the most granularity over the gateway.



Firewall Access Policy

Outgoing access to the Internet

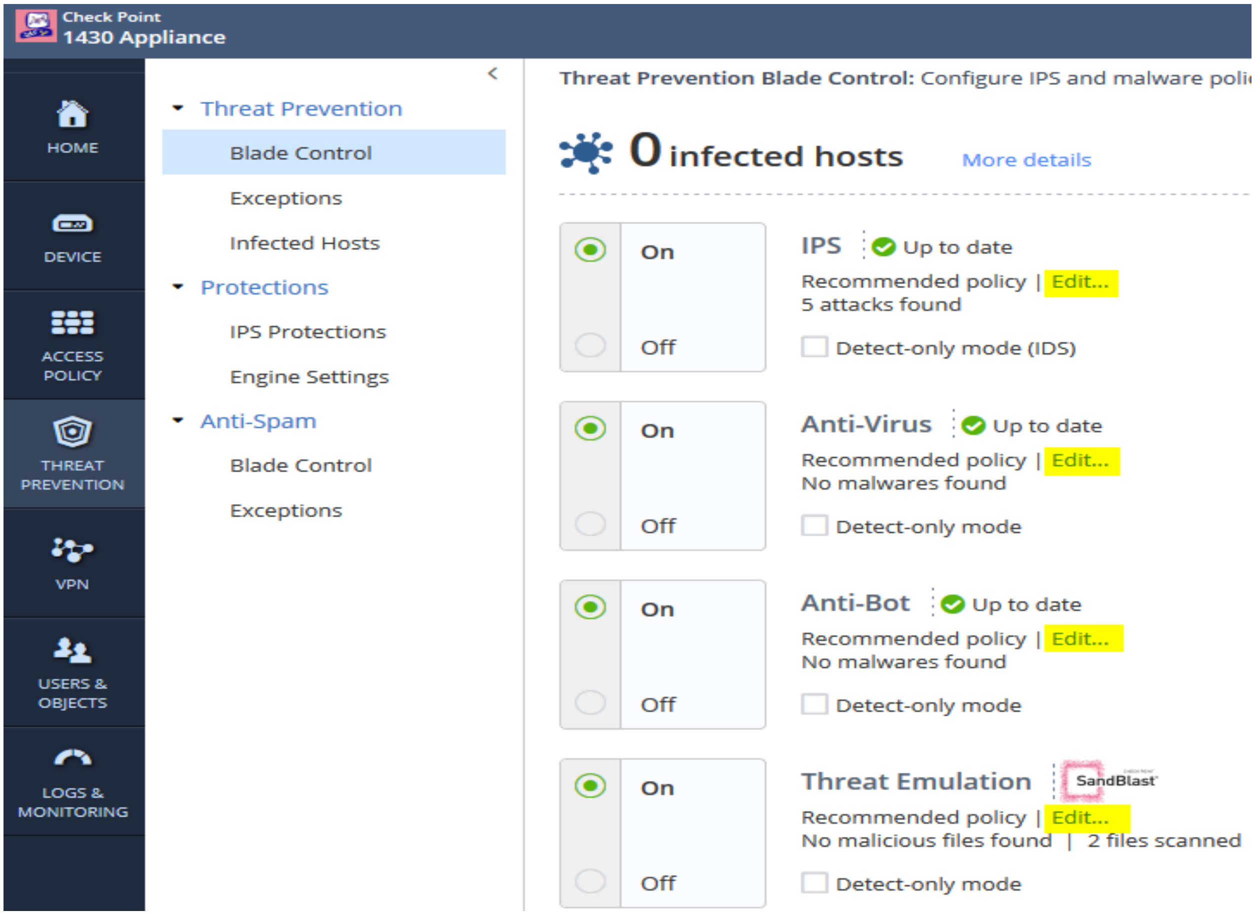
No.	Source	Destination	Application	Service	Action	Log	Comment
Auto Generated Rules							
1	Any	Internet	Undesired applications	TCP/UDP	Block	Log	Standard default policy is c
2	Any	Internet	Any	Any	Accept	Log	Standard default policy is c

Incoming, Internal and VPN traffic

No.	Source	Destination	Service	Action	Log	Comment
Auto Generated Rules						
1	Lab-1430	Any	Any	Accept	— None	*Generated rule:* Access polic
2	LAN networks	Any	Any	Accept	— None	Default policy is configured
3	Any	Any	Any	Block	Log	Default policy is configured

How To Configure A Threat Policy

1. Within the WebUI, navigate to Threat Prevention > Blade Control.
2. In addition to turning protections on/off, you can click ‘Edit…’ to fine tune individually.



Threat Prevention Blade Control: Configure IPS and malware poli

0 infected hosts

● On ○ Off — IPS | Up to date
Recommended policy | Edit...
5 attacks found
□ Detect-only mode (IDS)

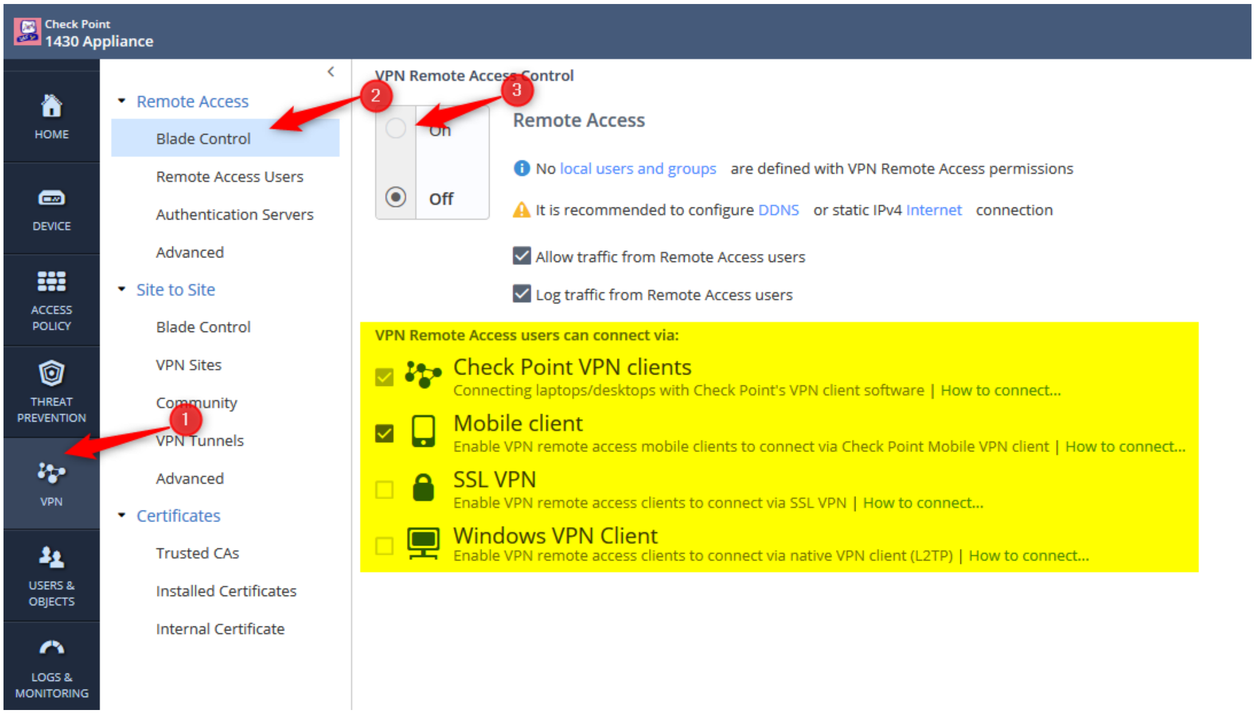
● On ○ Off — Anti-Virus | Up to date
Recommended policy | Edit...
No malwares found
□ Detect-only mode

● On ○ Off — Anti-Bot | Up to date
Recommended policy | Edit...
No malwares found
□ Detect-only mode

● On ○ Off — Threat Emulation
Recommended policy | Edit...
No malicious files found | 2 files scanned
□ Detect-only mode

How To Configure VPN Connectivity

1. Within the WebUI, navigate to VPN > Blade Control.
2. Here you can turn Remote Access VPN on by clicking as shown in the screenshot, then clicking ‘Apply’ on the bottom of the screen. The highlighted portion shows remote access methods that are currently supported.
3. Site to Site VPN tunnels are fully supported by setting the blade (VPN > Site to Site > Blade Control) to on and clicking ‘Apply’ on the bottom of the screen.
4. Site to Site tunnels can then be configured under the VPN > Site to Site > VPN Sites > Add a new VPN site.



VPN Remote Access Control

○ On
● Off

Remote Access

No local users and groups are defined with VPN Remote Access permissions

It is recommended to configure DDNS or static IPv4 Internet connection

☑ Allow traffic from Remote Access users

☑ Log traffic from Remote Access users

VPN Remote Access users can connect via:

☑ Check Point VPN clients
Connecting laptops/desktops with Check Point's VPN client software | How to connect...

☑ Mobile client
Enable VPN remote access mobile clients to connect via Check Point Mobile VPN client | How to connect...

□ SSL VPN
Enable VPN remote access clients to connect via SSL VPN | How to connect...

□ Windows VPN Client
Enable VPN remote access clients to connect via native VPN client (L2TP) | How to connect...

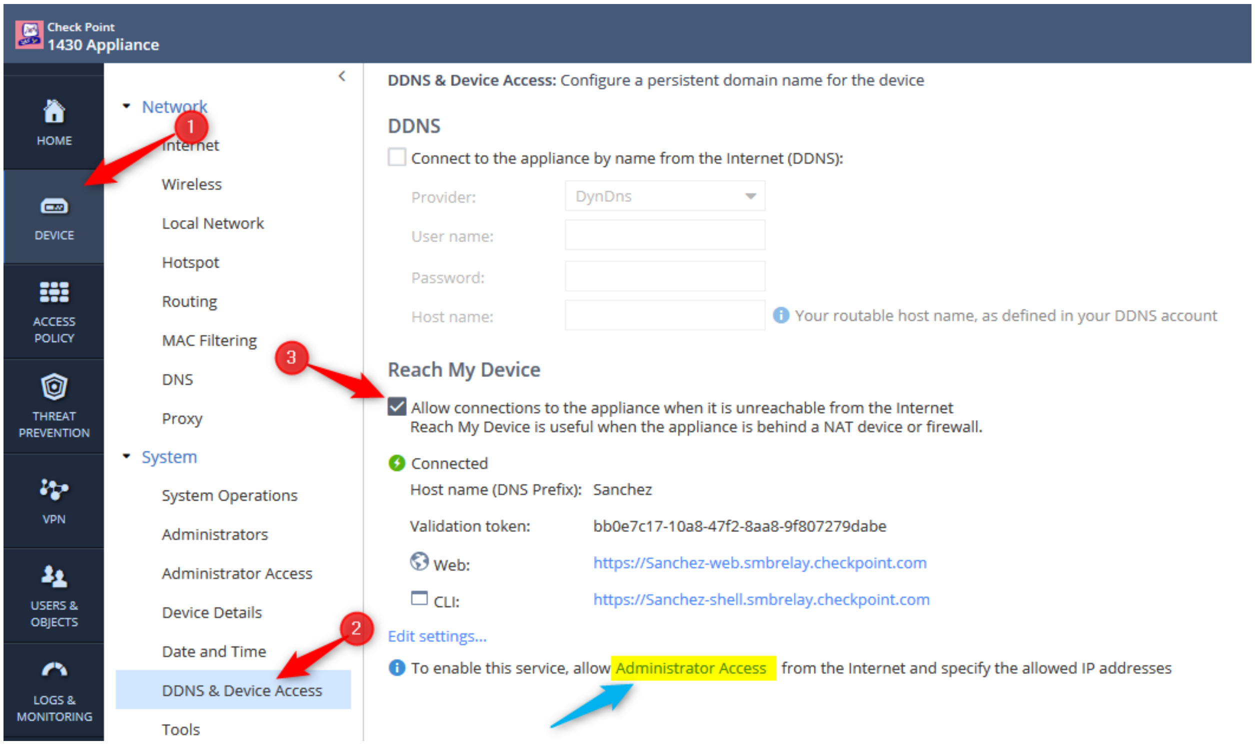
What Exactly Is SMB Relay?

SMB relay allows you administer the firewall (Both WebUI and SSH) as long as the WAN port receives a DHCP address with an Internet connection. This service is useful when the gateway is behind a NAT and is not directly accessible from the Internet.

Configuring SMB Relay

1. Within the WebUI, navigate to Device, DDNS & Device Access.

2. Enable ‘Reach My Device’ and click ‘Apply’.
3. The IP address(es) that you wish to manage the gateway from will need to be listed in the ‘Administrator Access’. This will apply to both local and SMB relay management.
4. The URLs to then manage the gateway will be shown, both for Web and CLI.



DDNS & Device Access: Configure a persistent domain name for the device

DDNS

□ Connect to the appliance by name from the Internet (DDNS):

Provider: DynDns

User name:

Password:

Host name: Your routable host name, as defined in your DDNS account

Reach My Device

☑ Allow connections to the appliance when it is unreachable from the Internet
Reach My Device is useful when the appliance is behind a NAT device or firewall.

Connected

Host name (DNS Prefix): Sanchez

Validation token: bb0e7c17-10a8-47f2-8aa8-9f807279dabe

Web: https://Sanchez-web.smbrelay.checkpoint.com

CLI: https://Sanchez-shell.smbrelay.checkpoint.com

Edit settings...

To enable this service, allow Administrator Access from the Internet and specify the allowed IP addresses

What is Check Point’s Security Management Portal (SMP)?

The Security Management Portal or SMP, makes it very easy to manage, monitor and collect logs for multiple SMB gateways, all in a central WebUI hosted by Check Point. Create templates to save on having to duplicate policies between gateways (Referred to as ‘Plans’). It provides one place to view and setup automated reporting such as network activity, high-risk activity and logging.

SMP On-Premise

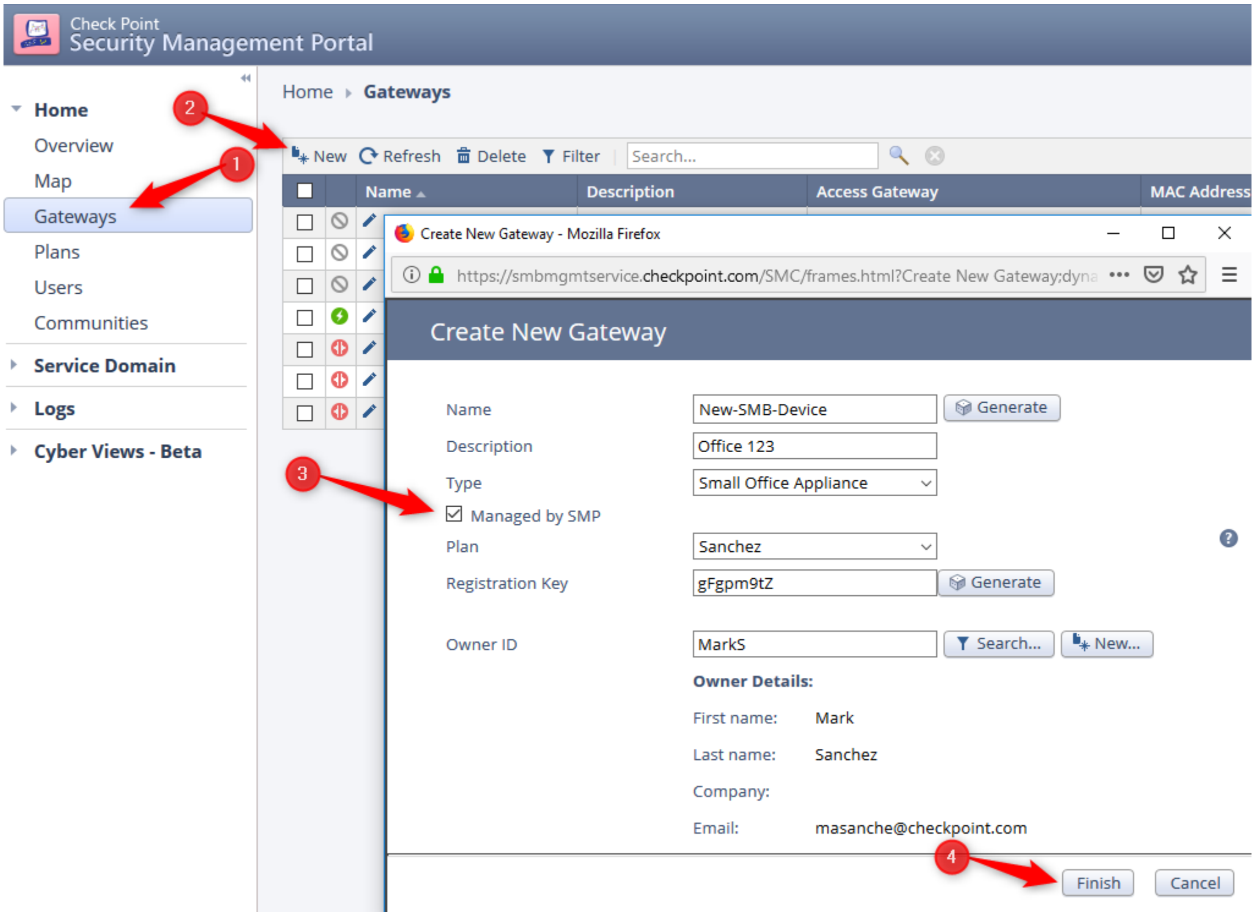
Instead of Check Point hosting the SMP, it can be self-hosted within your own environment. This is a common option for larger environments such as Telcos and larger MSPs.

SMP Licensing

Each customer who purchases an SMB gateway, is able to manage up to 10 SMB gateways free of charge (CPSB-SMP-CLOUD-BASE-10-DEMO). The smallest SMP package for purchase is for up to 20 gateways (CPSB-SMP-CLOUD-BASE-20), which can be added onto as the environment grows.

Adding A Gateway To The SMP Portal

1. Navigate to https://smbmgmtservice.checkpoint.com and login.
2. Navigate to Gateways and click New.
3. Enter a Name, Description, Plan of your choosing.
4. The Registration Key is just a one-time password for the initial sync of the SMB gateway.
5. The Owner ID assigns ownership to a gateway and becomes default email for reporting.

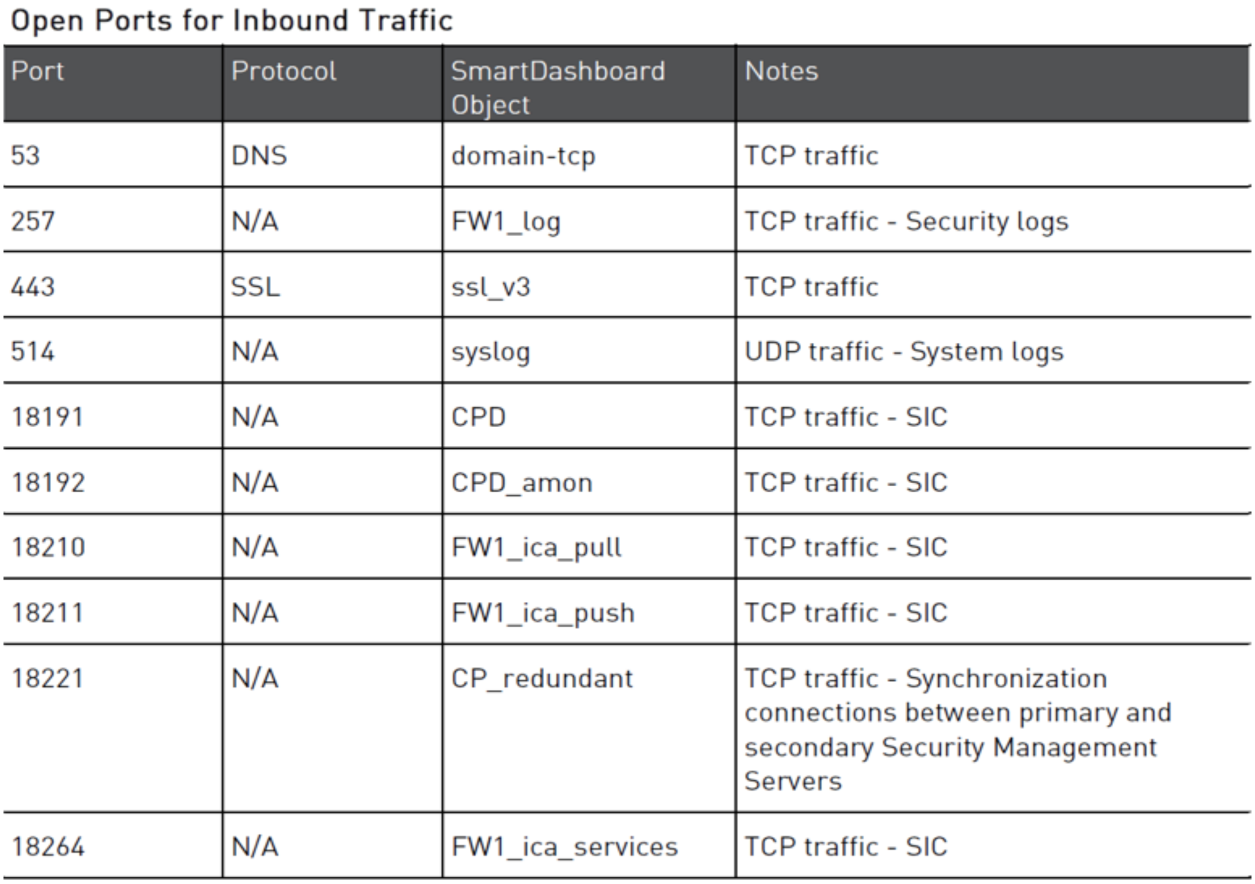


Name: New-SMB-Device
Description: Office 123
Type: Small Office Appliance
☑ Managed by SMP
Plan: Sanchez
Registration Key: gFgpm9tZ
Owner ID: MarkS

Owner Details:
First name: Mark
Last name: Sanchez
Company:
Email: masanche@checkpoint.com

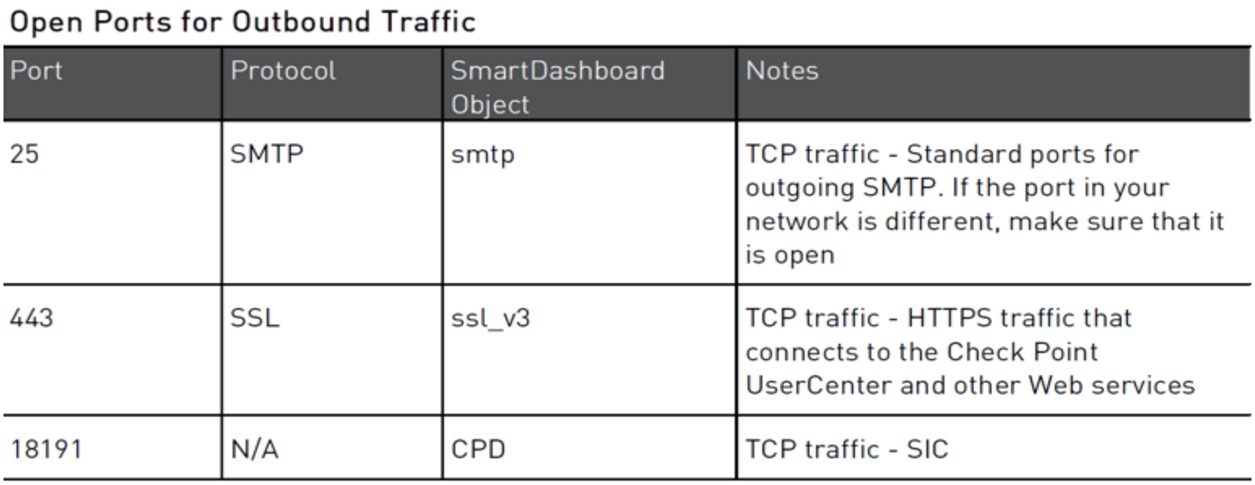
No Open Internet Access? No Problem

If your gateway connects directly to the Internet, you likely won’t need to worry about this. For full SMP functionality, ensure the following ports are open to the SMB gateway, from SMP point-of-view:



Open Ports for Inbound Traffic

Port	Protocol	SmartDashboard Object	Notes
53	DNS	domain-tcp	TCP traffic
257	N/A	FW1_log	TCP traffic - Security logs
443	SSL	ssl_v3	TCP traffic
514	N/A	syslog	UDP traffic - System logs
18191	N/A	CPD	TCP traffic - SIC
18192	N/A	CPD_amon	TCP traffic - SIC
18210	N/A	FW1_ica_pull	TCP traffic - SIC
18211	N/A	FW1_ica_push	TCP traffic - SIC
18221	N/A	CP_redundant	TCP traffic - Synchronization connections between primary and secondary Security Management Servers
18264	N/A	FW1_ica_services	TCP traffic - SIC



Open Ports for Outbound Traffic

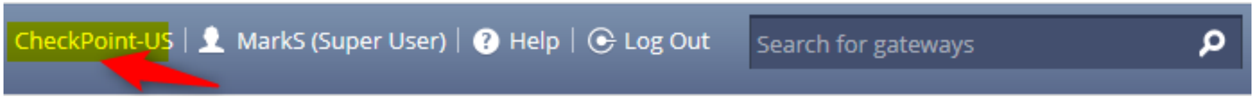
Port	Protocol	SmartDashboard Object	Notes
25	SMTP	smtp	TCP traffic - Standard ports for outgoing SMTP. If the port in your network is different, make sure that it is open
443	SSL	ssl_v3	TCP traffic - HTTPS traffic that connects to the Check Point UserCenter and other Web services
18191	N/A	CPD	TCP traffic - SIC

SMP Highlights

There is a lot you can do within SMP, listed below are some of the heavy hitters:

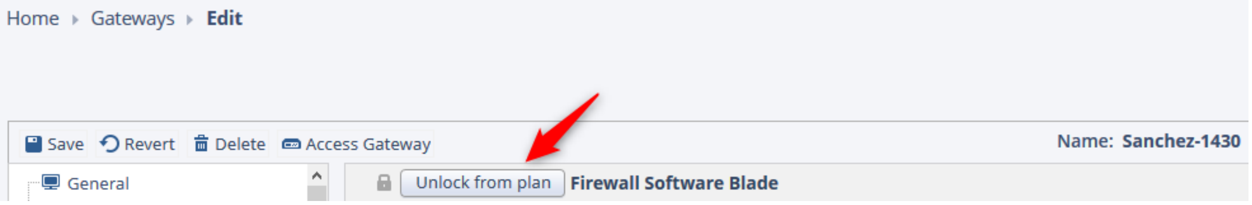
- **New Domain Request:** Have multiple customers you wish to keep separate? From the SMP login screen (https://smbmgmtservice.checkpoint.com/SMC/index.jsp) , click on 'New Domain Request'.

  Once logged into SMP, in the upper right-hand corner, click the current domain hyperlink to switch domains without having to log out & back in.



- **Home > Plans:** Want all your SMB boxes to send their logs to the SMP, send weekly network/high-risk activity report to the device owner and perform firmware/signature upgrades at 2am? How about having the same IPS, Anti-virus and Anti-bot config? Create a custom plan instead of applying the same configuration repeatedly.

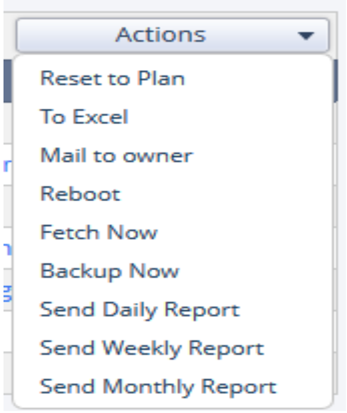
  Need to deviate from plan currently assigned? Navigate to Home > Gateways > [Gateway Name] and select the category for the change you wish to make. Choose 'Unlock from plan' at the top and add your per-gateway custom configuration.



- **Service Domain > Settings> Custom Alerts:** Want to receive a notification whenever the SMB gateway cannot reach the SMP – or any other custom type of alerting within the SMP itself? Create your own custom alert, then save.

- **Home > Gateways > Actions:** A menu of shortcuts to easily select the gateway(s) of your choice and perform a number of tasks including resetting a gateway's policies to plan defaults, export to excel, send email to owner, reboot, fetch config, backup gateway, send daily/weekly/monthly report(s).

  Note: These actions are not supported when a gateway resides behind a NAT.



- **Logs > Gateway Logs:** Easily search the logs and create custom queries to find exactly what you're looking for.

- **Cyber Views:** Review in-depth reporting outlining what attacks and other high-risk traffic is traversing the network, along with traffic utilization details and alerting.

What is SmartProvisioning?

Starting in R80.20, support for the 1100, 1200R and 1400 series SMB gateways is included with SmartProvisioning. Within the SmartProvisioning console, a profile is created to manage settings such as DNS, firmware, routing table, backup schedule etc., that make up many of the settings typically managed individually inside of the WebUI.

In addition, the gateway then checks into the SmartProvisioning server, at a default of every 4 hours, to fetch an updated configuration, if one exists. Policies can be also be pushed manually, if an immediate change is needed.

To work with SmartProvisioning, you need to configure Small Office Appliance Security Profile in the SmartConsole, Install Policy on the profie, and then switch to SmartProvisoning application, Create LSM Provisoning Profile to be able provision the networking and OS settings. The LSM Gateway object will include both security profile and provisioning profile.

For further details, please review the R80.20 administration guides for SmartProvisioning: https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_SmartProvisioning_AdminGuide/html_frameset.htm

LARGE-SCALE DEPLOYMENT OPTIONS

Check Point currently has two solutions built with the sole intention of making large-scale deployments as simple as possible. A brief overview of the ZeroTouch Provisioning and Rapid Deployment with USB tools along with their advantages are listed below.

What Is ZeroTouch Provisioning?

Available on the entire SMB gateway lineup, ZeroTouch provisioning allows the administrator to create a template for the initial deployment configuration within the Check Point hosted Zero Touch portal.

When an SMB gateway boots and establishes an Internet connection, if the first-time wizard has not been completed yet, the gateway will check to see if a zero-touch configuration exists for itself. If it does, then it is downloaded and installed, thus eliminating the need for the first-time wizard to be performed on each individual SMB gateway.

For further details and a video demonstration, please visit:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk116375

Rapid Deployment with USB

A configuration can be loaded onto a USB drive and inserted into an SMB gateway for automatic deployment of its configuration. It will first search for the autoconf.clish file and apply the configuration contained therein. Next, it will search for autoconf.XX-XX-XX-XX-XX.clish (XX's represent gateway's mac-address) and if it exists, deploy this configuration as well, potentially overwriting settings from the previous autoconf.clish file. The autoconf files are simply a list of the plain-text commands that are to be applied to the gateway.

This process eliminates the first-time wizard along with any configuration items included within autoconf files, saving a considerable amount of time for larger deployments.

For further information, please visit:
https://community.checkpoint.com/docs/DOC-2634-usb-first-time-config-using-autoconfclish-files-how-it-is-written

SMB TECHNOLOGY ROADMAP

- **Virtual SMB:** Check Point will be releasing the virtual SMB gateway in the near future. This will enable you to leverage your current virtual infrastructure and enjoy the technology and security that SMB offers. The virtual SMB gateway is lightweight (only 150MB image file), can be managed by local Web UI portal, or centrally by SMP or SMS.

- **SSLi Email Expansion (IMAPS/POP3S):** The SMB gateways can already perform SSL inspection for HTTPS traffic, however this capability will be expanded to include email protocols IMAPS and POP3s.

If you would like to participate in any of these pilot programs, please reach out to your local Security Engineer or Account Manager for further information.

ADDITIONAL RESOURCES

Notable SKs:

- Check Point SMB Appliances Releases
- Check Point SMB Features and Known Limitations

YouTube Channel:

- Official SMB Playlist by Check Point
- SMB Playlist by Sunny (R&D)

CheckMates Community:
https://community.checkpoint.com/community/infinity-general/smb-smp

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to corporate enterprises and governments globally. Its solutions protect customers from 5th-generation cyber-attacks with an industry leading catch rate of malware, ransomware and other targeted attacks. Check Point offers a multilevel security architecture with our new Gen V advanced threat prevention that protects all networks, cloud and mobile operations of a business against all known attacks combined with the industry's most comprehensive and intuitive single point of control management system. Check Point protects over 100,000 organizations of all sizes.