SD-WAN ARCHITECTURAL REFERENCE GUIDE

SCOPE

This how-to guide is intended for enterprises looking to reduce the cost of their WAN, while increasing business agility and application performance, in a secure manner.

The recommendations in this document are designed to inform engineers, architects, and enterprise security professionals, who want to deploy SD-WAN, and are looking for advice on choosing the right reference architecture for their specific environment.

Various use cases are also listed to help the reader find the most appropriate solution for their business needs.

> “By 2023 more than 90 percent of WAN edge infrastructure refresh initiatives will be based on virtualized customer premises equipment (vCPE) platforms or SD-WAN software/appliances.”
>
> Gartner, 2018

Contents

What is SD-WAN?

SD-WAN stands for Software-Defined Wide Area Network.

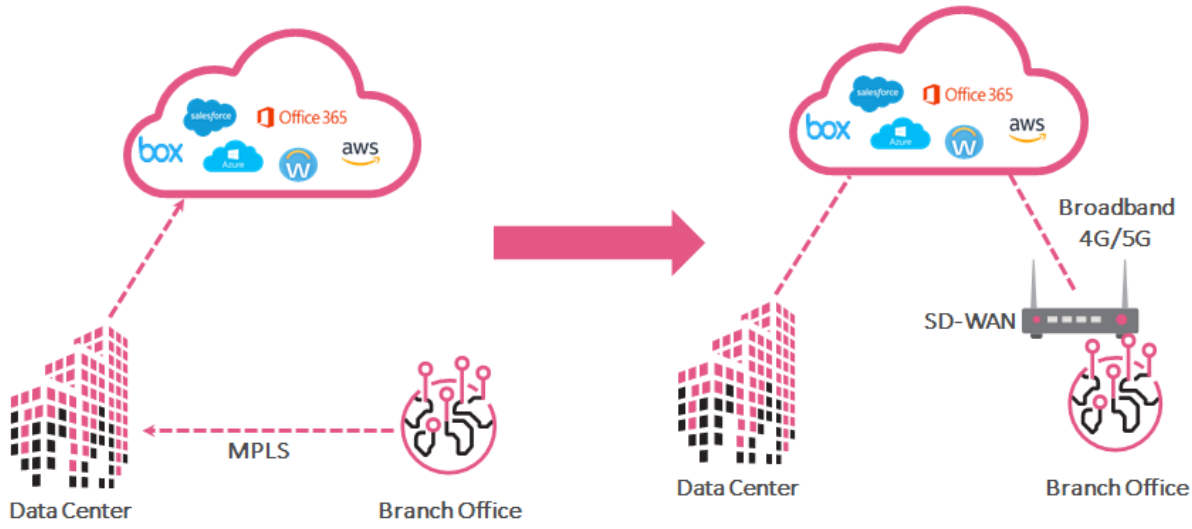
It is a virtual wide-area network architecture that allows enterprises to use any type (or combination of types) of connectivity (i.e. MPLS, IP VPN, broadband, cellular, etc.) to connect their users to applications in a secure way.

The simplification of the management and operation of the WAN, by switching to SD-WAN, is achieved by separating the networking hardware from its control mechanism.

Business drivers for switching to SD-WAN

1. Cloud adoption:

As enterprises rapidly move their data centers to the cloud, backhauling the traffic to the hub site and using the centralized Internet break-out there, may not be the best option in terms of cost and/or latency for users in branch offices wanting to access the cloud.



Replacing the VPN or MPLS routers in branch offices with an SD-WAN device, typically means that all traffic is no longer routed to the hub site and the branches will almost always get local Internet access (although this depends on the policy).

Connecting branch offices directly to the Internet significantly increases their security risk and security management costs. Branches are also no longer protected by centralized data center security, which exposes them and the enterprise WAN to sophisticated multi-vector Gen V cyber-attacks.

To combat this issue, enterprises can deploy traditional security gateway appliances in all branch offices to protect Internet traffic. Although this approach will provide the maximum security for all branches, it can be very costly. Moreover, some locations may not have the local IT resources to provide them with ongoing support.

Enterprises therefore need additional security solutions that can be quickly deployed across all branch offices, are always up to date with the latest security, and can be seamlessly integrated with existing routers or SD-WAN solutions.

2. **Instant upgrades:**

   Upgrading multiple physical gateways is time-consuming and leaves security inconsistent and lagging; converting to a SD-WAN system will eliminate this issue.

3. **Ease of deployment:**

   Enterprises are looking for a zero-touch provisioning solution, which is centrally managed and easy to deploy and scale.

4. **Increase business agility and user satisfaction:**

   A dynamic link selection will ensure that the best path is always automatically chosen if multiple access circuits are present.

5. **Improve security and reduce threats:**

   There are options to increase security to a level that can deal with gen V attacks, even with old EOL perimeter equipment.

6. **Cost reduction:**

   Traditional Wide Area Networks can be quite expensive and enterprises are looking at cheaper alternatives, such as broadband connections, with similar features. SD-WAN can help reduce costs by up to 90%.

The Check Point CloudGuard Advantage

Check Point's CloudGuard Connect and CloudGuard Edge transform branch SD-WAN Security with the industry's leading threat prevention technology, flexibility to deploy in the Cloud or on-premise, and a unified threat management platform that can reduce operational expenses by up to 40%.

		
Secure Top-rated threat prevention with 100% cyber attack catch rate	**Flexible** Five-minute set-up to protect SD-WAN in the cloud or on-premise	**Cost-Effective** Unified security architecture reduces OpEx costs by up to 40% and CapEx by up to 20%

The following sections will help the reader choose between Check Point's CloudGuard Connect and CloudGuard Edge technologies.

Some factors to consider will include:

- The importance of owning a platform vs. using it as a service
- The necessity of inbound access to public servers in the branch
- The ability to use cloud services for security vs. having a strict policy that restricts to on-premise solutions only

CloudGuard Connect vs. CloudGuard Edge

The main difference between the two solutions is the type of Customer Premise Equipment (CPE) used and whether or not cloud-based security controls are enforced.

This is due to CloudGuard Connect administering all the security controls in the cloud, while CloudGuard Edge enforces all the security controls on-premise as a virtual security gateway on an SD-WAN device.

CLOUD NETWORK SECURITY AS A SERVICE

Easily deployed and consistent security across thousands of branches

ON-PREMISE VIRTUAL SECURITY GATEWAY

Secures incoming and outgoing connections, maintain privacy and compliance

The following technology partners are interoperable with CloudGuard Connect (using IPsec or GRE). Other devices capable of standard IPsec or GRE, will also be compatible.

aruba a Hewlett Packard Enterprise company

CLOUDGENIX NETWORKS WITHOUT NETWORKING

CITRIX

silver peak

cisco Meraki

viptela

cradlepoint Connect Beyond

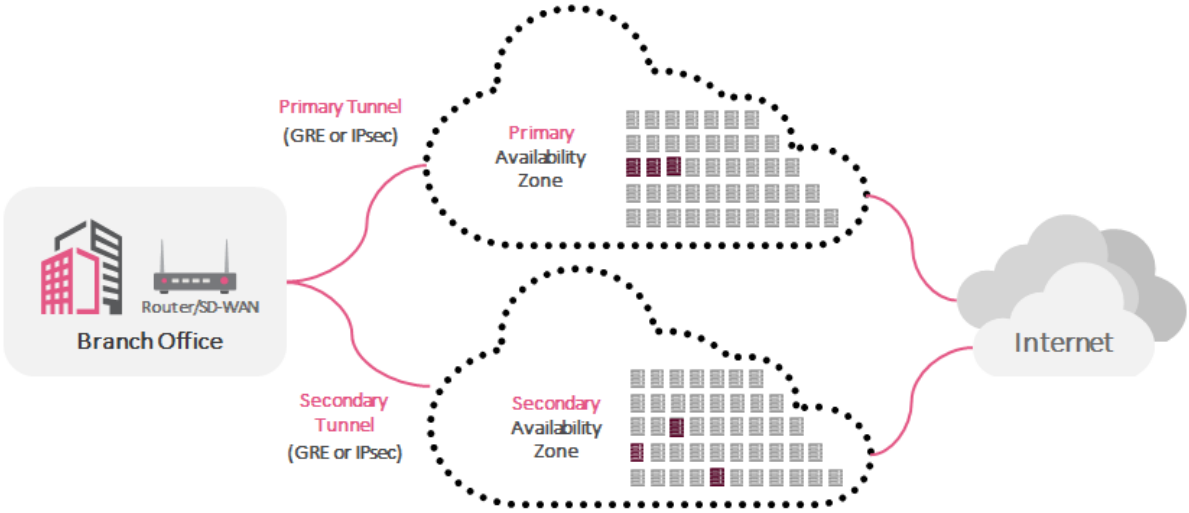
The following technology partners are interoperable with CloudGuard Edge (using a Check Point VNF on their hardware).

VERSA NETWORKS

velocloud

CloudGuard Connect

The CloudGuard Connect solution consists of an on-premise device that builds a redundant pair of VPN tunnels to two geographically close Check Point Cloud service points or availability zones. The required security controls are then enforced before allowing the traffic to exit to the Internet.

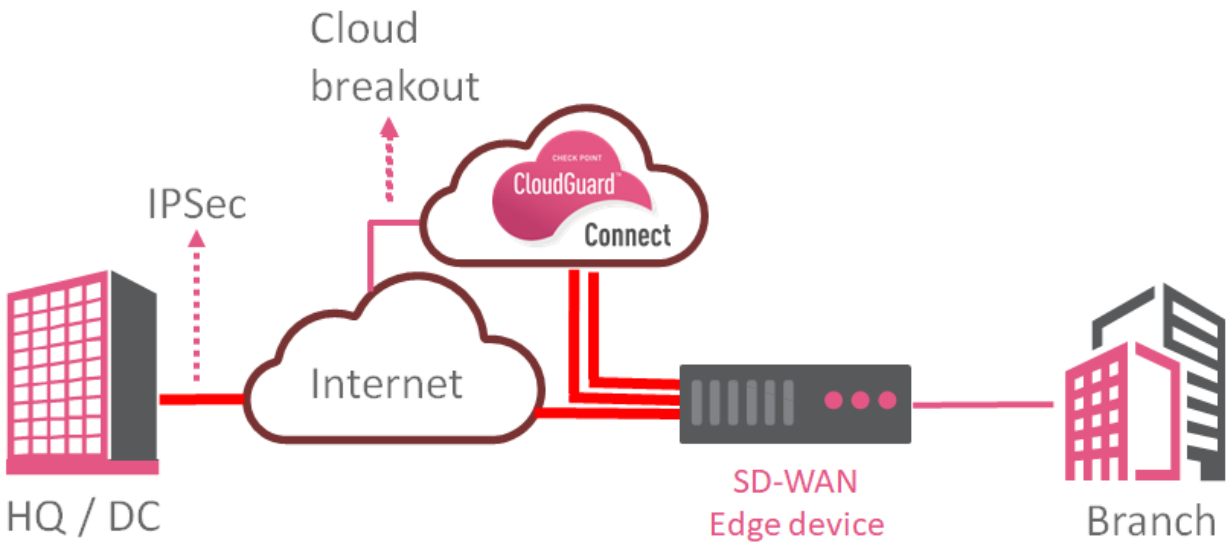


The on-premise device can be a dedicated SD-WAN device of one of Check Point's technology partners or it can be any type of simple router with the sole purpose of building the two tunnels. This type of architecture is often considered for branches with old hardware that does not support the latest firmware and software versions and is therefore not able to protect against modern-day threats. Building an IPsec VPN tunnel to a cloud instance is another option, even on very old hardware.

This deployment type is also recommended in case the local SD-WAN appliance is not powerful enough to support a local Check Point VNF running on it (aka the CloudGuard Edge solution).

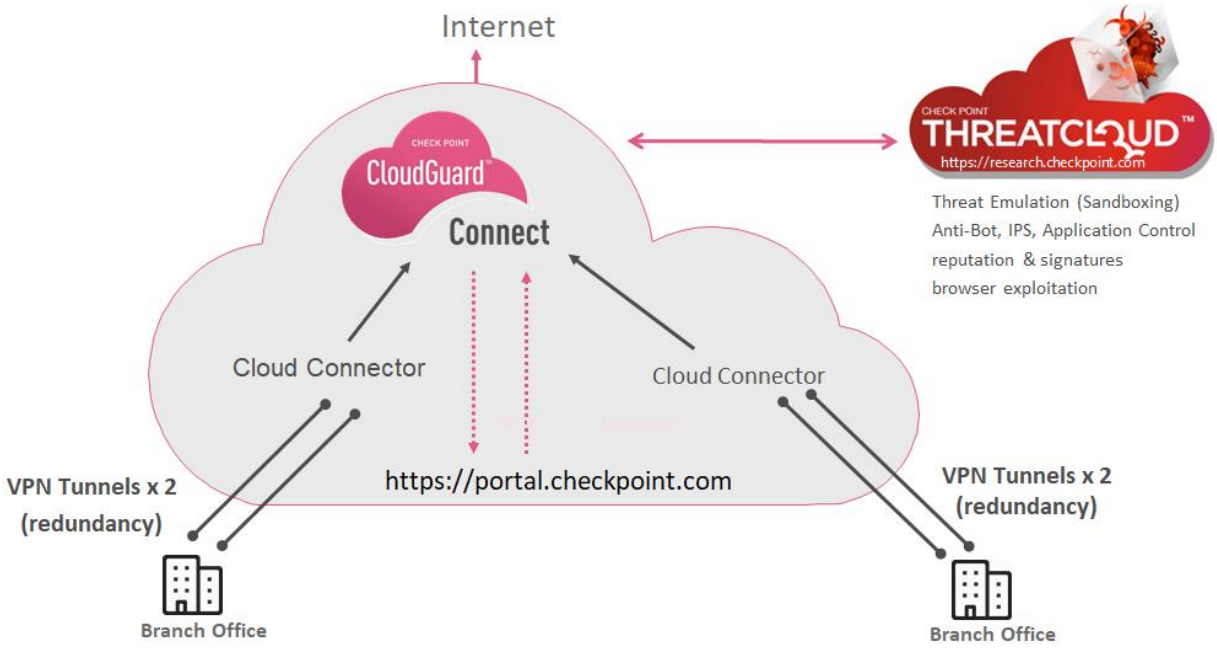
In the following diagram, an SD-WAN device has been used.

It has a redundant pair of tunnels to the CloudGuard Connect data center and another tunnel to the HQ of the enterprise, to allow a local branch to access company resources that have not yet been moved to the cloud.



The tunnel is built from the CPE in the branch to a Cloud Connector, which in turn forwards traffic to the CloudGuard Connect infrastructure: the enforcement point.

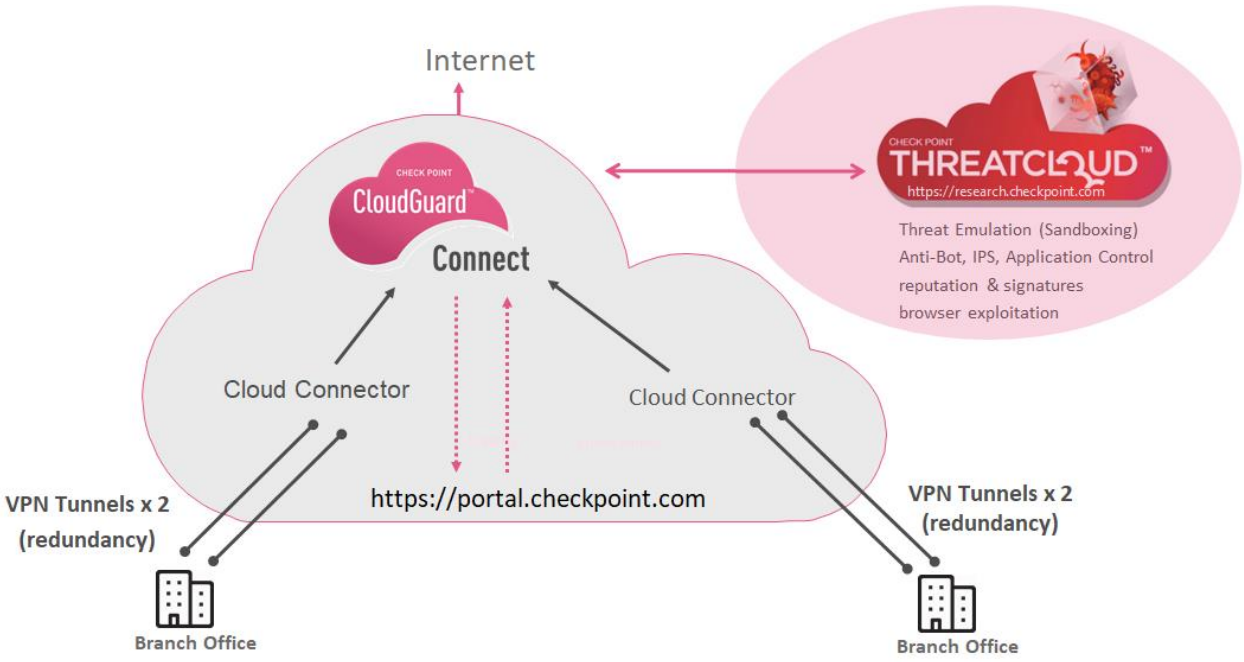
This is where all the security controls are enforced and can be managed from SmartConsole or via the Infinity Web portal.



The CloudGuard infrastructure is automatically updated to the latest version and immediately scales according to the customer's capacity needs.

This translates to not having to deal with the networking platform, upgrades, scalability, and redundancy: it is all delivered automatically, as a service.

Check Point's ThreatCloud is designed to prevent the most sophisticated attacks and is Check Point's most valued security technology on top of the SD-WAN network optimizations.



ThreatCloud is the cloud-based threat prevention mechanism that allows for all the advanced security controls to be at the application layer, therefore preventing both known and unknown attacks. ThreatCloud is used by all of Check Point's products.

How it works: When a new threat is first discovered and successfully blocked with sandboxing technology, a signature is created for it and any other customer using the ThreatCloud will benefit from it as it will automatically get blocked if it is seen elsewhere.

How should Internet traffic be routed?

It all depends on the destination and how secure it is.

SaaS applications such as Salesforce, Office 365, Dropbox, and the likes can be secured with a Check Point cloud instance using APIs. In such cases, this type of traffic can be trusted and can be accessed from the edge device directly. Also, sending SaaS and IaaS traffic directly across the Internet from the branch ensures the best response time and quality of experience for the user.

However, there are other cloud apps, and Internet-bound flows, that are less trusted or secure and may require additional screening. It is suggested to send this type of traffic to the CloudGuard Connect instance. Alternatively, it

could be sent to the HQ where the perimeter gateway can take care of the additional screening. This decision should be made based on the response time and security controls that are required.

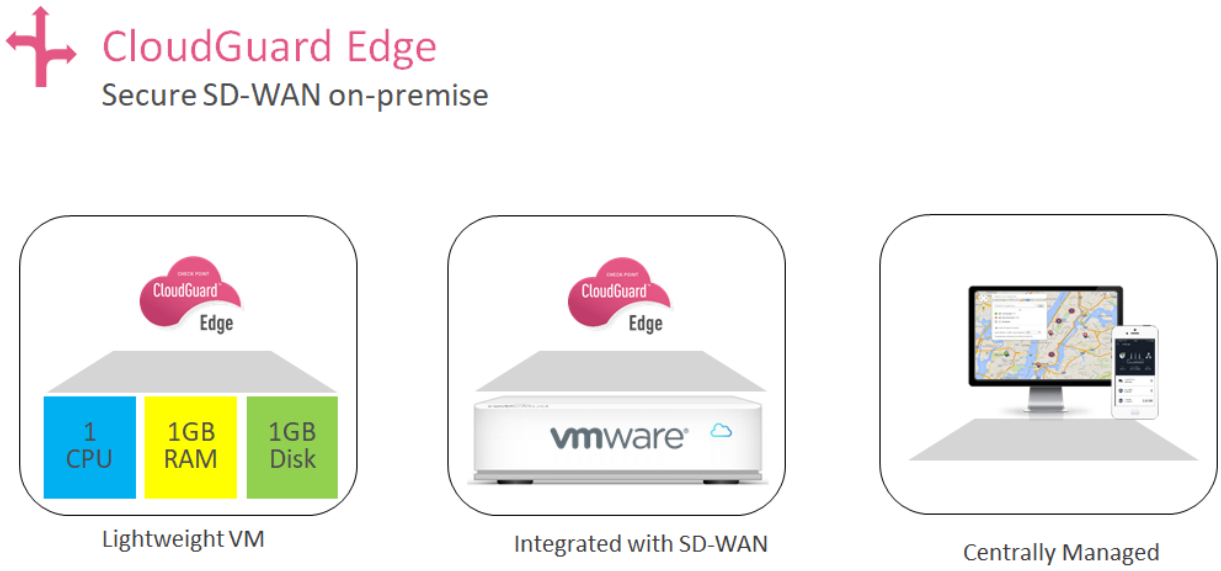
In some cases, branch-to-branch communication is needed (i.e. for VoIP traffic or IP video conferencing). For this type of traffic, QoS is usually a requirement and the Internet does not support it. Therefore, it is recommended to route this type of traffic over a private network that supports end-to-end QoS, such as MPLS.

In case MPLS has been entirely decommissioned in favor of multiple Internet links, the local SD-WAN appliance can pick the best path (i.e. with the lowest latency and jitter) and send the VoIP traffic over it. It should be noted that there are no guarantees for the quality of the call in this case.

Finally, it is recommended to encrypt the VoIP traffic if it is sent over a public medium like the Internet, to prevent eavesdropping.

CloudGuard Edge

When using CloudGuard Edge, the CPE is required to be a dedicated SD-WAN device, capable of running a Check Point Virtualized Network Function (VNF). The VNF is essentially a Check Point gateway running as a Virtual Machine on the SD-WAN appliance; it is a small footprint image that requires little resources and runs on a VMware VeloCloud appliance.



The main difference between CloudGuard Connect and CloudGuard Edge is that inbound traffic to servers in the branch office can be allowed, in the case of CloudGuard Edge.

There is also no need to route any Internet-bound traffic to a Check Point cloud instance as all the necessary security controls are enforced locally on the VNF before it leaves the SD-WAN appliance.

Enhanced privacy is an additional advantage of inspecting the traffic locally instead of routing it to a cloud instance. In this case, the data does not leave the branch before inspection.

Check Point and VMware® SD-WAN by VeloCloud™ have partnered to assure the performance and security of enterprise cloud applications over the Internet and hybrid-WAN, while dramatically simplifying deployments and reducing costs.

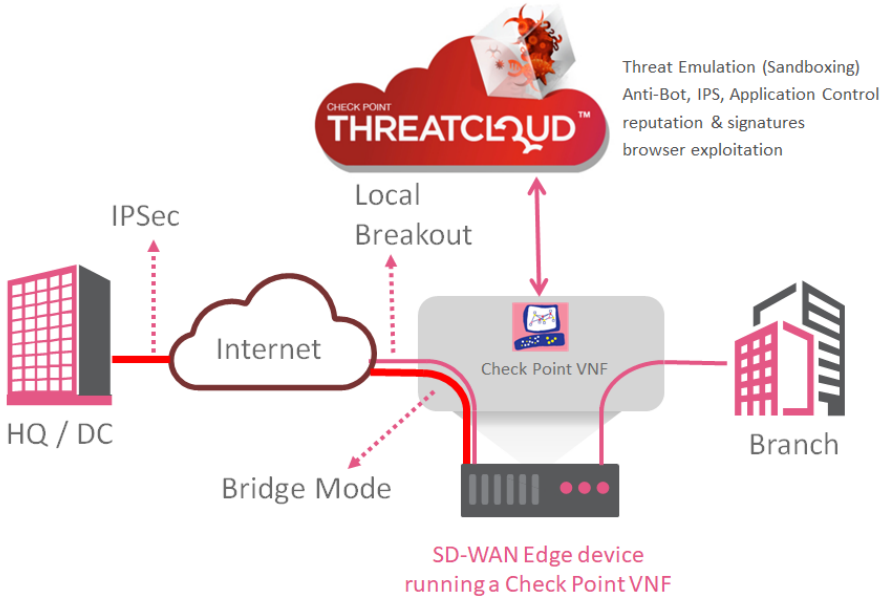
VMware SD-WAN by VeloCloud is the industry's most widely-deployed branch and data center connectivity platform that enables simple, agile, and more secure branch connectivity for thousands of customers globally. The solution establishes a secure and optimized overlay network between VMware SD-WAN Edges in distributed sites or data centers and cloud-hosted VMware SD-WAN gateways. The overlay is independent of physical transport and providers, enabling unified control and visibility, business-level abstraction, and incremental migration.

The key benefits include:

- Assured application performance: VMware SD-WAN Dynamic Multipath Optimization™ (DMPO) with application-aware, per-packet steering, and on-demand remediation, assures transport-independent performance for demanding, real-time applications.

- Simplified WAN via business policy automation: VMware SD-WAN can be deployed as zero-touch appliances, virtual appliances, or hosted as multi-tenant service platforms. Business-level policies enable one-click, policy-based service chaining of traffic, e.g. Check Point firewall insertion, to enterprise service hubs on the branch edge or in the cloud.

- Managed cloud on-ramp: VMware SD-WAN's system of cloud gateways uniquely provides a managed cloud onramp. Unlike "best-effort" direct branch-to-cloud alternatives, the full capabilities of VMware SD-WAN are deployed at the doorstep of cloud apps and provide optimized and secure connectivity to SaaS, IaaS, and network or cloud security services.



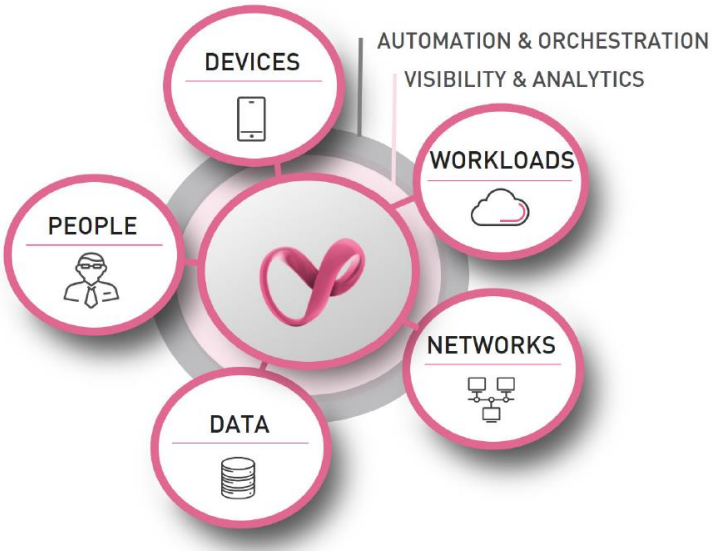
In the above deployment scenario, the Check Point VNF running in layer two mode interacts directly with the Check Point ThreatCloud to enforce all the advanced security controls.

Both CloudGuard Connect and CloudGuard Edge are compatible with the VMware CPE.

Align with the zero trust model

Choosing the right architecture for branches will lead to a correctly segmented and secured environment.

Remember: never trust, always verify!



- **Zero trust network:**
  In case inbound access is required, CloudGuard edge can be used to segment the DMZ from the user's segment and apply the necessary security controls between the segments. Either the local VNF, the security gateway, or CloudGuard Connect instance will segment the branch from the next hop, which will protect the corporate network from lateral malware movements.

- **Zero trust people:**
  Use Identity Awareness on the CloudGuard Edge VNF, or on the CloudGuard Connect instance, to verify the identity of users.

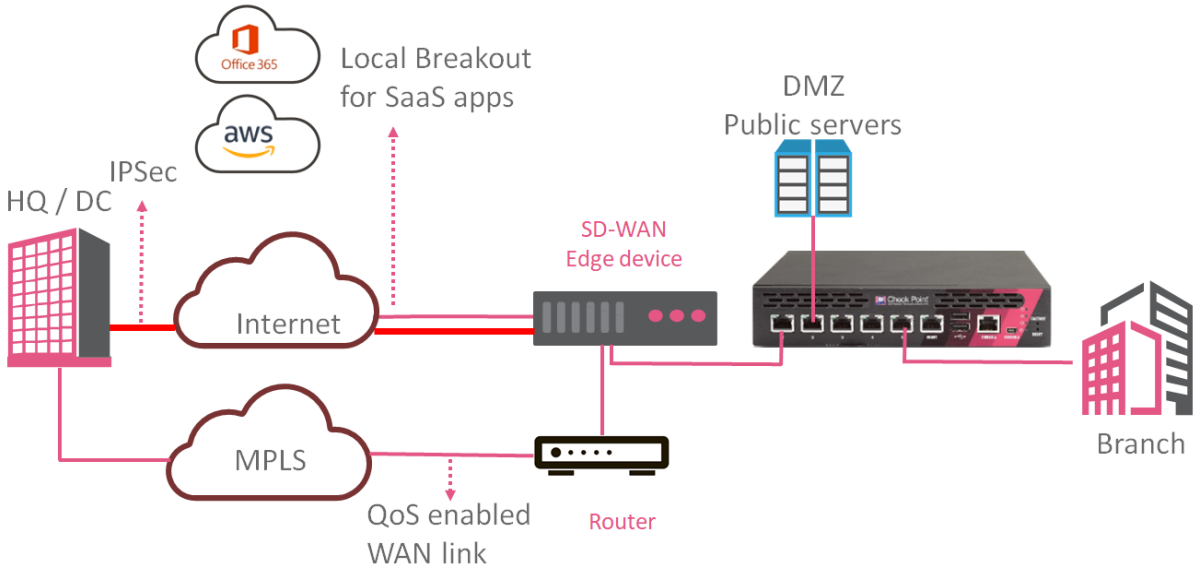
- **Zero trust devices:**
  Enforce the installation of on-device security protection for all employee devices (including BYOD), to prevent zero-day malware, malicious app installations, phishing attacks, bot attacks, and more. (Please note that this is not a feature of CloudGuard Connect or Edge.)

- **Zero trust data:**
  The DLP blade can be enabled on the CloudGuard Edge product, and content awareness can be enabled on the CloudGuard Connect instance.

- **Zero trust workloads:**
  Enable full threat prevention for all south-north communication between the branch and data center/ IaaS assets/ SaaS apps.

Use cases

Check Point gateway + SD-WAN appliance



Two circuits in the Branch: Internet and MPLS.

On-premise hardware: a Check Point security gateway, an SD-WAN appliance, and an MPLS router.

The local Check Point security gateway enforces the required NGTP security controls for outbound traffic towards the Internet and secures the inbound traffic towards the DMZ.

In this case, CloudGuard Connect is not an option as inbound access to the DMZ is required.

The local SDWAN device takes care of the dynamic path selection:

- MPLS for Branch-to-HQ traffic that requires QoS (i.e. VoIP, video conferencing)
- Direct Internet breakout for cloud-based IaaS and SaaS services (AWS, O365…)
- IPSec VPN for access to the data center in the HQ using the local Internet line. There is no QoS for this type of traffic as it flows via the Internet, but it is encrypted for privacy reasons.

Required products:

- An SD-WAN appliance of choice
- A Check Point gateway
- A WAN router

Pros:

- Inbound access to the DMZ is possible
- Segmentation of the DMZ and the users
- Dedicated QoS between the HQ and Branch
- Dynamic path selection is done by the SD-WAN device

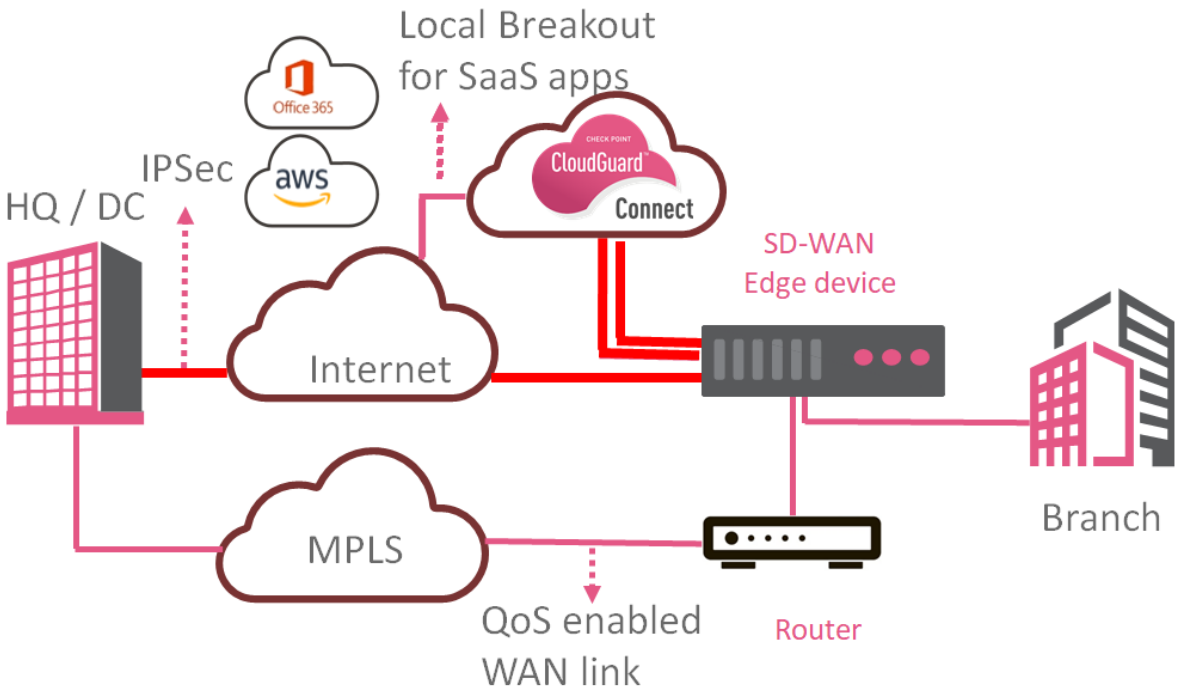
Cons:

- Three different solutions managed by different platforms; no single pane of glass
- Triple the hardware maintenance and support required per platform
- Troubleshooting on three platforms can be complicated
- Expensive WAN costs

Conclusion:

- Check Point recommends using this type of architecture in the case of the local Check Point gateway and SD-WAN only recently having been purchased and there being no need to replace either one with another solution.
- There is a possibility to move to CloudGuard Edge in the future once the local Check Point gateway and/or SD-WAN appliance have been written off.
- The local gateway can be replaced with a Check Point VNF running on the SD-WAN appliance, provided it is powerful enough.
- CloudGuard Connect is never an option here as inbound access to the DMZ is required.
- The only reason to keep this type of architecture is because the SD-WAN appliance will never support running a Check Point VNF on it.

SD-WAN appliance with CloudGuard Connect



Two circuits in the Branch: Internet and MPLS.

On-premise hardware: an SD-WAN appliance and an MPLS router.

The local SD-WAN appliance builds a pair of redundant IPSec or GRE tunnels to the Check Point CloudGuard Connect infrastructure, which enforces the required NGTP security controls for outbound traffic towards the Internet. The SD-WAN appliance also builds an IPSec VPN tunnel to the HQ so resources in the data center can be accessed securely.

In this case, CloudGuard Connect is chosen because the local SD-WAN appliance is not powerful enough to run a Check Point VNF on it.

The local SDWAN device takes care of the dynamic path selection:

- MPLS for Branch-to-HQ traffic that requires QoS (i.e. VoIP, video conferencing)
- Direct Internet breakout for cloud-based IaaS and SaaS services (AWS, O365…)
- IPSec VPN for access to the data center in the HQ using the local Internet line. There is no QoS for this type of traffic as it flows via the Internet, but it is encrypted for privacy reasons.

Required products:

- An SD-WAN appliance of choice
- A WAN router

Pros:

- Dedicated QoS between the HQ and Branch
- Dynamic path selection is done by the SD-WAN device
- Easy to scale in terms of users and bandwidth; no forklift upgrades required unless the bandwidth exceeds the performance limits of the CPE

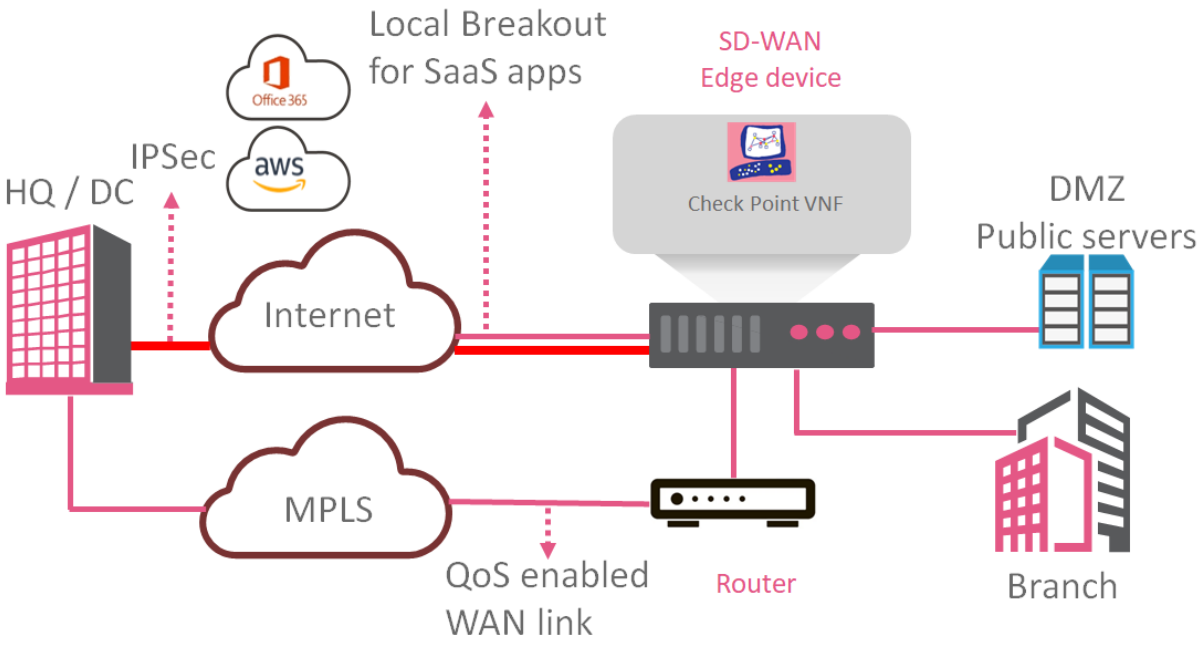
Cons:

- Inbound access is not possible

Conclusion:

- If the local SD-WAN appliance is powerful enough, CloudGuard Edge is also an option, which will be discussed in the next use case.
- This type of scenario is not an option in case inbound access to public servers in the DMZ is a requirement.
- In case no inbound access is required, CloudGuard connect is the ideal product.

SD-WAN appliance with CloudGuard Edge



Two circuits in the Branch: Internet and MPLS.

On-premise hardware: an SD-WAN appliance and an MPLS router.

The local SD-WAN appliance has a Check Point VNF running on it, which enforces the required NGTP security controls for outbound traffic towards the Internet and secures the inbound traffic towards the DMZ.

The SD-WAN appliance also builds an IPsec VPN tunnel to the HQ so resources in the data center can be accessed securely.

In this case, CloudGuard Edge is chosen because inbound access is a requirement.

The local SDWAN device takes care of the dynamic path selection:

- MPLS for Branch-to-HQ traffic that requires QoS (i.e. VoIP, video conferencing)
- Direct Internet breakout for cloud-based IaaS and SaaS services (AWS, O365…)
- IPSec VPN for access to the data center in the HQ using the local Internet line. There is no QoS for this type of traffic as it flows via the Internet, but it is encrypted for privacy reasons.

Required products:

- An SD-WAN appliance of choice (provided it is powerful enough to run a Check Point VNF on it)
- A WAN router

Pros:

- Dedicated QoS between the HQ and Branch
- Dynamic path selection is done by the SD-WAN device
- Inbound access is possible
- Segmentation of the LAN is possible

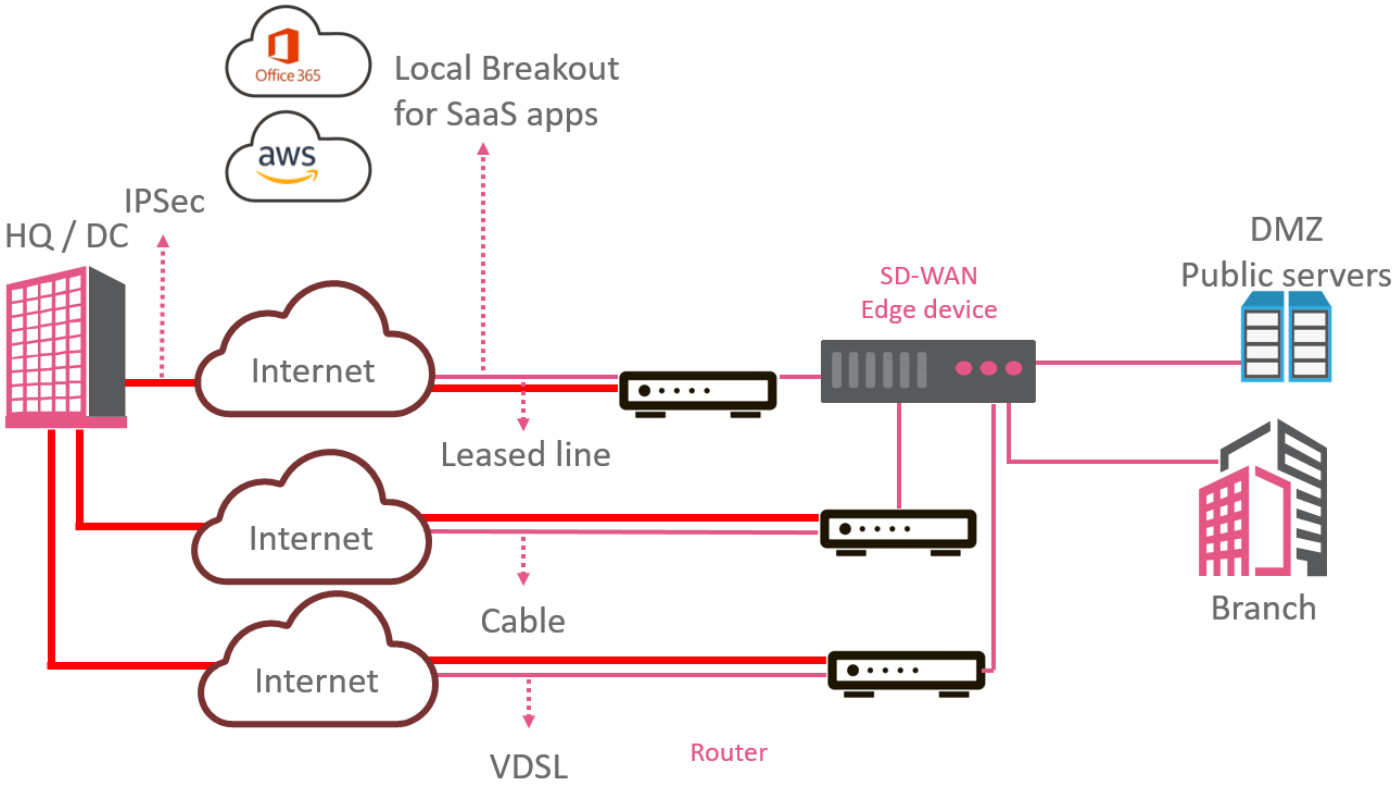
Cons:

- Expensive MPLS circuits are still in place, no real WAN cost reduction

Conclusion:

- For this type of environment, CloudGuard Edge is the ideal product.

SD-WAN appliance, CloudGuard Connect & multiple ISP links



Three circuits in the Branch: a leased line and two broadband connections.

On-premise hardware: an SD-WAN appliance and three routers.

The local SD-WAN appliance has two redundant tunnels to the Check Point CloudGuard Connect infrastructure, where all the necessary NGTP security controls for outbound traffic are enforced.

The SD-WAN appliance also builds three IPsec VPN tunnels to the HQ so resources in the data center can be accessed securely.

The local SD-WAN device takes care of the dynamic path selection:

- Instead of an expensive MPLS circuit, dynamic path selection takes place to pick the best tunnel to the HQ in terms of response time, latency, and jitter. There is no guaranteed QoS over any of the three links, but the likelihood of several ISP links all offering subpar performance for latency-sensitive traffic *at the same time* is quite low. This is usually sufficient for branch offices

- Direct Internet breakout for cloud-based IaaS and SaaS services (AWS, O365…).

Required products:

- An SD-WAN appliance of choice
- A WAN router for the leased line and two modems: one for the VDSL line and one cable modem

Pros:

- Cost reduction by eliminating the expensive MPLS circuit
- Dynamic path selection is done by the SD-WAN device
- Easy to scale in terms of users and bandwidth; no forklift upgrades required unless the bandwidth exceeds the performance limits of the CPE

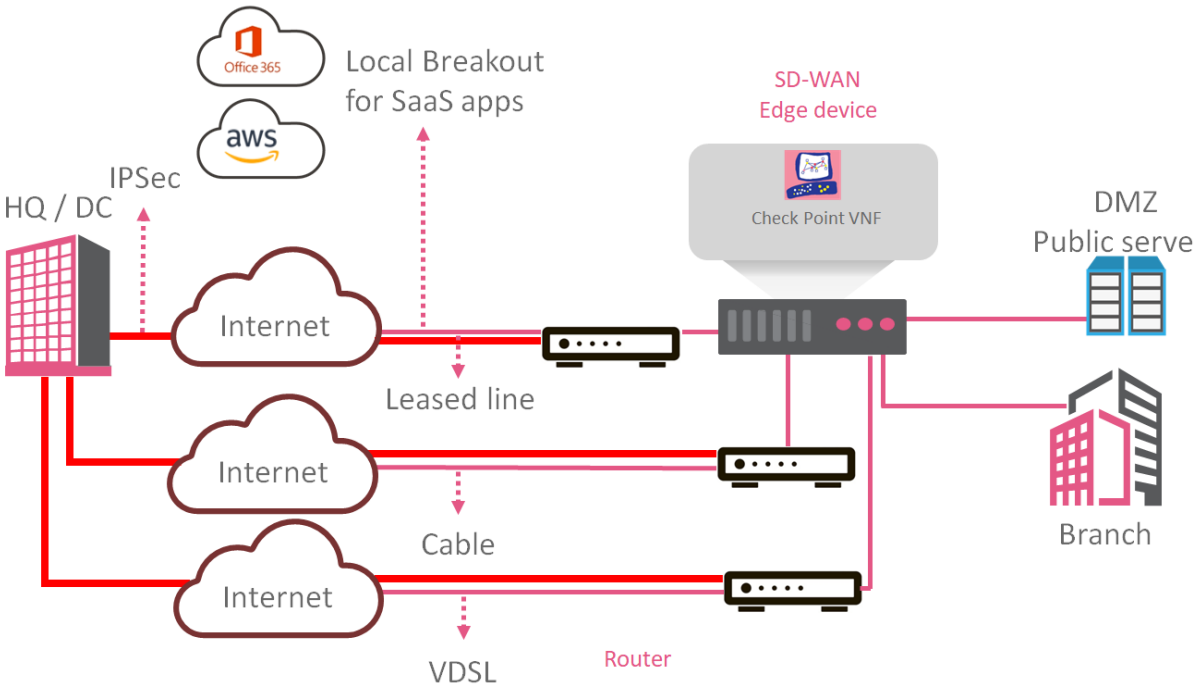
Cons:

- Inbound access is not possible
- No local segmentation possible
- No guaranteed QoS possible, however, this is the tradeoff that was made to reduce TCO by eliminating the MPLS circuit

Conclusion:

- If local segmentation is not required (i.e. only one subnet with users and no other resources), CloudGuard Connect is the ideal product.

SD-WAN appliance, CloudGuard Edge & multiple ISP links



Three circuits in the Branch: a leased line and two broadband connections.

On-premise hardware: public resources in the DMZ, an SD-WAN appliance, and three routers.

The local SD-WAN appliance has a Check Point VNF running on it, which enforces the required NGTP security controls for outbound traffic towards the Internet, and secures the inbound traffic towards the DMZ.

The SD-WAN appliance also builds three IPsec VPN tunnels to the HQ, so resources in the data center can be accessed securely.

In this case, CloudGuard Edge is chosen because inbound access is a requirement.

The local SD-WAN device takes care of the dynamic path selection:

- Instead of an expensive MPLS circuit, dynamic path selection takes place to pick the best tunnel to the HQ in terms of response time, latency, and jitter. There is no guaranteed QoS over any of the three links, but the likelihood of several ISP links all offering subpar performance for latency-sensitive traffic *at the same time* is quite low. This is usually sufficient for branch offices

- Direct Internet breakout for cloud-based IaaS and SaaS services (AWS, O365…).

Required products:

- An SD-WAN appliance of choice (must be powerful enough to run a Check Point VNF on it)
- A WAN router for the leased line and two modems: one for the VDSL line and one cable modem

Pros:

- Cost reduction by eliminating the expensive MPLS circuit
- Dynamic path selection is done by the SD-WAN device
- Inbound access is possible
- Local segmentation of the LAN is possible

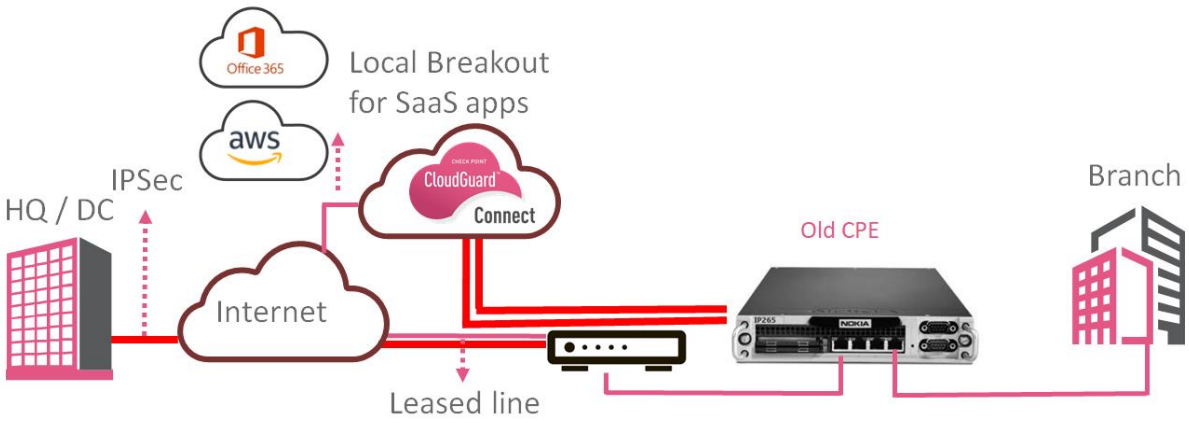
Cons:

- No guaranteed QoS possible, however, this is the tradeoff that was made to reduce TCO by eliminating the MPLS circuit.

Conclusion:

- Because inbound access is a requirement, CloudGuard Edge is the ideal product.

Local CPE is EOL but cannot be replaced



One circuit in the Branch: a leased line.

There is a need for a local Internet break out to access SaaS applications directly. However, the local hardware is too old to run the full stack of NGTP security controls.

On-premise hardware: an EOL security gateway capable of building two IPsec tunnels.

The local gateway has two redundant tunnels to the Check Point CloudGuard Connect infrastructure, where all the necessary NGTP security controls for outbound traffic are enforced.

The local gateway also builds an IPsec VPN tunnel to the HQ so resources in the data center can be accessed securely.

Required products:

- No additional hardware is required

Pros:

- There is no need to invest in any additional hardware, therefore enabling a window for migration towards a dedicated SD-WAN architecture with multiple access circuits, like in use case four
- Access to SaaS applications is now locally possible without having to make any architectural changes to the network in remote sites
- Local segmentation of the LAN is still possible but running IPS between the segments may not be possible (dependent on the hardware)
- Easy to scale in terms of users and bandwidth; no forklift upgrades required unless the bandwidth exceeds the performance limits of the CPE

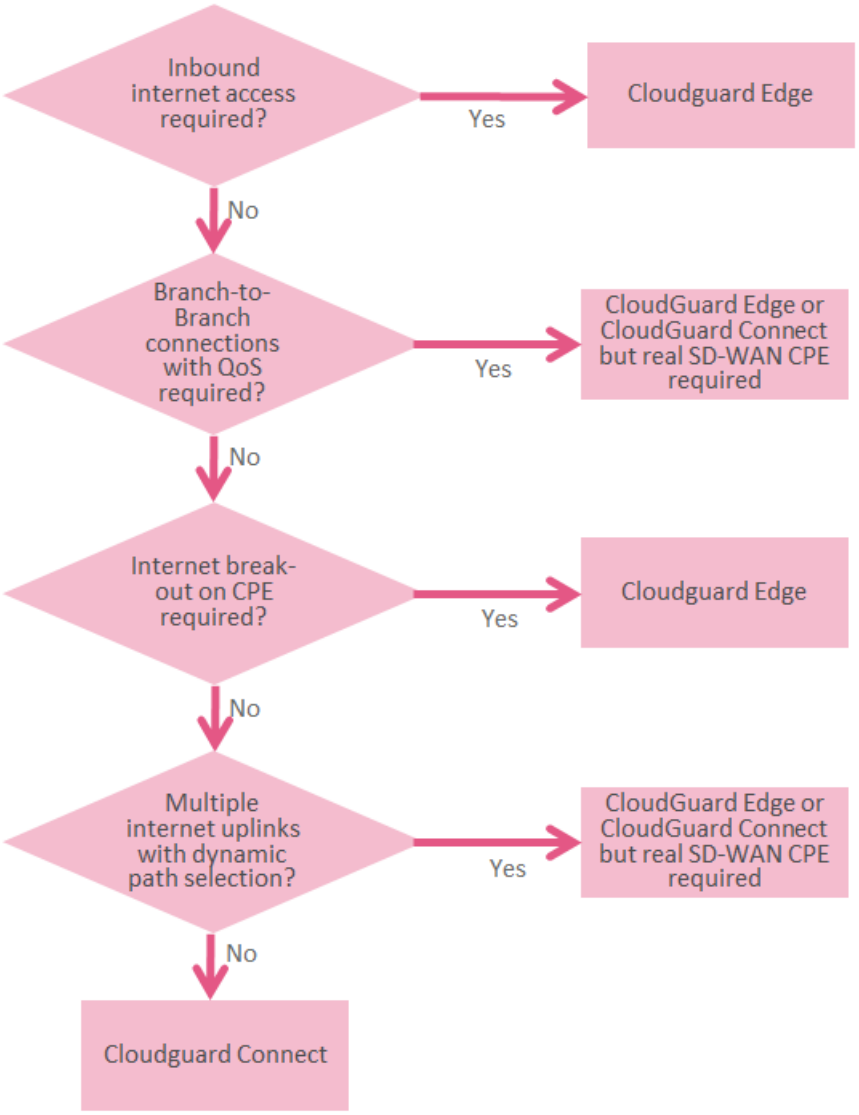
Cons:

- Inbound access is not possible
- No guaranteed QoS possible as all traffic traverses the Internet

Conclusion:

- CloudGuard Connect is the only possible product in this case.

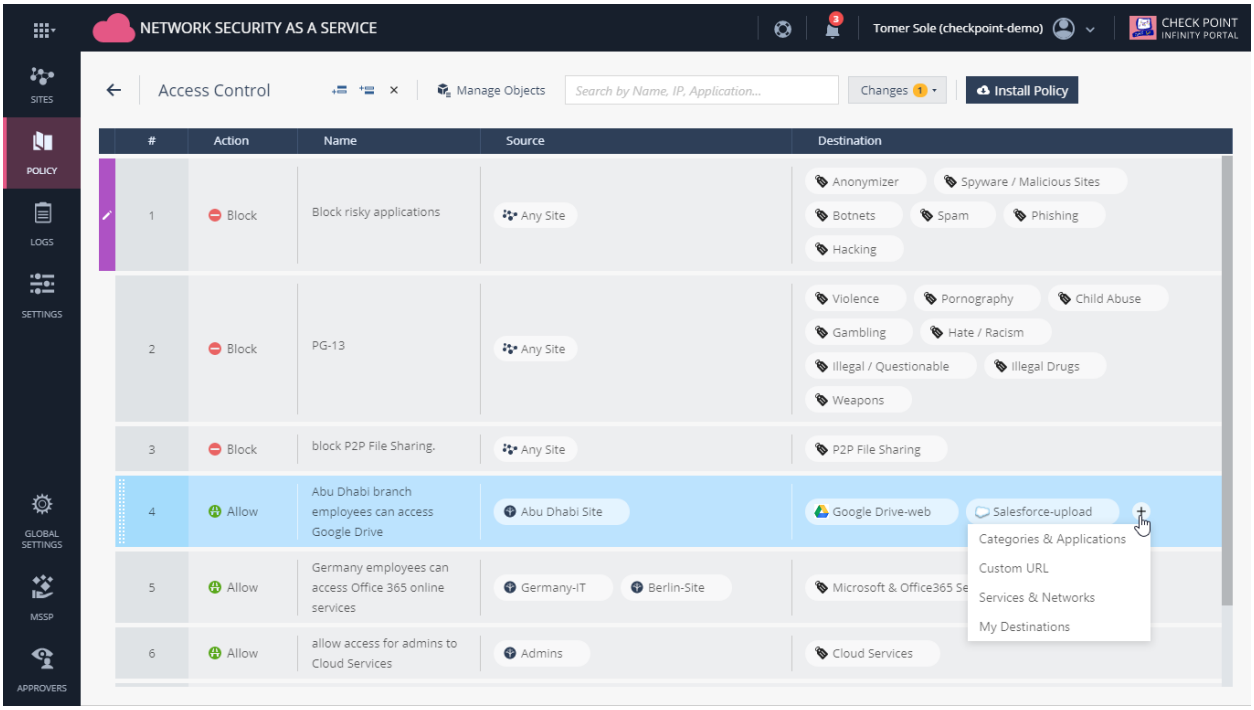
Summary: How to choose between the two solutions?



Management and reporting

CloudGuard Connect is managed via the Infinity Portal and also with an R80.20, or above SmartCenter.

The following is a screenshot of the Infinity Portal:

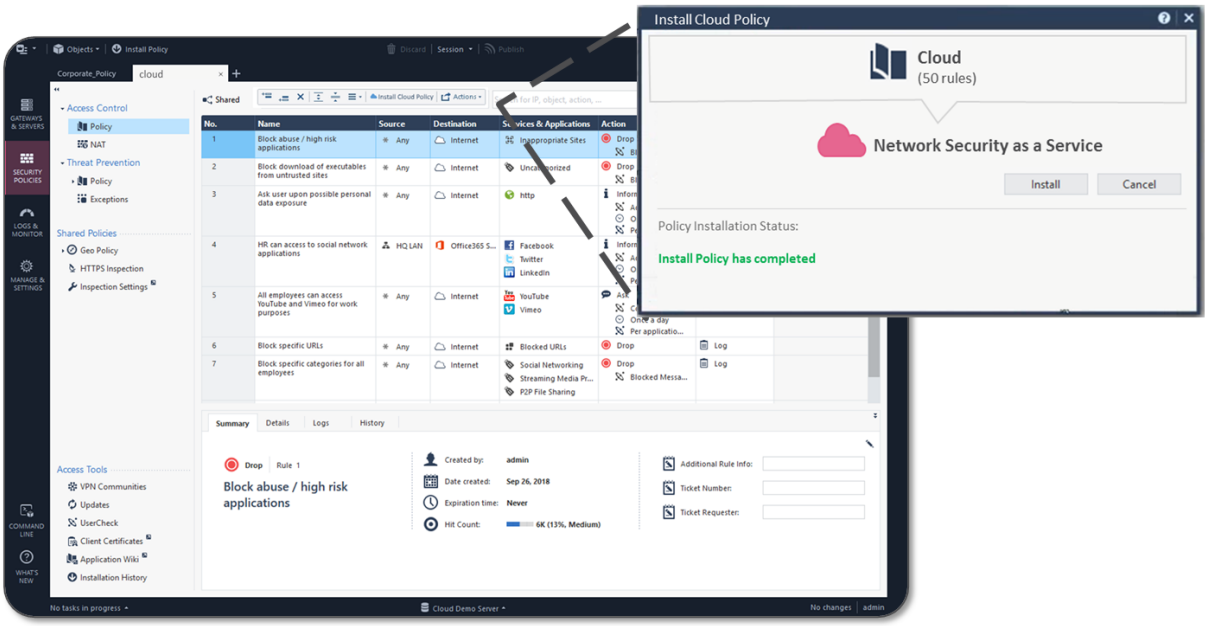


Benefits for managing Internet policy within the Infinity Portal:

- The destination column consolidates applications, custom IP's and custom URL's
- A single, unified policy for all branch offices ensures central management
- The first three predefined security policy rules in the security portal are out-of-the-box-defaults which secure branch offices with zero customization.

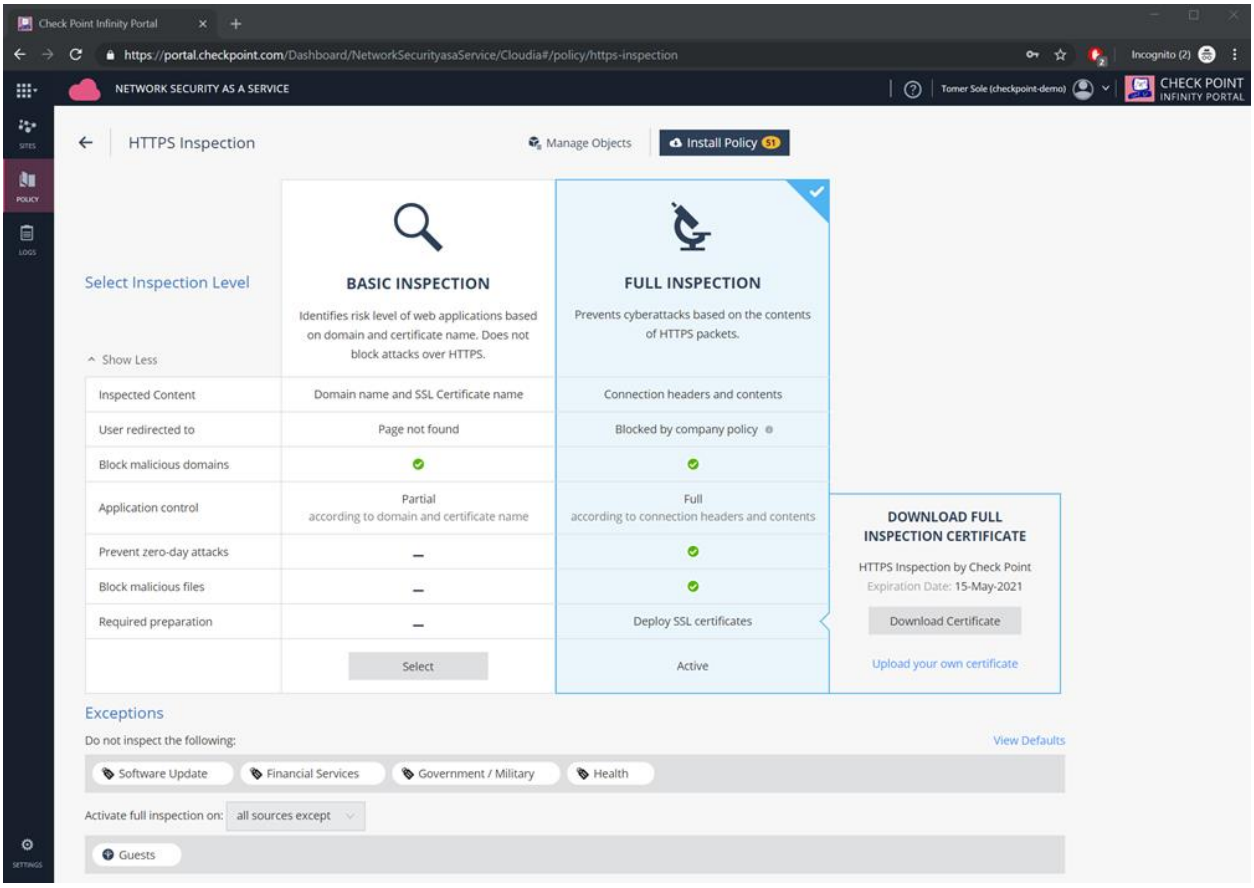
Another option is to manage the SD-WAN policy using an >R80.20 management station.

This method is supported both by CloudGuard Edge and CloudGuard Connect.



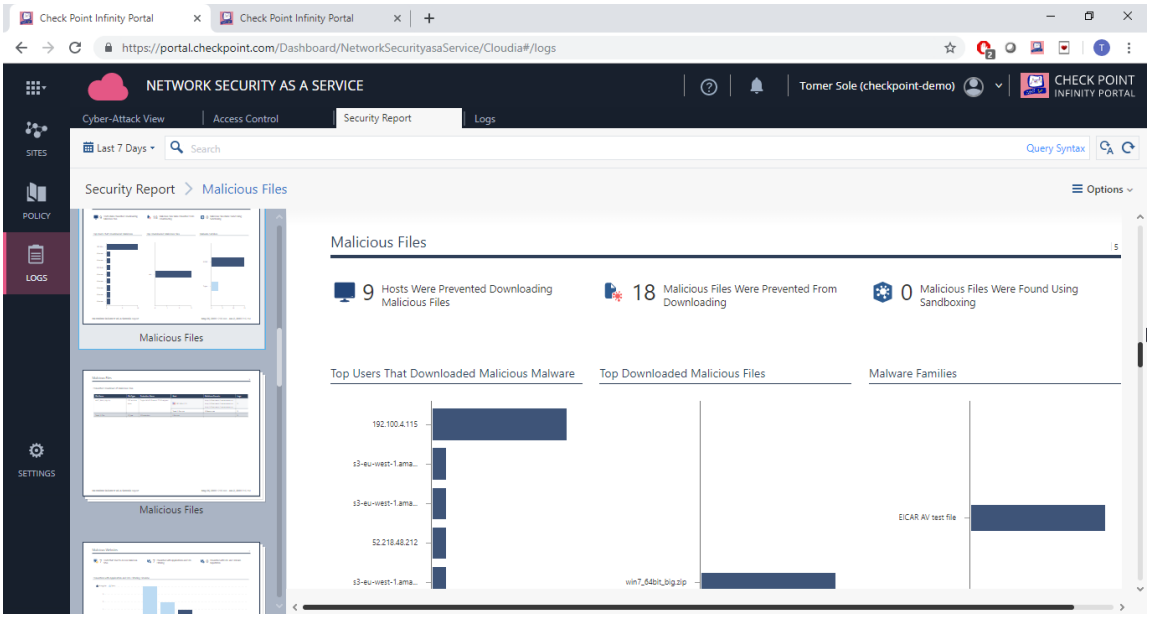
The CloudGuard Edge VNF is a gateway SMB image, so it can be managed by the local web, SMP cloud web management, or by SmartConsole of any version that supports Check Point's Large-Scale Management (LSM), which is essentially any version except for R80.10.

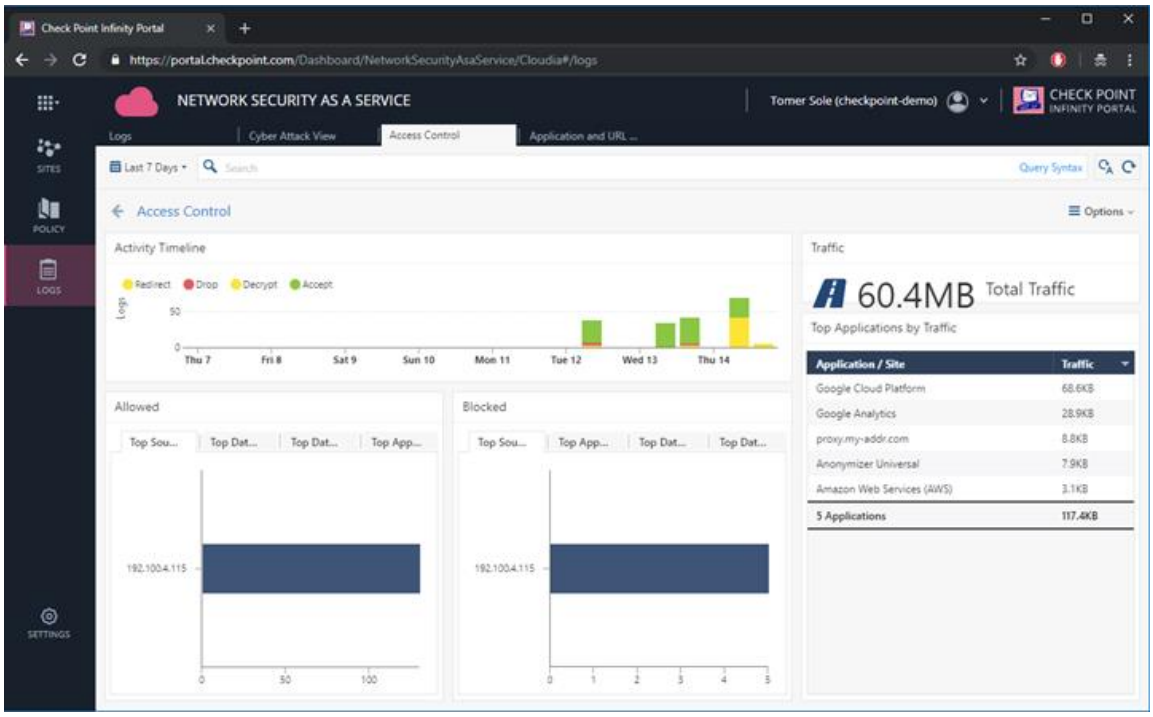
Full HTTPS inspection is also supported:



As can be seen at the bottom of the screenshot, HTTPS inspection can be bypassed for traffic originating from specific sources at the branch office.

Examples of a weekly threat report and logs:





Conclusion:

Redesigning an existing Wide Area Network is an excellent opportunity to enhance business agility, reduce costs, and increase security.

However, SD-WAN technology is not a single product that fits all possible enterprise security needs.

Check Point's CloudGuard Connect and CloudGuard Edge are two versatile products that can easily be deployed, to help support SD-WAN technology, and meet the specific needs of each business and their unique infrastructure.

Contact your local Check Point team for assistance in easily boosting your cyber security measures, today.