Data Center Handbook

For CounterPoint Business Partners

Contents

About the Data Center..... 2

What Makes Our Data Center Different?..... 3

Basic Requirements for the Data Center..... 5

Infrastructure Requirements and Recommendations..... 6

Data Center Do's and Don'ts..... 8

Remote Backup Services..... 11

How to Quote the Data Center..... 12

IPSEC Tunnel Overview..... 13

FAQ's..... 14

About the Data Center

More and more retailers and their CounterPoint partners are realizing that Cloud Computing and Managed Hosting is a smart business decision. Choosing the right hosting provider allows your Customers to benefit from reduced risk, greater peace of mind, predictable IT costs and a reduction in their IT staffing/Infrastructure. Partners enjoy a renewable revenue stream, better security for their Customers and a highly sought after service to sell. RCS delivers the same cutting-edge technology and best practices employed by national providers and makes it available to you and your Customers.

RCS approaches hosting from the perspective of Partners and their Customers' needs by supporting a wide range of requirements from a single server to extremely complex environments. With a dedicated hosting and support team, you'll benefit from the full time monitoring and management of your systems where we become your technology partner, allowing you to focus on selling and supporting and your Customers to focus on what matters most — their Customers and business.

What to expect from a first class Data Center

Making sure that your data is secure will give you peace of mind and keep your business operating smoothly. This is what you can expect when you host with RCS

- 24x7x365 Physical and electronic security.
- Climate Controlled Facility with full redundancy for temperature and humidity.
- 24x7x365 Server health & performance monitoring.
- Antivirus and three levels of Backup protection.
- 24x7x365 Firewall Management and monitoring and PCI compliant server configurations
- Numerous redundant internet backbone connections
- Redundant server hardware and a full week of diesel back up power with redundant generators
- Routine patching for security and functionality. Patches tested for compatibility.
- SAE 16 (SAS 70 I & II), and PCI DSS Compliant

Benefits of the RCS Data Center PCI Compliant Hosting Solution

- The ability to quickly scale your solution and bandwidth as your business changes
- The ability to use both collocation and managed hosting depending on your requirements
- Equipment that is protected in safe and highly secure data centers.
- Always on environment with redundant power, connectivity and environmental controls.
- 24x7x365 on-site support provided by experienced data center engineers
- Driven to listen to our clients and always exceed their needs and expectations
- Industry leading Service Level Agreements (SLAs)

PCI Compliant Hosting Solution

The Payment Card Industry Data Security Standard, frequently referred to as PCI, applies to organizations that store or transmit credit card data. PCI Compliance is a large responsibility and it requires many economic and technical resources. The hosting environment provides you and your Customers a smoother path to achieve PCI compliance. This allows those precious resources to be spent elsewhere.

What makes our Data Center Different?

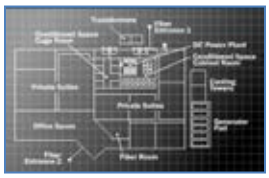
Support. Experience. Technology.

When you host with RCS your data is in a top tier facility and is managed by an incredibly experienced and responsive team.

RCS constantly invests in the technology and the knowledge to stay current with all systems from security, to servers, to software. RCS maintains the training of dedicated staff and has direct access 24 hours a day to onsite datacenter engineers. This approach has paid off for our customers; they enjoy a 99.9+ uptime four years running.

Radiant Systems, the makers of CounterPoint, regularly seek information from RCS on all matters related to hosting software and datacenter operations because of RCS' deep knowledge on the subject and track record of superior performance.

Datacenter Basics



- 100,000 SF+ Facility with expansion capabilities to Over 250,000 square feet
- Managed 24x7x365 by on-site Network Operation Center with a second independent NOC at a separate datacenter to ensure security and overwatch.
- SSAE 16 SOC I Certified (formerly known as SAS-70)

Power Architecture

- 5000 Amp 480v AC Main Paralleling switchgear
- Up to 10,000 Amp DC power plant
- Back-up power provided by four 1,000 KW, Fully Redundant Diesel Generators
- Redundant Liebert & Mitsubishi UPS Systems
- A PVC Conduit is provided from the main building for grounding

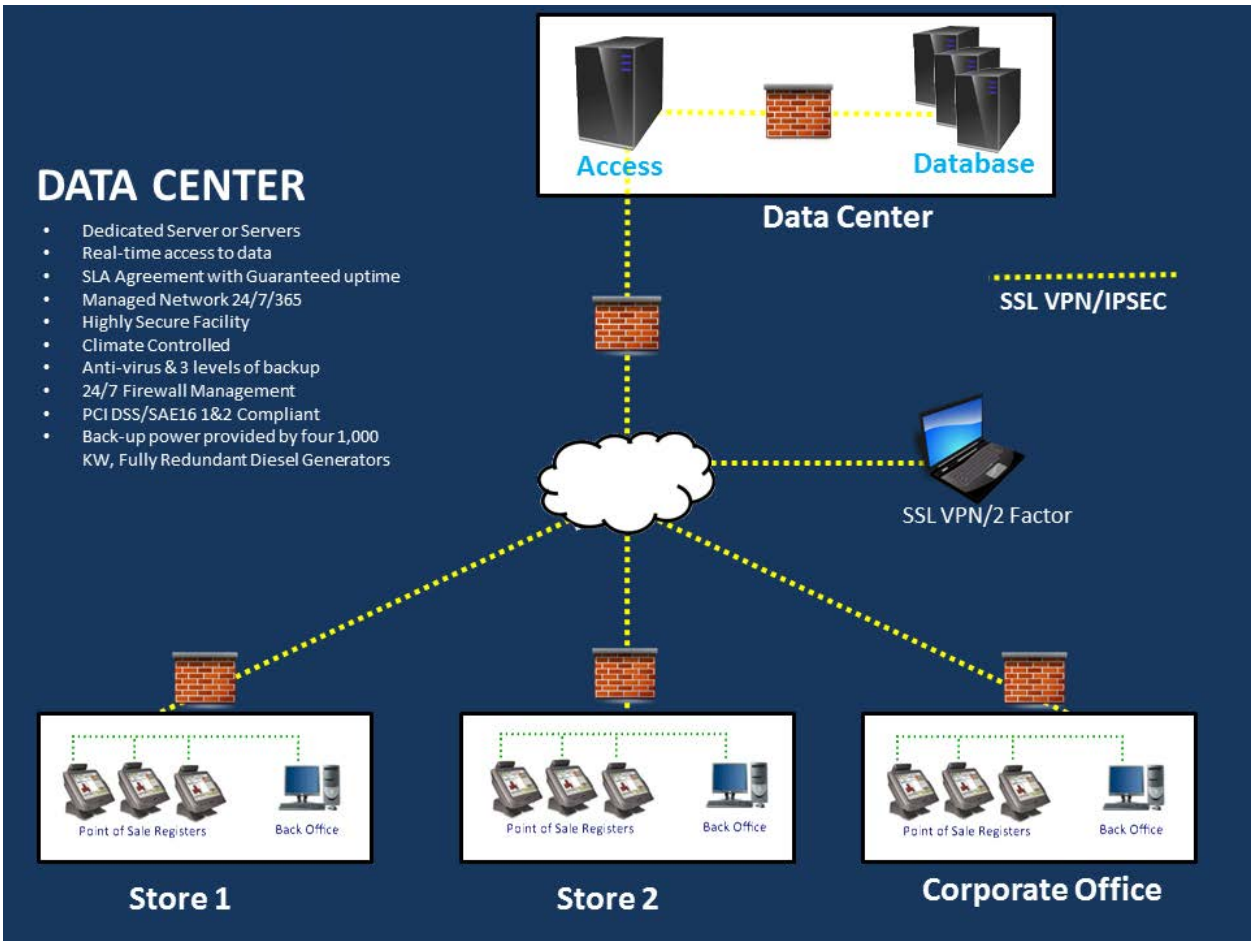
Network Architecture

- Dual Path Fiber Entrances from Diverse Fiber Rings & Copper Facilities
- Multi-Gigabit Ethernet IP Backbone with Level 3, AT&T, Global Crossing & Internap Services
- Carrier Neutrality – Ability to accept circuits from all carriers:
- Verizon, AT&T, Expedient/Yipes, Veroxity, One Communications, Qwest, Lightower & RCN/Neon, Comcast and Level3 all have fiber onsite

Environmental Controls

- Temperatures maintained between 65°-75°F and humidity between 40-60%.
- Environment monitored through building automation AND a Third Party Vendor
- Fire Suppression is a double, preaction, dry system linked to smoke and heat detectors.
- 24x7x365 NOC Staff, Monitoring, Facility Access, Video Surveillance & Security.
- Multiple 30 Ton Liebert Units provide cooling for the facility

Data Center Architecture



Basic Requirements for the Data Center

Internet Service

Static IP Service capable of supporting "bridge mode"
Hardware firewall
Business Class Cable, DSL or T1
Minimum bandwidth up to 5 machines: 1.5 MB down and 768K up

Notes

Streaming audio, video and web based security cameras, voice over IP phones and public or mis-configured WIFI can significantly impact performance.

Different provider's quality of connection can vary depending on service type.

Register users tend to need more bandwidth than back office users.

The Ideal Connection

Stand alone, business class cable internet connection, scaled to the number of connecting machines, with a static IP service, terminating into a commercial grade firewall.

Fail Over

Modem for back off credit card processing
Offline Ticket – in the event of internet interruption.

Hardware Requirements

Hardware must meet the following requirements:

http://www.counterpointpos.com/counterpoint-sql-enterprise-retail-pos-software.htm

Hardware Intake Sheets

These are Excel sheets that detail the environment that your Customer has in place. These sheets allow you to identify any areas of concern prior to deployment. This goes a long way towards a successful implementation. These documents must be filled out prior to client acceptance to the Data Center. To request the intake sheets contact:

support@lparetail.com or call 952-814-4800 ext 1

Infrastructure Requirements and Recommendations

Power

POS units and the networking equipment they connect to require an AC 120V 60Hz outlet for proper power. POS units should be connected to these power sources only through a line conditioner. Line conditioners correct variations in the power that feeds the network equipment and the POS computer(s) and protects them against less than ideal power or damaging conditions within the limits of the line conditioner's capability. Failure to have proper power protection can lead to damaged POS units or erratic behavior such as blue screens, restarts, freezes and problems with connected devices.

Correct power protection for additional network components (switches, routers, firewalls, etc.) is vital as power fluctuations can impact network equipment and cause damage to machines connected to those devices as well as unpredictable network stability or loss of connectivity.

Power lines and outlets should only be installed and tested by an appropriately licensed electrician prior to use.

Firewalls

POS units and their Internet connection must be protected by a properly configured commercial grade firewall in order for you to be in compliance with credit card security requirements. Only a correctly deployed commercial grade firewall contains the capabilities required to protect a credit card handling system including the Counterpoint system.

Common providers of these firewalls include Dell (Sonicwall), Watchguard and Cisco among many others. Your professional IT resource will be able to guide you on acquiring and deploying these devices.

Internet

The hosted Counterpoint system is accessed "live" exclusively through your Internet connection. As such it is imperative that your Internet connection is as stable as possible and meets or exceed the following minimum specifications.

- A business class Internet service
- A static IP address service
- A minimum throughput of 1.5 MB per second download and 756K upload per second for each two POS units connected. 3 MB per second download and 1 MB per second upload speeds are recommended.
- A stable connection with few to no drops in connection or quality.

There are network activities that have the potential to disrupt Counterpoint communications by saturating your Internet connection. These include video and audio streaming, file sharing, hosting

internal services accessible to the Internet (FTP, emailservers, web servers, etc.), VOIP systems, wireless access and many others.

> It is imperative that the Internet service that is used for the Counterpoint system be for Counterpoint alone or have sufficient network rules in place to assure that the Counterpo int system traffic is provided with the needed minimum standard above.

Antimalware

All systems in your network including but especially the Counterpoint system must have properly configured, updated and scheduled antimalware protection installed. This is a requirement not only for best practices of computer security but also for required credit card security compliancy as detailed in the PCIDSS standard.

There are many antimalware providers that offer software solutions sufficient to meet the PCIDSS standard. Some of the better known companies providing this software include AVG, Symantec Corporation, Trend Micro, Sophos and McAfee. Your professional IT resource will be able to guide you on acquiring and deploying this software.

Cabling

Network cabling has many components for optimal performance. Minimally the Counterpoint systems should be provided with individual CAT 5e or CAT 6 network connections that are properly run, terminated and tested according to the TIA/EIA 568A & 568B standards (one or the other, not both). These same standards should be followed for any cabling that provides network access to the POS units (switches, patch panel, routers, firewalls, etc.).

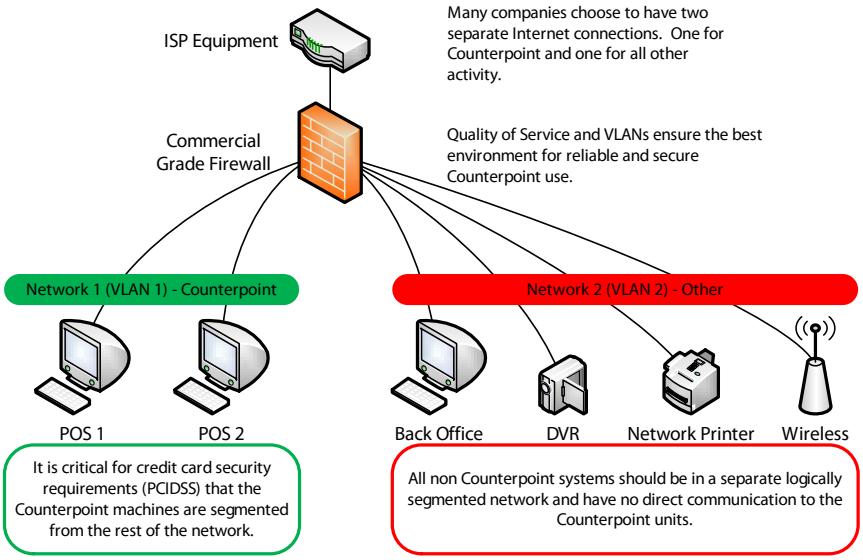
Data Center Do's and Don'ts

"Dos" and "Don'ts" of network cabling are provided below by way of reference but this should not to be considered an "exhaustive" list. This information is provided as is. Always check with your certified data cabling specialist for authoritative network cable assessment and implementation.

Do	Run all cables in a Star Configuration so that all network links are distributed from or homerun to, one central hub. Visualize a wagon wheel where all of the spokes start from on central point, known as the hub of the wheel. (see BasicCounterpoint Network Topology below).
Do	Each cable run must be kept to a maximum of 295 feet (90 meters), so that with patch cords, the entire channel is no more than 328 feet (100 meters). This is a requirement of the standard.
Do	Maintain the twists of the pairs as close as possibleto the point of termination, or no more than 0.5" (one half inch) untwisted.
Do	Make only gradual bends in the cable where necessary to maintain the minimum bend radius of 4 times the cable diameter or approximately 1" radius (about the roundness of a half-dollar).
Do	Dress the cables neatly with Velcro cable ties, using low to moderate pressure.
Do	Cross-connect cables (where necessary), using appropriately rated punch blocks and components.
Do	Use low to moderate force when pulling cable. The standard calls for a maximum of 25 lbf (pounds of force).
Do	Use cable pulling lubricant for cable runs that may otherwise require great force to install.
Do	Keep cables as far away from potential sources of EMI (electrical cables, transformers, light fixtures, etc.) as possible. Cables should maintain a 12inch separation from power cables.
Do	Install proper cable supports, spaced no more than 5 feet apart.
Do	Always label every termination point at both ends. Use a unique number for each network link. This will make moves, adds, changes, and troubleshooting as simple as possible. The TIA-606A administration standard provides guidance for properly labeling an installation.
Do	Always test every installed segment with a cable tester. "Toning" alone is not an acceptable test.
Do	Always install jacks in such a way as to prevent dust and other contaminants from settling on the contacts. The contacts (pins) of the jack should face up on flush mounted plates, or left, right, or down (never up) on surface mount boxes
Do	Always leave extra slack neatly coiled up in the ceiling or nearest concealed place. It is

	recommended that you leave at least 5 feet of slack at the work outlet end, and 10 feet of slack at the patch panel end.
Do	Always use grommets to protect cable when passing through metal studs or anything that can possibly cause damage.
Do	Choose either 568A or 568B wiring scheme before you begin your project. Wire all jacks and patch panels for the same wiring scheme (A or B).
Do	Always obey all local and national fire and building codes. Be sure to firestop all cables that penetrate a firewall. Use plenum rated cable where it is mandated.
Do Not	Splice or bridge cable at any point. There should never be multiple appearances of cable.
Do Not	Install cable that is supported by the ceiling tiles. This is unsafe, and is a violation of nearly all building codes.
Do Not	Skin off more than 1" of jacket when terminating the cabling.
Do Not	Use excessive force when pulling cable.
Do Not	Over tighten cable ties or use plastic ties.
Do Not	Use oil or any other lubricant not specifically designed for network cable pulling as they can infiltrate the cable jacket, causing damage to the insulation.
Do Not	Never install cables taught. A good installation should have the cables loose, but never sagging.
Do Not	Allow the cable to be sharply bent, twisted, or kinked at any time. This can cause permanent damage to the geometry of the cable and cause transmission failures.
Do Not	Tie cables to electrical conduits, or laycables on electrical fixtures.
Do Not	Mix 568A and 568B wiring on the same installation.
Do Not (1 exception)	Use staples on UTP cable that crimp the cable tightly. The common T-18 and T-25 cable staples are not recommended for UTP cable. However, the T-59 insulated staple gun is ideal for fastening both UTP and fiber optic cabling, as it does not put any excess pressure on the cable.

Basic Counterpoint Network Topology

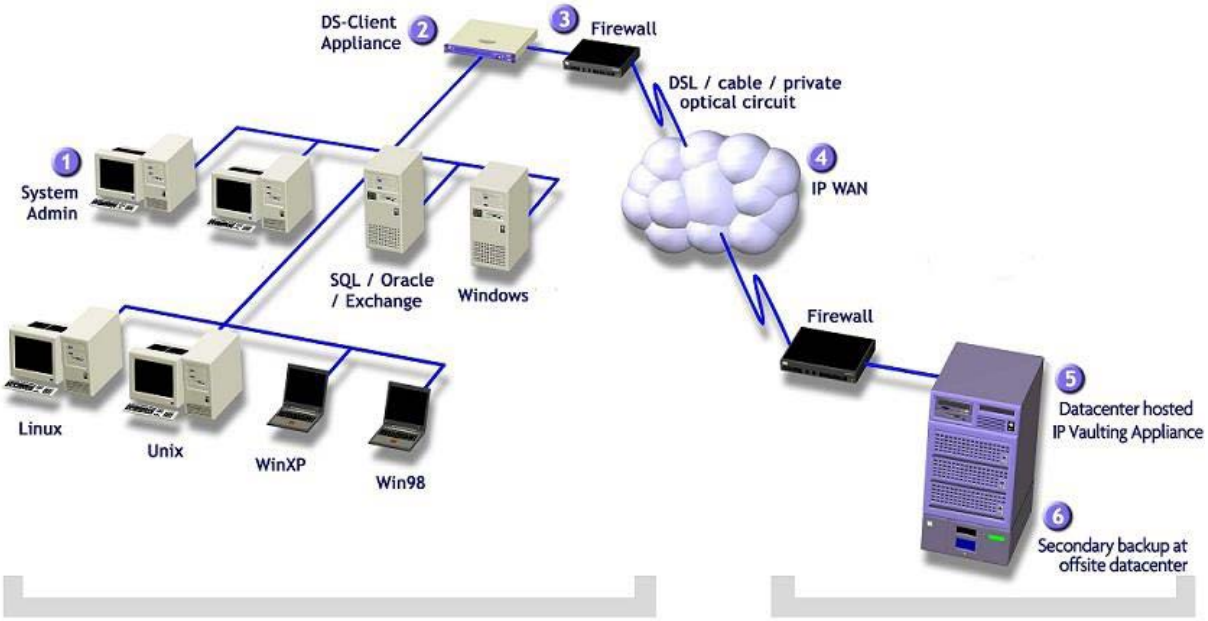


All Counterpoint units and the network equipment they attach to must be connected to a line conditioner to ensure proper power protection.

Remote Backup Services

Most companies still trust the backup of their most vital resource data to a fragmented and often ineffective policy of distributed tape devices, manual routines and offsite tape storage. RCS Remote Backup addresses the drawbacks of the common approach to backup with a unique service offering:

- A fully automated process with backups held on disk for rapid file restoration.
- Secure online transfer of fully encrypted data to an offsite datacenter, ensuring regular backups are stored safely and remotely.
- A sound basis for business continuity planning; whatever happens, your data is safe.
- A cost effective solution with an all-inclusive monthly service charge.
- Agentless
- Common File Elimination
- Service Level Agreement
- Open File Backup



How to Quote the Data Center

1. Determine # of Counterpoint users.

2. Determine the # of Locations

   Make sure your quote includes Offline Ticket Entry CounterPoint option
   Be sure to quote 1 firewall per location and business class antivirus equal to the total number of computers
   Communicate minimum requirements for Computers & Internet Speeds

What's included in Data Center Setup

Data Center Setup fee includes the setup of your data center virtual server with integration to the antivirus, backup, monitoring and IPS/IDS security platform, installation of your CounterPoint Software, and the setup of your remote users, computers and peripherals through a VPN tunnel.

Hosting Services– Data Center Tunnel Set up & Services

The Datacenter tunnel service is a dedicated hardware to hardwarebased IPSEC tunnel that securely connects your locations to their Datacenter CounterPoint server. All traffic through thetunnel is encrypted, logged and monitored by an intrusion prevention service. This system provides for outstandingperformance, security and stability. The Datacenter tunnel setup is the process we use to put the service in place. Our network engineers work with your staff to put the tunnel in place and test it.

IPSEC Tunnel Overview

Technology

Internet Protocol Security (IPSEC) is an advanced technology for securing communications between networks across the internet. IPSEC accomplishes this by verifying the identity of each network or devices and encrypting every piece of communication. IPSEC establishes trust between different networks at the beginning of the session and automatically negotiates the cryptographic keys to be used during communication. All data entering or leaving the RCS datacenter environment is secured using military grade encryption.

Advantages

There are many advantages to the managed IPSEC tunnel system:

"Set it and forget it" connection. These connections get set up once on a single network device. This keeps IT deployment time and fixes to a minimum.
Faster performance. The IPSEC tunnel makes use of a dedicated network hardware device to secure and manage the connection as opposed to software installed on individual workstations or registers.
Better security. The IPSEC tunnel gains an additional layer of intrusion prevention and monitoring and can be tailored to only connect or answer to specific networks even if an intruder knows everything about your IPSEC setup.
Greater stability. The IPSEC tunnel is always on and runs from your dedicated network hardware. It works on your behalf to keep itself running and tuned.

IPSEC Deployment

Retail Control Systems creates your IPSEC tunnel access to the datacenter and works with your team and service providers to deploy the settings needed for your networks. Our datacenter team ensures that the connection at the datacenter is maintained, logged and monitored using Intrusion Prevention Services for every packet of data moving through the system. The entire system is built on redundant, high availability, auto failover, and enterprise-grade devices. These devices are monitored and their configurations regularly backed up offsite.

FAQ's

Q: I would like to connect another computer to the data center from within the same location.

A: If it's an additional station that needs access then quote the station setup onetime fee. If it is an additional CounterPoint user then quote a user bump, another monthly user fee and, if needed, an additional station setup.

Q: When and why do I quote IPSEC tunnel services?

A: Tunnel services should be quoted per location. This is to ensure that you have a secure, dedicated connection to the Data Center. See IPSEC Tunnel Overview for more details

Q: I have 25 CounterPoint users but, I would like to host 10 users.

A: This is not a preferred but is possible. This situation will be discussed on a case by case basis.

Q: Do I have to be at a specific version of CounterPoint?

A: You must be current on CSS, and at the latest version of CounterPoint whenever possible.

Q: Can I back up my data locally?

A: Yes. The method depends on a number of factors.

Q: What happens if I lose my internet connection?

A: All installations that are hosted are required to have Offline Ticket Entry installed. We highly recommend an analog modem as a backup for credit card Processing.

Q: How is fire suppression handled at the Data Center?

A: Fire suppression at the Datacenter is provided by a double, pre-action, dry system linked to smoke and heat detectors.

Q: How many servers will be required if I have a large quantity of users?

A: Customers with large amounts of users/data may require two or more servers. This is all covered with your initial set up costs and monthly fees.

Q: Can you host accounting software, such as, QuickBooks?

A: We do host various accounting packages using the Customer's existing licensing only. For security purposes these packages should be maintained on a server separate from the CounterPoint server Fees for hosting these packages are determined on a case by case basis.

Q: Can I have a local IT company create a Private Network with one large tunnel to eliminate the need for tunnels at each location?

A: If you already have an internet connection at each location the tunnels will cost less and provide better survivability than moving all data through a single location before reaching the datacenter.