Oracle® Corente Cloud Services Exchange

Security Guide for Release 9.4.3

E76017-04
May 2017

Oracle Legal Notices

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Preface

The Corente Cloud Services Exchange Security Guide provides information about how to configure and deploy Corente Cloud Services Exchange securely.

This document is intended for users with network administration experience. It is assumed that readers are familiar with data networking and data network security.

Related Documentation

The documentation for this product is available at:

http://www.oracle.com/technetwork/server-storage/corente/documentation/index.html

Feedback

Provide feedback about this documentation at:

http://www.oracle.com/goto/docfeedback

Conventions

Hyperlinks can be used to navigate through the guide or the procedures related to an overall activity, or to jump to a cross-referenced topic or Internet URL.

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Document Revision

Document generated on: 2017-05-01 (revision: 1222)

Chapter 1 Introducing Corente Cloud Services Exchange

Table of Contents

This chapter includes some background information on virtual private networks and then describes the technology and protocols that Corente Cloud Services Exchange is based on.

1.1 About Virtual Private Networks

Virtual private networks (VPNs) were intended to usher in a new generation of enterprise data networking by moving companies from dedicated private connection infrastructure to shared public connection infrastructure. The benefits of using public rather than private infrastructure for connecting disparate local area networks (LANs) include greater flexibility and faster time to market through the use of any connection; improved security through the use of open, standards-based encryption and authentication technologies; and lower costs by capturing the economies of scale of public versus private infrastructure.

VPN technologies provide advanced networking and security capabilities, including:

- **Tunneling:** Encapsulation technology that wraps unroutable packets (using private address space) inside routable packets (using public address space) for delivery across public networks

- **Encryption:** Encoding packets using secret keys to prevent reading or tampering as they traverse the public network

- **Authentication:** Guaranteeing the identities and authorization of remote systems

VPN technologies are mature and well proven. Unfortunately, it has been difficult for companies to realize the benefits of VPNs over private connection infrastructures because VPN technologies have been difficult to successfully deploy and manage. These difficulties have caused companies to implement VPNs that compromise security because they are one or more of the following:

- **Incomplete -** Strong encryption is implemented without strong authentication, as public key infrastructure technology is even more complex than VPN.

- **Overly complex -** A mixture of strong and weak encryption is used to accommodate export restrictions and the limitations of legacy hardware.

- **Impossible to manage -** Static solutions are implemented because of the inability to manage dynamic changes.

- **Only partially deployed -** Implementations are created that can only be deployed in locations with static public addressing and non-conflicting LAN IP address ranges.

- **Labor intensive -** They rely heavily on manual procedures to ensure integrity and compliance with changing policies.

The best security technology in the world will not protect business critical information and applications if it cannot be deployed and managed in a reasonable manner. Corente Cloud Services Exchange uses a host of patented capabilities that build on best-in-class, standards-based security technologies to deliver a secure and manageable solution.

1.2 About Corente Services Gateways

The Corente Services Gateway is installed on generic Intel x86 platforms or in virtual environments. The software runs on a hardened version of the Oracle Linux operating system (OS), which turns the computing platform into a secure applications traffic device with performance that can meet or exceed the throughput of most hardware systems.

The Corente Services Gateway includes IPSec VPN gateway, firewall, DHCP server/client, Internet connection sharing (ICS), QoS, backhaul, DNS, and routing support in addition to the hardened OS and drivers.

When a Corente Services Gateway receives traffic destined for a remote segment of the secure network, the packets are encrypted and encapsulated, and then sent to the appropriate gateway for that segment. A Corente Services Gateway may be configured to route all traffic for a LAN (secure and insecure), or may be configured to work with existing routers and firewalls, managing only the secure segment of the traffic.

1.3 Supported Protocols

At the heart of networking are the security protocols. Different protocols are used to authenticate the identity of the participants, to structure and transmit the data over the network, and to encrypt and decrypt the data. Corente Cloud Services Exchange are built on several key protocols that are widely accepted as standards for secure networking.

The most significant of these is the Internet Protocol Security (IPSec) standard. IPSec provides a protocol framework for the secure, authenticated transmission of data between systems. It has been widely examined in the cryptographic community and is believed to be cryptographically sound. IPSec provides the framework for most VPN architectures deployed today.

Corente Cloud Services Exchange employs IPSec as the core protocol for data transport. While the protocol permits a wide range of configuration options, Corente Cloud Services Exchange constrains the configuration of the protocol to the choices that offer the highest known security. This greatly simplifies configuration of the secure network and ensures that insecure configurations cannot be created. The following IPSec options are used by Corente Cloud Services Exchange:

- ESP (Encapsulating Security Payload)
- Tunnel Mode
- 192-bit AES encryption
- 1024-bit Public/Private Keys
- SHA-2
- Deflate

Where protocol standards do not exist or are incomplete, Corente Cloud Services Exchange employs proprietary protocols. These include a control and monitoring protocol that allows secure networking devices to be centrally managed, protocols for tunneled transport of packets via TCP and UDP protocols, and protocols for the management and distribution of keying and authentication information.

Chapter 2 The Service Control Point

Table of Contents

The Corente Services Control Point (SCP) provides configuration and policy updates for Corente Services Gateways and Corente Cloud Services Exchange IPSec Clients, as well as collecting performance and usage data for reporting, monitoring, and proactive real-time alerting.

Because customer traffic never passes through the Corente SCP but flows directly from site to site, the Corente Cloud Services Exchange solution scales extremely well. Only a small amount of monitoring and control data is sent to the Corente SCP.

All administration is performed using the App Net Manager application, which is hosted by the Corente SCP. App Net Manager allows administrators to manage their networks and to define users.

2.1 Password Settings

Password settings can be made that apply to all entities that use a password to log into the domain, such as administrators of App Net Manager, administrators of Gateway Viewer, and the Corente Client.

Administrators can change password settings at any time in App Net Manager by right-clicking the domain name, opening the Domain Preferences window, and accessing the Passwords tab. This tab includes the following fields:

- **Password Minimum Length:** Enter the minimum length of passwords that can be set for login accounts. The default value is 8, but this value can be up to 20 characters.

- **Expire Passwords After:** Select this option if you would like to enable password expiration. If this option is selected, you must enter the length of time that passwords will remain valid until they expire. The default is 30 days, but this value can be from 1 to 365 days.

  When a password expires, the user will be instructed to choose a new password, with the minimum length you specified and containing at least one lower-case letter, one upper-case letter, and one numeric character.

2.2 Root Administrator for App Net Manager

A root username is used to access App Net Manager to create and manage a domain. You may add additional administrator accounts once your domain has been activated.

Specify the following for the root administrator:

- **Root Administrator:** Choose a root administrator username that can be used to log into the App Net Manager. For example, johnsmith or amy123.

- **Password:** Choose a password for the Root Administrator. Section 2.1, “Password Settings” describes how to set the password policy for App Net Manager.

- **Confirm Password:** Re-enter the password to avoid any mistakes.
- **Password Challenge:** This challenge question will be used to verify your identity if you should forget your root administrator password and require assistance in obtaining it.
- **Challenge Response:** This is the answer to the Password Challenge. Your password will only be provided to you if you can provide the correct Challenge Response.

2.3 Administration Logs

The Administration Logs allow you to view monthly summaries of the activity of administrators in your domain. Each monthly log displays the following:

- **Date/Time:** The date and time when the action occurred.
- **Administrator:** The user account who performed the Action.
- **Action:** The action that was taken by the Administrator.
- **Category:** The category of Object that was changed.
- **Object:** The specific item in the domain that was changed. There may be two objects if the change occurred between them.
- **Source:** Where the action originated from, if applicable.
- **User Host Name (IP):** The location from where App Net Manager was accessed.

2.4 Mutual Consent Trust Model

Key information is exchanged between Corente Services Gateways only if the administrators of both gateways mutually consent to the connection. This is a unique feature of the Corente Cloud Services Exchange solution that is extremely valuable in establishing inter-corporate extranet connections or bridging organizations and business units within a single company.

Administrators completely control their own security domains, including tunnel connections and user groups. Connections between domains are established through this mutual consent model. When the administrator of one of the gateways decides to end the mutual consent (the decision can be made unilaterally), key revocation is immediate. All on-line gateways are notified instantaneously and tunnels are terminated. Off-line gateways are notified of the revocation the next time they contact the Corente SCP.

2.5 Authentication in Corente Cloud Services Exchange

A significant feature of the Corente Cloud Services Exchange approach to authentication is the automated distribution of authentication materials.

Primary identification between the Corente SCP and a customer is accomplished by a Corente Cloud Services Exchange Gateway-specific, 1024-bit randomly generated shared secret. The secret is securely distributed to the customer using strong cryptographic protocols (SSL authenticated with Corente Cloud Services Exchange's VeriSign certificate).

Secondary authentication is performed using a 1024-bit key. The public/private key pair is generated locally by the gateway at system initialization, and the public key portion is securely transmitted to Corente Cloud Services Exchange where it is bound into a certificate and stored at the Corente SCP. Corente Cloud Services Exchange never generates, receives, or escrows private key information from any customers.

Customers have control of their keys and can regenerate them at any time using App Net Manager.

2.6 Certificate Revocation

Revocation is immediate in the Corente Cloud Services Exchange architecture while a site is in contact with the Corente SCP. Customers have complete control over their Corente Cloud Services Exchange Gateway keys, which can be regenerated on-demand at any time. Revised certificates are automatically distributed to authorized recipients through the secure channels.

Unlike the generic certificate or shared secret approaches, where revocation only takes effect the next time authentication is performed (and perhaps not even then if certificate revocation lists are not assiduously checked), revocation under Corente Cloud Services Exchange usually takes place within a few seconds for all connections affected by the revocation.

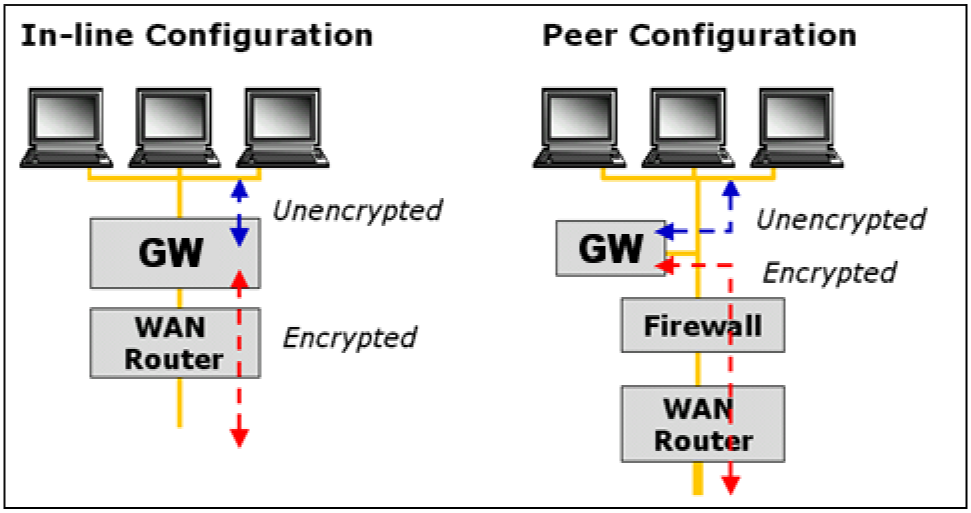
Chapter 3 Gateway Network Configurations

Table of Contents

There are two basic network configurations for a Corente Cloud Services Exchange Gateway: on a single-Ethernet connection to a LAN (*peer configuration*), and on a dual-Ethernet connection between a LAN and a WAN (*in-line configuration*). See Figure 3.1, “Gateway Network Configurations”.

The two basic configurations support a range of customer LAN environments and security methods, some of which are described in this chapter.

Figure 3.1 Gateway Network Configurations



A Corente Services Gateway in the peer configuration is a secure device with a single Ethernet card that sits on the same network as the machines that will be participating in the VPN.

A Corente Services Gateway in the in-line configuration is a secure device with two Ethernet cards: one Ethernet card is connected to the internal trusted network, while the other card is connected to the external untrusted network.

Both configurations can provide services such as a VPN Gateway, router, backhaul client/server, DHCP client/server, stateful inspection firewall, DNS, and Internet connection sharing (ICS) device.

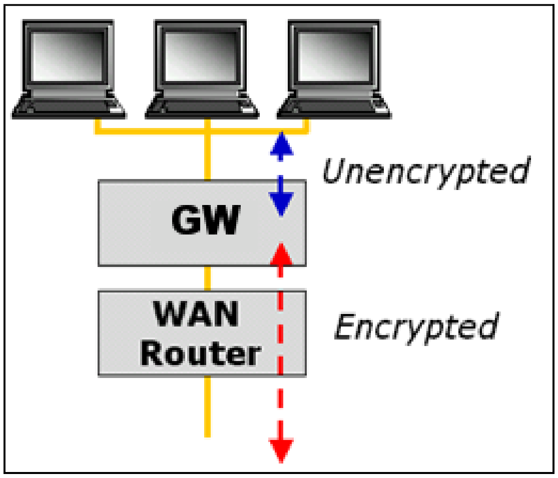
When deploying a VPN, each location must select the best position in the network to meet security needs. A Corente Services Gateway can be deployed at demarcation point between WAN and LAN, or behind the network firewall on the trusted LAN. The following sections describe the benefits and risks of each of these designs.

3.1 Corente Services Gateway as a Firewall, Router, and VPN Gateway

For many enterprises, their large data centers and corporate sites have ample security and networking infrastructure. However, smaller regional offices and home offices have very little preexisting security in place. In this design, the gateway provides an all-in-one, remotely managed solution ideal for branch and small office/home office (SOHO) environments that need a combination of VPN, firewall, router, and DHCP services.

See Figure 3.2, “Network Deployment Using a Corente Services Gateway as a Firewall, Router, and VPN Gateway” for an example of this deployment.

Figure 3.2 Network Deployment Using a Corente Services Gateway as a Firewall, Router, and VPN Gateway



The untrusted interface on the gateway is connected to the local Internet access device (such as a WAN router, DSL, or cable modem) and the trusted interface connected is to the LAN. The gateway can be assigned a static, globally routable IP address for its untrusted interface or can receive its address dynamically as a DHCP client.

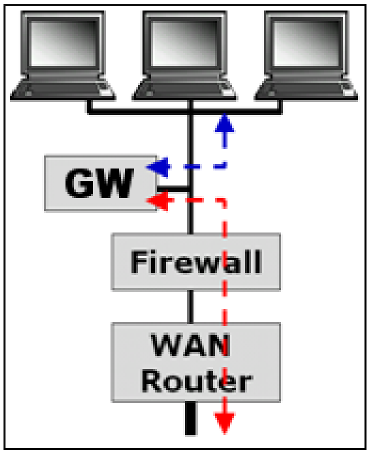
Customers can employ the gateway firewall to permit simultaneous access to the Internet and to the VPN. Alternatively, customers can restrict all traffic to the VPN and backhaul external traffic so that Internet access is only available through centralized corporate firewalls.

3.2 Corente Services Gateway Behind an Existing Firewall

Installing a Corente Services Gateway behind an existing firewall on a private address is the most secure method for deploying a gateway in conjunction with existing network infrastructure. In this configuration, the gateway can be located closest to the client systems it is protecting.

See Figure 3.3, “Network Deployment Using a Corente Services Gateway Behind a Firewall” for an example of this deployment.

Figure 3.3 Network Deployment Using a Corente Services Gateway Behind a Firewall



Many customers use this configuration to securely connect individual LAN segments across wide areas. For example, connecting the finance department LAN in Chicago to the finance department LAN in Los Angeles. With this deployment, traffic is encrypted near the source, instead of at the network demarcation point, so it is protected on the LAN as well as other intervening networks.

Furthermore, by putting the gateway behind an existing firewall and using private addresses, the VPN gains the general benefits of NAT. The outside world has no visibility into the security of the VPN, since even the address of the VPN gateway is hidden from the public network.

3.3 Firewalls and Corente Cloud Services Exchange

Although Corente Cloud Services Exchange supports all standard VPN configurations, it offers unique capabilities that support installation behind NAT devices including firewalls, web proxies, and routers, with minimal preparation of the NAT device.

See Chapter 4, *Firewall Provisioning for Corente Cloud Services Exchange* for details of firewall configuration for Corente Cloud Services Exchange.

3.4 Third-Party VPN Devices

Corente Cloud Services Exchange supports secure connections between Corente Services Gateways and third-party VPN devices, such as Cisco Adaptive Security Appliance (ASA) or Juniper devices.

Corente Services Gateways use the following ports and protocols to establish tunnels with third-party VPN devices:

- **UDP 500** for `ISAKMP`
- **UDP 4500** for `NATT`
- **IP Protocol 50** for `IPSec`

To authenticate with third-party VPN devices, you configure Internet Key Exchange (IKE) settings in App Net Manager. Internet Key Exchange (IKE) is an Internet Protocol Security (IPsec) standard that secures VPN negotiation and access between networks.

When you set up third-party VPN devices, you must specify a pre-shared key (PSK), or shared secret, in the IKE settings. To ensure network security, you should follow these PSK best practices:

- Use a PSK generator to create random secrets with large character sets.
- Generate a unique PSK for every VPN tunnel.
- Ensure the PSK is at least 30 characters long to prevent brute force attacks.
- Do not transmit PSKs over the Internet. You should use fax, SMS, or phone to transmit PSKs to other users.
- Do not store PSKs. After you specify the PSK on a third-party VPN device, you should discard it. If you need to configure the PSK again, you should generate a new one.
- Change PSKs periodically. You should change PSKs at a frequency that matches your corporate password policy.

Chapter 4 Firewall Provisioning for Corente Cloud Services Exchange

Table of Contents

This chapter describes how to configure firewalls for use with Corente Cloud Services Exchange.

4.1 The Corente Service Port

TCP port 551 is the Corente service port and is used to terminate authenticated connections between trusted Corente Cloud Services Exchange elements: Corente Services Gateways, Corente Cloud Services Exchange IPSec Clients, and the Corente Services Control Point (SCP).

When placed behind an existing firewall, customers must define firewall rules that redirect port 551 traffic to the gateway. Corente Cloud Services Exchange offers two options to accomplish this. One option is designed to deal with the dynamic nature of IP addressing in today's Internet world. The second option is the more traditional approach where every endpoint has a static, non-changing IP address.

4.2 Firewalls and Dynamic IP Addressing

The introduction of broadband as an Internet connection option also introduced the need to support dynamic endpoint IP addresses. Many broadband vendors use DHCP to supply IP addresses to Internet access devices (IADs). These IP addresses are leased for a specific period and can change without notice when the lease expires. DSL and cable modems are usually provisioned with IP addresses assigned via DHCP.

Corente Cloud Services Exchange has built support for these environments into its core service. This support for dynamic IP enhances the VPN, allowing the IP address of a destination to change without compromising the VPN connections. This support also impacts the specification of firewall rules at central sites and data centers. Since the IP addresses of remote VPN locations change, the firewalls that permit access to (or from) these locations cannot specify individual static IP addresses in the rule set. Instead, rules must be specified using ANY IP ADDRESS settings for the VPN to function properly.

The support of dynamic IP addresses is also necessary for dynamic failover with the Corente SCP. Corente Cloud Services Exchange supports geographically dispersed data centers that use different IP addresses for redundancy and scalability. Each new VPN element must download software from the Corente SCP when first being installed. When establishing connections, each VPN element first attempts to contact the Corente SCP for security updates and location information. This connection is maintained for monitoring, alerting, and distribution of updates.

To ensure that gateways can contact or be automatically rehomed to a different Corente SCP without having to modify firewall rules with new IP addresses, Corente Cloud Services Exchange recommends the use of ANY IP ADDRESS in the firewall rules for the Corente SCP connections.

See Section 4.3, "Recommended Firewall Settings" for recommended firewall settings when your locations on the VPN use dynamic IP addresses.

See Section 4.4, “Recommended Router Configuration” for recommendations on how to configure the routers on the network at your locations.

4.3 Recommended Firewall Settings

If you have a firewall at a Location that will operate in front of your Corente Services Gateway, then you must configure specific mandatory settings for your firewall.

See the *Corente Services Gateway Deployment Guide* for information about mandatory firewall settings.

4.4 Recommended Router Configuration

If you have one or more routers on the network at your Location, configure your routers as follows:

- Add or modify routers to forward UDP broadcast packets to the Corente Services Gateway if you have multiple subnets in your network participating in the Corente Services network; OR turn on RIPv2, or OSPF on your routers if you plan to use RIPv2, or OSPF for automatic Corente Services network routing
- Add or modify static routes to ensure that Corente Services network traffic is routed properly if you do not intend to configure the Corente Services Gateway as the default gateway on the network
- For Peer Corente Services Gateways, route traffic from the machines on the LAN to the Corente Services Gateway
- If you plan to configure your Corente Services Gateway as a backhaul client, configure routers to send all outgoing Internet packets to the gateway

4.5 Establishing Connections Between Gateways When Both Sides Are Firewalled

A unique feature of Corente Cloud Services Exchange is the ability to establish connections between gateways when each is assigned a private address behind a firewall. This set up occurs frequently in business-to-business connections where business partners are establishing connections through each of their existing security infrastructures.

For each pair of gateways, at least one must be reachable inbound on TCP port 551, as well as on UDP port 551. Note that in a *hub and spoke* topology (a typical extranet design), only the hub location requires an inbound firewall port to be opened. In each remote spoke site, a gateway behind an unmodified firewall can initiate outbound TCP connections to the hub gateway that is behind the modified firewall.

A remote Corente Cloud Services Exchange IPSec Client can only initiate (not terminate) tunnels. Therefore, any associated gateways that are behind firewalls must have inbound port 551 requests assigned to them.

Chapter 5 Other Security Features of Corente Cloud Services Exchange

Table of Contents

Corente Cloud Services Exchange employs a number of other measures to ensure the security of corporate networks and resources, including fine-grained access control, proper insurance, and no access to customer gateways.

5.1 Fine-Grained Access Control

User Groups provide a powerful security tool when setting up inter-entity networks. A Corente Cloud Services Exchange User Group limits the visibility of remote users and locations to a specific set of local IP addresses. Although a local network may include one hundred systems, an administrator can configure the local Corente Services Gateway so that remote users and gateways can only access five of those one hundred. The rest of these computers are completely blocked from outside view.

In many ways, User Groups create a virtual demilitarised zone (DMZ). Although one hundred systems are physically connected to the LAN, remote locations can be limited to access only the extranet server, the email server, and the public FTP server.

Routers are capable of performing similar access limitations, but not to the same extent as User Groups. Routers can confine problems such as excessive broadcasts, duplicate IP addresses, unauthorized DHCP servers, and misbehaving Windows servers, as well as remote users snooping around the network. When problems occur, few users are affected and the problems are easy to troubleshoot. However, routing alone does not solve security. User Groups are also required.

A User Group in Corente Cloud Services Exchange is a group of statements. Each statement defines a range of IP addresses that are either included or excluded from the User Group. As a traffic packet comes through a tunnel to a gateway, the gateway’s User Group is scanned for a pattern that matches the incoming packet. An include/exclude rule associated with the pattern determines whether the packet is accepted or rejected by the gateway.

Corente Cloud Services Exchange improves User Groups by taking them a step further with *fine-grained access control*, allowing access rules to be defined on a per-source address, per-destination address, and per-protocol basis. Administrators can define multiple User Groups on each gateway, which can each be matched with User Groups in the partner location. The administrator can then choose the type of traffic that is allowed to be transported between these sets of IP addresses, effectively banning the use of certain services or applications over the VPN by all or specific computers. This also allows the creation of asymmetrical tunnels, in which local computers can be used to access remote computers on the VPN, but be inaccessible themselves (or the opposite).

Fine-grained access control allows a single gateway to be in place on each corporate network, serving a wide array of computers with different VPN and Internet access requirements.