White Paper

Cisco Cloud Services Router 1000v and Microsoft Azure: Access Microsoft VNet Securely

What You Will Learn

The Cisco® Cloud Services Router 1000v (CSR 1000v) sets the standard for enterprise network services and security in the Microsoft Azure cloud. The Cisco CSR 1000v is based on Cisco IOS® XE Software, which powers cutting-edge routers including the Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000 Series) and Cisco 4000 Series Integrated Services Routers (ISRs), and represents decades of Cisco IOS Software development accelerated by innovation and customer demand. The CSR 1000v brings these features and use cases into the realm of virtual and cloud computing, and introduces new features specific to cloud networking.

Solutions for integrating Microsoft Azure with your existing network are scarce and complex, and they pose a challenge for IT departments seeking a transparent expansion into Microsoft Azure. The CSR 1000v provides the familiar user interface of Cisco IOS XE Software, and enables you to take advantage of your existing network management tools and processes. In addition to the Cisco IOS XE Software command line, the CSR 1000v includes a Representational State Transfer (REST) application programming interface (API), allowing orchestration tools to not only provision the CSR 1000v, but also configure and monitor it.

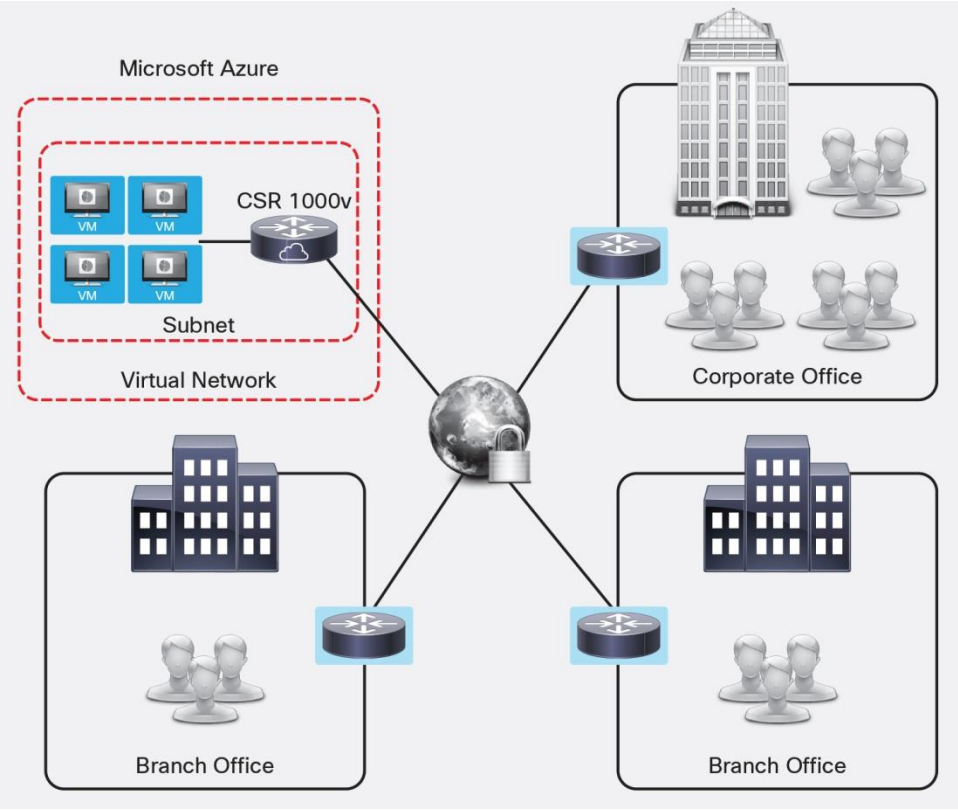
Unlike similar products that offer just gateway or security features, the CSR 1000v is a complete multiservice cloud networking platform offering scalable enterprise-class routing features, VPN, stateful firewall, and application inspection. At the core of the CSR 1000v is a modular architecture that allows you to add more services to meet changing business and user demand.

Cisco CSR 1000v Use Cases in Microsoft Azure

Easily Extend Enterprise Networks

A typical approach to Microsoft Azure VPN access is to provision a single VPN "backhaul" between an existing data center and a Microsoft Azure Virtual Network (VNet). By deploying the Cisco CSR 1000v in Microsoft Azure, every branch-office, campus, and data center location can directly access the Microsoft Azure VNet securely, without backhauling through an existing data center (Figure 1). This process reduces latency, eliminates expensive private WAN links, and enables route-based VPN topologies. You can choose from a wide variety of VPN technologies supported on the CSR 1000v, including point-to-point IP Security (IPsec), FlexVPN, Dynamic Multipoint VPN (DMVPN), and Easy VPN. Familiar Cisco IOS XE VPN configuration allows IT staff to quickly integrate a Microsoft Azure VNet into existing enterprise VPN topologies. In addition, the CSR supports up to 1000 concurrent VPN tunnels per CSR instance running on Azure.

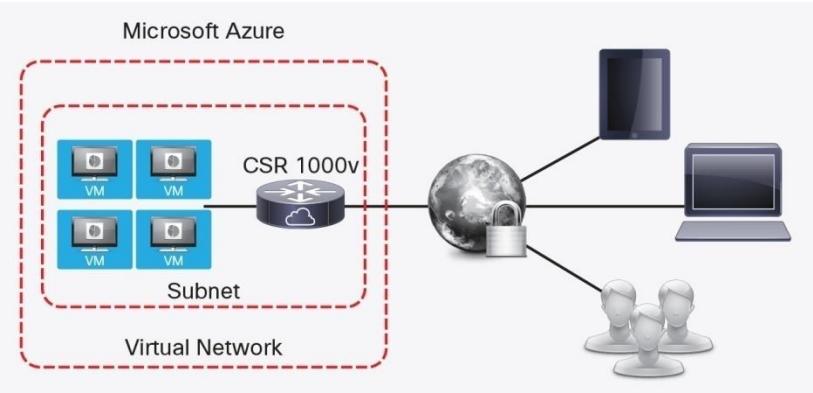
Figure 1. Secure Access to Microsoft VNet with Cisco CSR 1000v



Securely Connect Remote Users to the Cloud

The CSR 1000v on Microsoft Azure supports Secure Sockets Layer (SSL) VPN access using Cisco AnyConnect® Client for teleworkers and remote users. It supports flexible authentication, authorization, and accounting (AAA; for example, RADIUS and TACACS+) server options for remote user authentication. You also can replicate or scale your applications in Azure regions geographically near your end users, providing a smooth transition for existing AnyConnect deployments. No new client software is required, and you can reuse existing configurations (Figure 2).

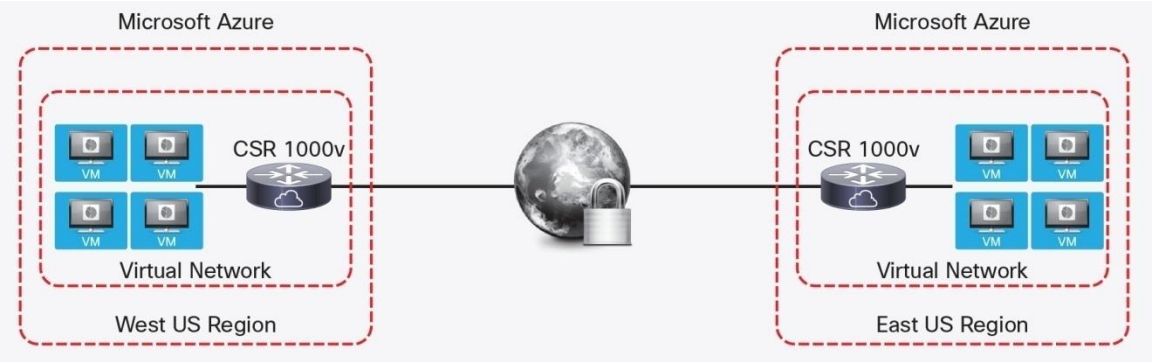
Figure 2. Remote Access VPN to Azure Using the Cisco CSR 1000v



Worldwide Hybrid Cloud Network

The CSR 1000v allows the interconnection of Azure VNets with enterprise locations (Figure 3). Multiple Azure regions can be interconnected transparently alongside physical locations. This implementation provides direct accessibility between any enterprise location and any Azure region, and supports up to 1000 concurrent VPN connections and avoids per-VPN-tunnel costs that Microsoft Azure charges. It extends existing enterprise routing architecture into Azure regions on the familiar Cisco IOS® XE platform and provides options for Network Address Translation (NAT) configuration for overlapping IP space on Azure VNets (Figure 3). You can also use the CSR 1000v to connect Azure to other public cloud services, including Amazon Web Services.

Figure 3. Interconnect Azure VNets Alongside Enterprise Locations



Monitor and Analyze Azure Cloud Security and Performance

The Cisco CSR 1000v features a zone-based firewall for securing your Azure cloud network. A stateful firewall between Azure VNets and enterprise locations, the CSR 1000v allows the extension of existing enterprise security policies using the Cisco IOS Zone-Based Firewall. This extension makes configuration easy because a common firewall configuration can be shared between physical routers running Cisco IOS XE Software and CSRs. With the security technology of the CSR routers, you can use NetFlow to export flow records for forensic analysis.

Application Visibility and Control (AVC) is a Cisco IOS XE Software feature that allows the CSR 1000v to identify and classify thousands of different applications, reporting key performance metrics for each. You can use quality-of-service (QoS) policies, when classified, to prioritize or block specific applications. You also can use AVC data collected from Microsoft Azure and external locations to pinpoint application performance degradation.

Further enhancing this capability, the IP service-level agreement (IP SLA) feature enables the CSR 1000v to measure network performance between Cisco devices. A CSR 1000v in Microsoft Azure may act as an IP SLA responder or source, implementing probes with time stamps to accurately measure delays, jitter, and other metrics that reflect network performance. IP SLA helps proactively identify cloud performance problems, helping ensure application availability and lower operational costs, and reducing downtime.

How to Deploy the Cisco CSR 1000v on Microsoft Azure

A deployment guide for the Cisco CSR 1000v on Microsoft Azure is available on the Cisco community website at: https://supportforums.cisco.com/document/12744996/cisco-csr-1000v-deployment-guide-microsoft-azure.

For More Information

For more information about the Cisco CSR 1000v “Bring Your Own License” option, please visit:

- For more information about the Cisco CSR 1000v and Microsoft Azure, please visit the Cisco CSR 1000v “Bring Your Own License” product page on Microsoft Azure: https://azure.microsoft.com/en-us/marketplace/partners/cisco/cisco-csr-basic-templatecsr-azure-byol-two-nic/.
- For more information about the Cisco CSR 1000v, visit: http://cisco.com/go/cloudrouter.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-736574-00 02/16