

Prepare Your company for
Unexpected
Threats Before
They *Impact*
Your *Business*

Pandemic Capacity Planning

For IT Infrastructure and Remote Access Managers

Table of Contents

- 1** Introduction
- 1** The Scope of the Threat
- 2** Pandemic Planning Solutions
- 5** Customer Case Study
- 5** About Virtela

Introduction

There is little doubt among authorities that a pandemic of some kind will strike the global population in the future. The question is not if, but rather when, and to what degree? Governments, utility companies, corporations and individuals are all preparing for the potentially devastating impact of a pandemic on global trade, production, safety and individual welfare. Because the potential scenarios are largely dependent on the nature and efficiency of a mutation that has not yet occurred, the various degrees of impact of a pandemic outbreak, as with the avian flu, are difficult to plan for with flexible and cost-effective means. A considerable amount of planning, policy engineering, training, and testing must go into an effective pandemic mitigation plan. One component of proper planning, which we will address here, is that of ensuring adequate network capacity for all employees, contractors and partners to enable them to work from home for an extended period of time (30 days up to two years). Ensuring that production, sales, operations, and supply chain all continue functioning during even the mildest of pandemic scenarios is the key objective of most companies today. Adequately planning now will ensure business continuity for those companies who execute proactively. Companies that fail to plan for this type of disaster will most likely not be able to withstand the strain on their infrastructure.

The Scope of the Threat

Business Requirements

From a capacity planning perspective, enterprises typically want to create a remote access infrastructure that supports the following requirements:

- Immediate increase in remote user connections and traffic. This generally follows an official announcement of a possible outbreak or official instruction to work from home. **Zero to seven days.**
- Sustained increases in remote user connections while the public determines the extent of a potential threat and its estimated duration. **Zero to thirty days.**
- Long-Term increase in remote user connections once a threat is identified and expected work disruption is quantified. **Thirty days to two years.**
- Limitation of access to various levels of critical user groups if immediate or short-term capacity is insufficient.
- Regional capacity increases in the event the pandemic is localized to a specific country or region where operations could be adversely impacted.
- Regular testing of the system, support and processes prior to use.
- Automatic access to alternative gateways in the event of capacity or infrastructure issues in the affected region.
- Accommodation for non-company issued devices, in the event employees working from home do not have company-issued laptops.

- Provider/Carrier/ISP redundancy and geographic redundancy in the event of carrier-wide outages or regional power outages, networking outages or congestion affecting multiple carriers.

A Pragmatic Approach

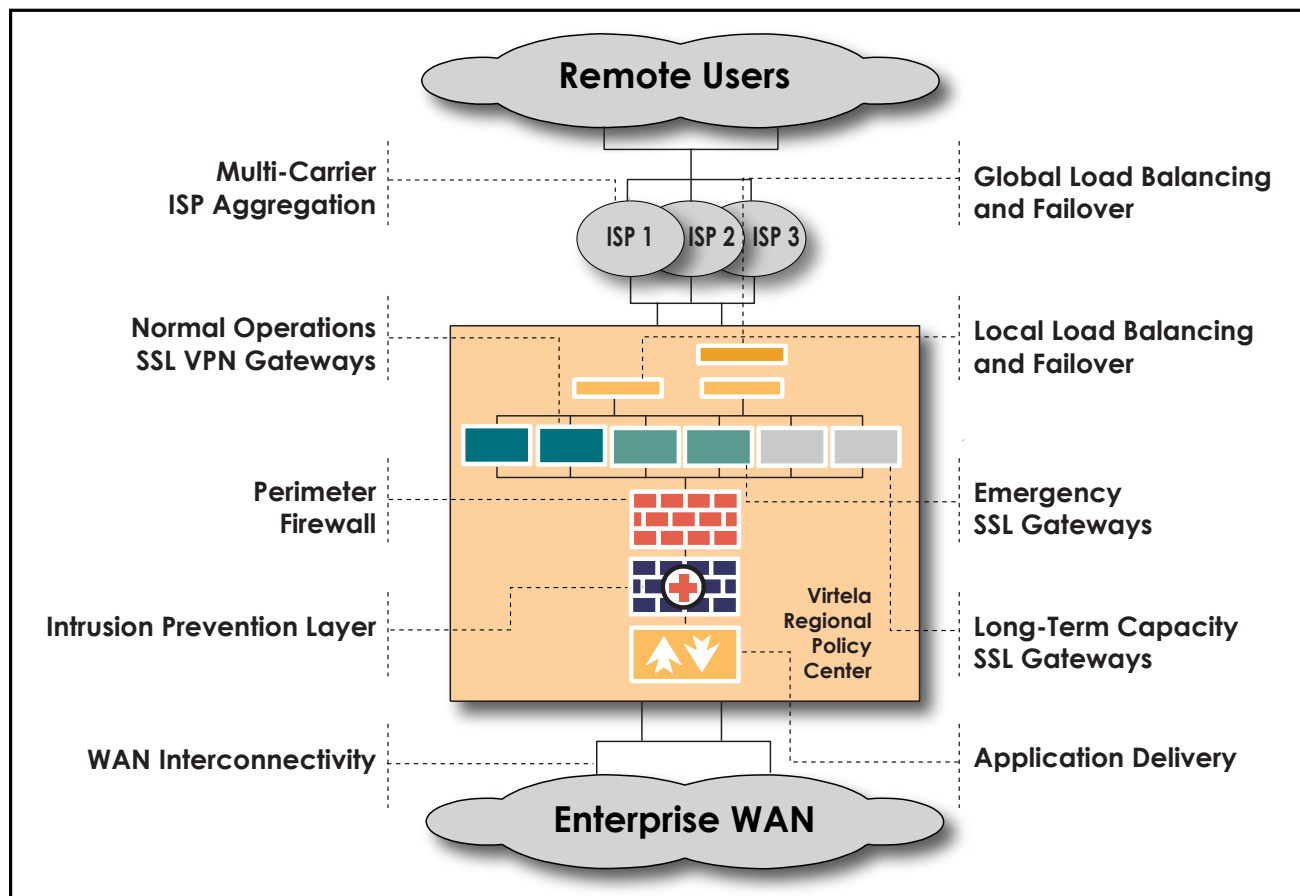
While it is relatively straight-forward to build and staff sufficient capacity and redundancy for all users to work remotely tomorrow, the cost of such an initiative can be exorbitant, and in some cases wasteful, depending on how or if the pandemic spreads. Fortunately, there is a solution and a variety of enabling technologies can be employed to create a remote access infrastructure that can quickly scale without the need to purchase idle long-term capacity. Many enterprises today are leveraging solutions from a variety of vendors and are seeking to create latent capacity that can be quickly dialed up (or down) as needed. Others are seeking ways to consolidate and leverage existing remote access capability across multiple regions and gateways to maximize the aggregate global capacity of their enterprise. Additionally, maintaining critical user groups enables enterprises to quickly limit access to only those users who are most critical to sustain operations during unexpected spikes in user connections. In this brief we will explore an integrated approach to remote access planning that incorporates all of these methods into a single, flexible and cost-effective infrastructure.

Pandemic Planning Solutions

As a managed service provider and technology integrator, Vireta provides the infrastructure, tools and personnel necessary to help enterprises develop pandemic planning solutions and avoid capital investments, headcount investments and facilities upgrades. Vireta accomplishes this by aggregating and integrating the best access and backbone infrastructures around the world into its Global Service Fabric via an intelligent architecture overlay of network nodes called Regional Policy Centers (RPCs). Following is a list of enablers that Vireta employs in remote network access settings specifically, for pandemic planning designs:

- Core Security
- SSL VPN
- Global Load Balancing
- Out of Region Access
- User Group Management
- Emergency Licensing Procurement (for a pandemic duration of 0-30 days)
- Long-term Licensing Procurement (for a pandemic duration of 7 days to 24 months)
- Baseline Licensing
- Multiple Global Access Points
- End User Support and Testing
- Training and Process Development

Sample Pandemic Capacity Planning Design



Core Security

Virtela manages high availability enterprise firewalls and Intrusion Prevention devices in its regional policy centers for advanced filtering, security and threat management. Firewalls and IPS devices form the core security layer between the Internet and the enterprise WAN.

SSL VPN

SSL VPN devices are utilized to terminate end user connections from employees, home PCs, partners and suppliers. No preinstalled software is needed by the remote person, so new devices can connect quickly during a pandemic or disaster situation. Depending on the security profile of the end user, traffic is passed through various security checks, firewall policies, and ultimately scrubbed by the IPS devices before entering the WAN/LAN.

Global Load Balancing

Local Traffic Manager Load Balancers are another remote access enabler capable of gracefully managing sessions across all SSL VPN devices at the gateway. These devices can also manage higher level sessions between gateways all around the world. The Global Traffic Managers choose the optimal gateway for the end user at all times and mitigate issues like gateway capacity, device outages, gateway outages, and global session distribution.

Out-of-Region Access

WAN Acceleration Devices, provide bandwidth management, local file caching, and general TCP and application acceleration from Virtela's RPCs across the WAN to Customer datacenters. These application acceleration devices enable a user in the US, for example, to enter the network from Asiapac (in severe circumstances) and still be able to adequately run applications.

Through the use of these remote access enabling technologies, the following can be accomplished:

- 1) Allow any user to gain access quickly and securely (SSL VPN, Firewall and IPS).
- 2) Maximize every available "slot" on the global network so enterprises can take advantage of all global

capacity. Users can also be re-directed to out-of-region gateways, if necessary, using application acceleration to increase performance. In addition, Virtela creates comprehensive load-balancing solutions to maximize efficiency and performance and minimize downtime.

- 3) Accommodate high spikes in traffic on both the Internet side as well as the WAN side with highly scaleable bandwidth (using burstable ports, fractional ports, and WAN Accelerators) .
- 4) Unprecedented redundancy by 1) hardware, 2) regional gateways, and 3) diverse ISP and carrier access.

From here, we can refine the solution further with:

User Group Management

Critical end user groups can be identified and flagged appropriately to allow for different levels of remote access based on realms. Realms can be enabled or disabled, depending on the strain on the network, to allow the most critical users access in even the direst of circumstances.

Emergency Licenses

Emergency licensing is available for SSL VPN hardware for instant emergency capacity. In the event of an immediate need, emergency licensing can be enabled to add immediate new capacity. This can substantially increase the total capacity of the network for a limited period of time. Emergency licenses can be used as an interim solution until permanent licenses can be purchased. Furthermore, emergency capacity can be selectively turned on or off in proportion to the need to save costs.

Baseline Licenses

Low-cost SSL VPN devices that come with a minimal baseline license can be racked, powered and configured in the same cluster as the other SSL VPN devices. These devices would remain idle until permanent or semi-permanent capacity is needed to accommodate users. Then, the appropriate number of standard user licenses could be purchased and activated. This process usually takes between 2 and 10 days (possibly longer during

pandemic circumstances), and only requires a software key instead of a hardware shipment which could prove impracticable if logistics lines are down. Through these means, total potential capacity can be created for all enterprise users and can be purchased and enabled only when a threat is identified and remote working requirements are quantified. This new capacity is combined with the emergency licensing and load balancing infrastructure.

The result is a system that requires minimal "idle" capacity investment, the ability to handle sudden increases of connections quickly (before threats have been qualified), and the ability to upgrade permanent capacity quickly, (once threats have been properly qualified).

End User Support

With more users and new devices (e.g. home PCs) accessing the network, failure to include adequate end user

support can ruin the execution of any pandemic mitigation plan. Virtela provides the "On Demand" support required for these situations and works with the enterprise to test the system support processes regularly.

Training and Process Development

Virtela also provides the end user training programs and operations/help desk training programs to help ensure proper usability and process control from end to end.

Impact on Investment

Finally, Virtela's services can bolt into any existing WAN, or even reside on existing customer premises. Furthermore, by leasing or renting the equipment necessary for this scale of planning, and by providing all management and support functions on the back end, Virtela can provide a tailored solution free of capital investment, headcount investment, or infrastructure overhaul.



Customer Case Study

One of Virtela's deployments included a fully redundant and scalable remote access infrastructure for a large manufacturing company with over 50,000 remote users around the world. The design utilized Virtela's regional policy centers as the foundation for a hosted, cloud-based solution, which Virtela currently manages today. For this deployment, the customer chose six Regional Policy Centers (RPCs) to host an array of dedicated network and security equipment, standardized across the globe.

Global Internet Diversity

Virtela's Regional Policy Centers (RPCs) are interconnected to multiple Tier 1 ISPs, that vary region by region for maximum interconnectivity and diversity. Each RPC for this customer was connected directly to their enterprise MPLS network, making each RPC act and look like a Customer Edge (CE) on their MPLS Wide Area Network. All Virtela RPCs are fully-meshed with one another via the Virtela multi-carrier MPLS core in the event of a Customer circuit failure.

Financial Highlights:

- The Virtela solution avoided over 80% of "idle" pandemic capacity license costs.
- Rolled \$2.1M in hardware Capital Investment into Operational Expense
- Required zero headcount addition for the entire rollout and ongoing management over 3 years.
- Required zero footprint on customer premises or datacenters.

Virtela's Preparedness

One of the most critical (and typically unchecked) components of pandemic planning is whether or not your service providers and carriers themselves are ready for a global pandemic outbreak. Virtela is a leader in the industry for pandemic awareness and preparedness in the event of disaster:

- Virtela has fully redundant network and VPN capacity capable of allowing all Virtela employees to work fully from home for any period of time. Operations are fully redundant between Denver and Mumbai, India.
- Critical Virtela resources have multiple methods of accessing Virtela network resources remotely, including wired and wireless broadband access.
- Since Virtela purchases capacity from multiple Tier 1 providers, in the event one or more providers are unable to provide adequate service levels, other providers are available to quickly supplement or replace service. In this way, Virtela spreads customer risk across the aggregate capacity of multiple major underlying providers, all over the world.

About Virtela

Virtela Communications Inc. delivers award-winning network and security solutions to many of the world's largest and fastest-growing multinational companies. Currently serving customers across six continents, Virtela's network reach spans more than 190 countries. Virtela's unique Global Service FabricSM offers the foundation for delivering critical applications via the company's acclaimed service methodology, with a services suite that includes IP-based virtual private networks (VPNs), security services, Voice over IP, Video over IP, and network consulting services.

Virtela is headquartered in Denver, Colorado, with a second Network Operations Center in Mumbai, India. Virtela is a member of Juniper Networks (Nasdaq: JNPR) Managed Network Solutions Preferred Alliance Program. For more information, please call +1 (720) 475-4000 or visit www.virtela.net.

Corporate Headquarters

Virtela Communications, Inc.
5680 Greenwood Plaza Blvd.
Greenwood Village, CO 80111

Phone: +1 (720) 475-4000
Toll Free: (877) 803-9629
Fax: +1 (720) 475-4001

Sales and Product Information

Phone: +1 (720) 475-4445
Toll Free: (866) 261-4607
Fax: +1 (720) 475-4305
www.virtela.com
e-mail: info@virtela.com

Copyright 2007 Virtela Communications, Inc. All Rights Reserved.

"Virtela" and the Virtela logo are registered service marks of Virtela Communications, Inc. All products and service names, marks and slogans of Virtela Communications, Inc. are trademarks or service marks of Virtela Communications, Inc. Products, service names, marks and slogans of third parties may be trademarks or service marks of their respective companies.

