HOW RADWARE CAN HELP YOU DELIVER BUSINESS CONTINUITY AND APPLICATION SCALABILITY DURING THE COVID-19 PANDEMIC

As the Coronavirus (COVID-19) pandemic spreads, many workers are being forced to work remotely. Organizations are experiencing a subsequent growth in demand for remote access to network services and a surge in external application traffic. Maintaining business continuity with minimal disruption under these extreme conditions can be a challenge. This guide outlines best practices that can help your organization ensure its infrastructure is ready to support the increased traffic volumes due to remote access.

First, test that any remote access infrastructure has sufficient resources to support the unexpected increase of concurrent remote access connections. Second, ensure all critical services and applications are accessible remotely.

- Ensure your inbound internet access pipe to the organization has sufficient capacity
- Internet links should be backed up, preferably from two independent ISPs, to ensure remote access continuity if one link fails
- Ensure the link load balancing solution and the routers supporting it are powerful enough (and have sufficient capacity licensing) to support the increase in usage.
- As virtual private network (VPN) connectivity becomes a critical resource for the organization, ensure your VPN solution can support the increase in the number of connections and in bandwidth and has complete redundancy for continuous connectivity. Load balancing multiple VPN gateways is a proven way to provide scalability and redundancy.
- Video conferencing and voice-over-IP (VoIP) are two services which should be expected to surge. It is imperative that these systems can scale. Load balancing these systems is a recommended way to enable seamless scalability and redundancy.
- Confirm there are sufficient licenses to support the authentication of concurrent connections.
- As remote access to internal services increase, ensure that any infrastructure designated to protect these applications has sufficient capacity. Internet pipe/network protection can include cloud-based DDoS protection and applications should be safeguarded by web application firewalls, either a cloud-based firewall service or on-premise appliance.
- As your business increasingly relies on remote access connections, it is important to gain visibility into the performance of these connections and to proactively manage SLAs for remote employees, partners and customers

HOW CAN RADWARE HELP SCALE CAPACITY AND MAINTAIN SERVICE AVAILABILTY?

As organizations increasingly move their employees to remote positions, Radware offers an array of solutions and services to assist in four primary areas:

CAPACITY EXPANSION

To enable more capacity for connectivity, gateways must support remote employees. Radware supports this by offering:

- Radware LinkProof and Radware Alteon both provide link load balancing capabilities to manage the load among internet links to help ensure scalability by adding more internet links on-demand
- Radware Alteon, an enterprise application delivery controller, that load balances SSL virtual private network servers to help ensure scalability and availability
- Radware's Cloud DDoS Protection Service and Radware DefensePro provide organizations with increased infrastructure protection capacity to parallel increasing levels of legitimate network traffic.

REMOTE ACCESS AVAILABILITY

As remote access becomes increasingly important, Radware solutions are geared to provide more resiliency for remote infrastructures

- Radware LinkProof and Radware Alteon's link load balancing capabilities can be used to monitor ISP link health and delays and help ensure that traffic is always directed through healthy and available links. They also help ensure that video conferencing and VoIP are directed to low latency links.
- Radware's Alteon ADC constantly monitors the health and availability of the SSL VPN servers and redirects traffic only to available servers.

PROTECT REMOTE ACCESS

It is imperative to secure both the infrastructure and applications that remote employees rely on, including internal portals, VoIP, ERP, CRM, etc. Radware security solutions include:

- Industry leading DDoS protection through Radware Cloud DDoS Protection Service and DefensePro Radware offers hybrid, always-on and on-demand DDoS protection services to protect the organization's internet pipe and infrastructure, as well as protect the VPN servers from attacks or overuse.
- Web Application Firewall (WAF) solutions including Cloud WAF Service, Alteon Secure and AppWall, – to protect organization's applications.
- Radware Bot Manager to identify and block malicious traffic originating from bad bots
- The Radware ERT Active Attackers Feed is used to block and filter known attackers from an organization's infrastructure.

ENSURE APPLICATION SLA

As the usage of applications surge, Radware offers multiple solutions to ensure scalability and availability

- Alteon physical and virtual appliances
- Alteon Multi-Cloud Solution provides global service load balancing to allow organizations to scale local, on-premise data centers or cloud-based virtual appliances via a single, reliable solution for any environment, delivering scalability and availability.
- Both aforementioned solutions can be combined with a single Global Elastic License to enable temporary capacity expansion across any environment or form factor.
- Radware solutions provide tools to monitor the performance and health of remote connections and transactions to help ensure remote employee productivity. Radware Alteon monitors application performance and provides reporting and root cause analysis to ensure SLAs are met.

To help ensure Radware solutions can be deployed quickly and efficiently, our professional services team is available to assist with the remote deployment of any solution in any environment.