GREAT PLAINS COMMUNICATIONS

GPC SD-WAN

SCALABLE SECURITY FOR THE FINANCIAL SERVICES NETWORK

Introducing SD-WAN managed service for the financial services industry from Great Plains Communications and powered by VMware®

Providing secure financial services today is much more than protecting ATM traffic or transactional banking applications. The expansion of on-line banking and cloud-based Fin-Tech solutions has expanded the security perimeter beyond the confines of the traditional premises firewall.

That is why Great Plains Communications (GPC) has partnered with VMware®, the market-leading software-defined wide area network (SD-WAN) solution, to improve application performance and network reliability for financial providers while also reducing the time needed to open new branches.

GPC SD-WAN is a fully managed network service that provides the financial IT staff with real-time visibility into the status and performance of networks and applications. The service includes integrated security features such as transporting all data via encrypted VPN tunnels to protect financial data in motion while meeting strict federal regulatory requirements for network security.

Ensuring Financial Quality of Service

When financial institutions employ advanced Unified Communications (UC) technologies to deliver personal banking services to customers, dropped calls or jitter-heavy video conferences are detrimental to providing high-quality interactions. UC applications require a higher level of reliable bandwidth and real-time quality of service that traditional network architectures were not designed to provide.

The unique capabilities of GPC SD-WAN can detect degradation on access links and select the best path for each application to ensure consistent performance and overcome network quality issues caused by delay, jitter and packet loss. This service can even improve performance when there is only a single connection, all of which has a very positive impact on the end-user experience.

Security and Compliance

No industry faces greater threats from malicious actors than financial services and, consequently, is subject to robust regulatory oversight at the state and federal level with significant penalties for allowing a data breach that compromises customer accounts. That is why GPC has partnered with VMware to provide an SD-WAN system that incorporates four pillars of security into its solution to create a robust, in-depth defense.

Management Plane - Orchestrator

- All communications between the edges and the orchestrator are secured by TLS 1.2 over IPsec encrypted tunnels, which conform to the security frameworks specified by the National Institute of Standards and Technology (NIST).
- The orchestrator includes password-controlled user access controls with Radius and dual-factor authentication.
- Event and firewall logs can be integrated with a third-party SEIM service.
- It includes a built-in private key X.512 certificate server.

Edge and Gateway Data Plane

- All traffic between edges and gateways is secured with Federal Information Processing Standard (FIPS) 140-2 compliant IKEv2/IPsec VPN tunnels, encrypted with AES/GCM-256-bit keys and SHA-256 hash to ensure data integrity.
- Edges have local access control features to prevent unauthorized access.
- Network segmentation can create separate domains (VRF-based) to provide isolation by user (guest, PCI or corporate) or by line of business (engineering or HR).

Gateway and Physical Infrastructure

- Gateways are located in Tier-IV SSAE 16 Type II and ISAE 3402 certified data centers.
- A dedicated Network Operations Center (NOC) team maintains 24x7x365 monitoring and troubleshooting.

Regulatory Compliance

- Designated gateways are certified to comply with the Payment Card Industry Data Security Standard (PCI-DSS) 3.2 with an Attestation of Compliance (AOC).
- Data plane and control plane communications are carried through VPN tunnels that are secured by strong encryption protocols that conform to NIST security frameworks and FIPS-140 requirements for use by federal agencies.

Other key security features include Layer-7 application-based firewall mechanisms on the edges that can recognize more than 3,000 applications and be configured to perform granular outbound filtering to prevent access to inappropriate or malicious sites. Actions include allowing or denying the application traffic, and any action taken be logged for auditing.

Additionally, SD-WAN integrates seamlessly with best-of-breed security vendors (such as Palo Alto Networks, Zscaler, Symantec and Check Point) as well as advanced cloud-based security services that perform network traffic inspection for IDS/IPS and anti-virus/anti-malware filtering.

Together, these features allow financial institutions to implement the security profile of their choice to better protect the network while improving application access and availability for its end users.