CASE STUDY

Fortinet Simplifies Networking and Security for a Community Bank with a Penchant for M&A

CBS&S Bank first opened for business in 1906 in Russellville, Alabama, which is a small farming community located between Huntsville and Birmingham, Alabama, with Memphis, Tennessee just to the west. Since the bank's beginnings, it has grown to serve residents of the Southeast with 55 branches scattered across Alabama, Mississippi, and Tennessee.

Values such as honesty, integrity, and real heart, are a few of the bank's founding principles. CB&S Bank is proud of its humble beginnings and still operates like a small community bank—dedicated to helping its neighbors.

"We take pride in being a community bank and making decisions at the local level as much as possible," says Jeremy Scott, CB&S Bank's CTO. "Most community banks are smaller than CB&S, and big banks usually do not make decisions locally.

We serve a number of small communities where banking consumers have a limited number of options."

In fact, in many locations, CB&S is the only bank in town. Still, Scott emphasizes, with most utilizing online banking these days, CB&S must compete for business even in small towns.

CB&S is mindful of the negative impact that system downtime or data breaches could potentially have on its business. "A security event that damages our reputation could cripple the business," Scott says. "If systems are down, we cannot take in deposits, close loans, or process other actions that brings money into the bank. Cyberattacks on businesses such as ours, can be extremely detrimental. Cybersecurity and ensuring the stability of our network are two of our top priorities!"

Consolidating Networking and Security with One Vendor

Scott's team is responsible for ensuring that CB&S avoids downtime and its consequences. In addition to network stability, efficiency is another crucial factor in the bank's security architecture and one of the primary reasons CB&S first deployed FortiGate Next-Generation Firewalls (NGFWs) to protect its network edge.

"Several years ago we used a different brand of firewalls," Scott explains. "We moved to FortiGates because their feature set was robust and we wanted to run them in high-availability [HA] pairs."

The bank rolled out an HA pair of NGFWs in its primary and secondary data centers but continued to utilize other vendors' switches and access points. Scott says, "We worked with two different switching vendors while trying to migrate to just one, but it was a slow roll. Our wireless network was completely separate from our corporate network and used access points from yet another vendor."

CB&S Bank

"I have the network up and running in roughly 30 minutes from the time I arrive at a location. It takes longer to physically install equipment than it does to configure everything. CB&S Bank is always on the lookout for M&A opportunities and it is comforting to know we can bring our infrastructure up-to-speed very quickly in a new environment."

Jeremy Scott
CTO,
CB&S Bank

Details

Customer: CB&S Bank
Industry: Financial Services
Headquarters: Russellville, Alabama
Number of Secure SD-WAN Locations: 55

Business Impact

- Configuration changes to networking or security devices companywide take only minutes
- Firmware updates take 20 minutes vs. up to 4 hours previously

Managing the hardware and relationships with all four solution providers was time-consuming. It was further complicated due to the fact that even devices from the same vendor were an assortment of ages. "Depending on the firmware the device was running, devices might not use exactly the same commands," Scott says. To reduce the complexity of network and security management, the team started looking at consolidating the bank's switches, access points, and firewalls with a single vendor.

Throughout the due diligence process on prospective networking and security providers, Scott says, manageability was a key decision factor. "Consistency of the look and feel across platforms was important to us," he says. The standardization of interfaces and centralization of management through FortiManager and FortiAnalyzer's single pane solution made FortiSwitch secure enterprise switches and FortiAP access points good additions to the FortiGate NGFWs the bank already had in place. "We saw we would be able to reduce the time spent managing these solutions," Scott adds.

Companywide Network and Security Changes in Minutes

Now CB&S uses FortiGate NGFWs, with the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle, both at the network edge and within each branch. "We have FortiGates for our core routing in both data centers," Scott says. "Each location has a FortiGate, as well as one or more FortiSwitches, depending on the branch's size, plus at least one FortiAP access point."

The bank deployed the FortiManager and FortiAnalyzer security management tools as well as the FortiNAC network access control solution. "All these management solutions run on virtual machines at our data center," Scott explains.

True to CB&S Bank's expectations, FortiManager streamlines firewall management companywide. "We use FortiManager to make necessary changes on our devices. We create configurations and easily push those out across the entire organization in a matter of minutes, whereas before we had to individually log into each firewall, switch, or access point in all 55 sites to make a change."

FortiAnalyzer ingests logs from the FortiGate NGFWs throughout the organization, aggregates their data, and then produces reports that a third-party security firm monitors. FortiNAC, meanwhile, gives Scott's team granular control over network access. This is particularly vital in ensuring that customers and others accessing the bank's guest networks are unable to slide into the corporate resources.

"We use the FortiGate firewall in each branch to segment out our bring-your-own-device guest Wi-Fi, and FortiNAC helps us keep that separated from our corporate Wi- Fi," Scott reports. "FortiNAC puts each device into the appropriate VLAN [virtual LAN]. All our switches link to FortiNAC, as well. In our previous environment, an audit indicated that plugging a device into a switch might give it access to the network. Now that we have implemented FortiNAC, nonauthorized users cannot gain network access. They may physically plug in a device, but it will go nowhere."

In fact, he says, FortiNAC proved its effectiveness recently when the CB&S networking team was building a branch in Tuscaloosa. "All our other locations have one ITM [interactive teller machine], but in this new branch we were installing both an ATM and an ITM," Scott says. "The team tried to connect the ITM to the network and it would not work. They called me, and I looked at FortiNAC. I discovered that we had a policy allowing only one ATM or ITM device in each location. I corrected that, and the team connected the ITM with no further issues."

Business Impact (cont.)

- Much greater network access control: Only devices with specific permission get on the corporate network
- 30 minutes to get network running in each new location enables bank M&A activity
- Faster response to security threats due to improved visibility into network access and events
- Zero latency from edge firewalls and other security solutions

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiNAC

Services

- FortiGuard AI-Powered Security Services UTP Bundle

"The intuitive GUI makes the Fortinet solutions easy to manage. And because they all use the FortiOS operating system, they integrate tightly. We can manage the FortiSwitches and FortiAPs through the FortiGate firewall itself."

Jeremy Scott
CTO,
CB&S Bank

Centralized Management Enables Efficient Device Management

Rollout of the Fortinet environment across the bank's myriad sites was highly efficient. For each branch, the team first deployed the FortiGate NGFW and then came back to install the switches and access points. "We were able to put in the FortiSwitches and FortiAPs and configure the NAC all in one evening," Scott says.

The speed of rollout continues to impress, as Scott's team helps set up new CB&S branches. "I have a spreadsheet with all the different IP addresses," Scott says. "I have the network up and running in roughly 30 minutes from the time I arrive at a location. It takes longer to physically install equipment than it does to configure everything."

"CB&S Bank is always on the lookout for M&A opportunities and it is comforting to know we can bring our infrastructure up-to-speed very quickly in a new environment."

Scott's team is now working on implementing Fortinet Secure SD-WAN. A key challenge in fully leveraging the capabilities of SD-WAN, is the rural areas in which many of our branches are located where broadband connectivity can be difficult to come by," Scott says. "Having the ability to use multiple vendors [for external connections], if there are multiple options available, helps us provide the best possible service to every branch."

Scott adds, "the appeal of moving to Fortinet Secure SD-WAN gets back to the centralized management through FortiManager. Although we do not have true SD-WAN yet, we utilize rules within the firewalls to force certain traffic out over certain interfaces." As an example, he points to his team's installation of IP security cameras. "We are currently installing a number of IP cameras and we are separating them off into their own VLAN. We force them out over the broadband connection, and if there happens to be a problem with the broadband, the camera traffic will failover to the WAN circuit."

Visibility and Control Provide Top-Notch Security

"The intuitive GUI [graphical user interface] in FortiManager and FortiAnalyzer makes the Fortinet solutions easy to manage," Scott says. "And because they all use the FortiOS operating system, they integrate tightly. We can manage the FortiSwitches and FortiAPs through the FortiGate firewall itself.

"For example, using FortiManager to update certificates in one place and push out to all the FortiGates saves my team a tremendous amount of time," he adds. "The same is true of firewall policies and firmware updates. In the past it was necessary to log into dozens of devices individually with every firmware update taking three to four hours. Now, even with all the devices rebooting, we are able to complete a firmware update companywide in about 20 minutes."

More important, according to Scott, "the Fortinet Security Fabric has made our corporate network much more secure. We're able to see and control the devices on the network. If an issue arises, we're able to identify a particular device and see where it is and what VLAN it's on. If we were to experience a security event, the visibility provided by the Fortinet infrastructure would greatly assist us in responding and expeditiously tracking down the origins of the event. This insight is invaluable."

Reliability has been excellent and CB&S has experienced no latency as a result of the improved security. "The only downtime we have experienced in the past five years was the result of a weather event. Severe storms came through over a weekend and killed a port or two on one of our FortiGates," Scott says. "Other than that, the only time I restart them is when I put on new firmware. We have not seen any latency whatsoever. Even on our edge gateway, doing the SSL inspection, we have seen no performance degradation."

Scott says, "When things are running smoothly, there is little to no feedback from the top down with regard to network security and that's great! Our organization is very happy with the Fortinet environment and we really appreciate the secure Wi-Fi access to the network they provide."

August 6, 2024 4:16 AM / 2781054-0-0-EN