Case Study

Network as a Service offers security, redundancy, and connectivity to single-site businesses

Client: Single-Site Business

Client is a single-site, customer facing business, such as a restaurant, salon, or retail merchant. Client accesses an average of three mission-critical applications in the cloud that most often support credit card transactions, inventory management systems, and CRM/ERP platforms. Client depends on broadband connectivity from an Internet Service Provider to access those applications.

Challenges	CBTS solutions	Results
• Broadband providers typically offer "best effort" service agreements, not Service Level Agreements, in the event of outages to single-site businesses. • Slow Wi-Fi experience that can impact POS and other applications when businesses share bandwidth with customers. • Broadband vendors provide a stateful firewall that does not look for malware or intrusions from known signatures.	• Network as a Service (NaaS) from CBTS allows clients to access a second broadband connection or wireless connection as a failover strategy. • NaaS allows businesses to regulate guest Wi-Fi, and institute traffic shaping polices. • NaaS includes malware protection, anti-virus, intrusion detection and prevention, and application or content filtering.	• Cost Efficiencies: Network as a Service allows customers to leverage a less expensive broadband solution. • Security: Network as a Service provides malware protection and is a fully managed service. • Full management: Network as a Service offers 'read-access' or co-management functionality, both of which give clients full visibility into the network.

Challenge

The Broadband connectivity from an Internet Service Provider offers single-site clients a more economical solution than an MPLS connection. However, this configuration also creates multiple challenges that can negatively impact the client's ability to serve customers.

- Most broadband providers do not offer Service Level Agreements. Instead, there is a "best effort" understanding, meaning the provider will make a good faith effort to restore connectivity as soon as possible in the event of an outage or disruption. This isn't good enough for time-sensitive businesses where hours – or minutes – matter.
- Single-site clients – particularly those in the restaurant or retail space – frequently offer customers complimentary Wi-Fi service. Businesses that rely on a standard configuration with a single modem can experience issues with internal applications if they are also providing guests with full access to their Internet bandwidth. Imagine, for example, a busy restaurant during lunchtime that starts experiencing POS challenges because it's giving customers full access to its Internet bandwidth.
- Broadband vendors provide a stateful firewall that does not look for malware or intrusions from known signatures. This means businesses that use these stateful firewalls are not providing a secure connection for their internal users or their guests. Hackers routinely target businesses that offer free Wi-Fi, assuming that the business is using a stateful firewall. Some businesses attempt to be more proactive and purchase firewalls from a retailer. However, those devices look for malware and intrusions based on their manufacture dates, and quickly become obsolete.
- Businesses that provide guest Wi-Fi want actionable analytics to understand their customers and deliver better service in the future. Businesses also want the ability to send timely push notifications over a mobile device that's connected to the Wi-Fi network and alert potential customers about special offers. Broadband ISPs don't offer this capability.
- Businesses have limited budgets to hire dedicated IT resources. In many instances, IT responsibility falls into the broad portfolio of a general manager who is focused primarily on generating revenue and value-added initiatives to help the business grow.

CBTS solution

Network as a Service (NaaS) from CBTS is built on Cisco Meraki technology and offers single-site clients a cost-efficient investment that will allow them to leverage broadband and still meet their service, Wi-Fi, security, and analytics needs. Features of Network as a Service include:

- Failover: NaaS allows clients to access a second broadband connection or wireless connection as a failover strategy if their main broadband connection is disrupted. This helps ensure continued access to mission-critical applications.
- Wi-Fi Connectivity: NaaS allows businesses to regulate guest Wi-Fi, and institute traffic shaping polices that include eliminating access to certain kinds of content, or eliminating certain applications like video. Network as a Service also provides visibility into the network so that the customer and their IT partner can quickly troubleshoot and resolve issues.

CBTS solutions (continued)

- Security: Network as a Service Unified Threat Management (UTM) includes malware protection, anti-virus, intrusion detection and prevention, and application or content filtering - all under a fully managed service offering. Analytics show the solution is blocking 2,000 or more attacks every month in many customer environments.
- Analytics: NaaS provides tools that allow clients to map consumer and visitor interests, and turn their Wi-Fi networks into a smart analytics and marketing opportunity to attract, engage, and better understand customer preferences and behavior.

Results

- Cost Efficiencies: NaaS allows customers to leverage a less expensive broadband solution and enjoy peace of mind that comes with knowing they will have access to mission-critical applications in the case of an outage or service issue with their broadband provider.
- Security: NaaS provides malware protection and is a fully managed service, which represents a significant upgrade from the stateful firewalls that ISPs provide, and that do not look for malware or intrusions from known signatures.
- Full Management: NaaS offers 'read-access' or co-management functionality, both of which give clients full visibility into the network. Clients can then tell CBTS experts to make necessary changes, and avoid internal user errors that lead to unintended consequences.