SecureCases security and redundancy

Physical

We often hear prospective customers' concern about their data not residing within their offices. However, in many cases their office server is not even behind a locked door. In most small offices the ability to "keep the servers lit" in a power outage is limited to less than 30 minutes, after which "business is down".

At the data center where the Secure Cases application is housed, access to the first chamber in the building requires swiping a badge and entering a security code. Once inside the first chamber, the badge must be swiped to enter into a second chamber in which there are no windows and only three doors (the door entered and the two doors into the data center itself). Access to the equipment requires the badge and a fingerprint, and once inside where the equipment is located, each piece of equipment is housed in a cage that requires a combination code for access.

The data center building is constructed will a steel reinforced inner wall. Even if you drive a truck through the outer wall it is unlikely you will break through the inner wall. The roof of the building is constructed to withstand a category 4 hurricane (a factor we must consider in Florida).

Power

The equipment in the datacenter gets its power from battery backups. Power from the local electric utility is used to keep the batteries constantly charged. Once a month the battery backups are tested by purposely turning of the electric utility power. The power to the building is on the same grid as a local hospital, so it is seldom that power is lost, and it is restored quickly when it is.

However, the data center also has five industrial generators that automatically start during a power loss and have the capability to power the data center for two days. In extended circumstances, like when that hurricane is coming, the data center has a contract with a local fuel supplier who will dispatch fuel tanker trucks on location with enough capacity to sustain operation for the anticipated duration circumstances require.

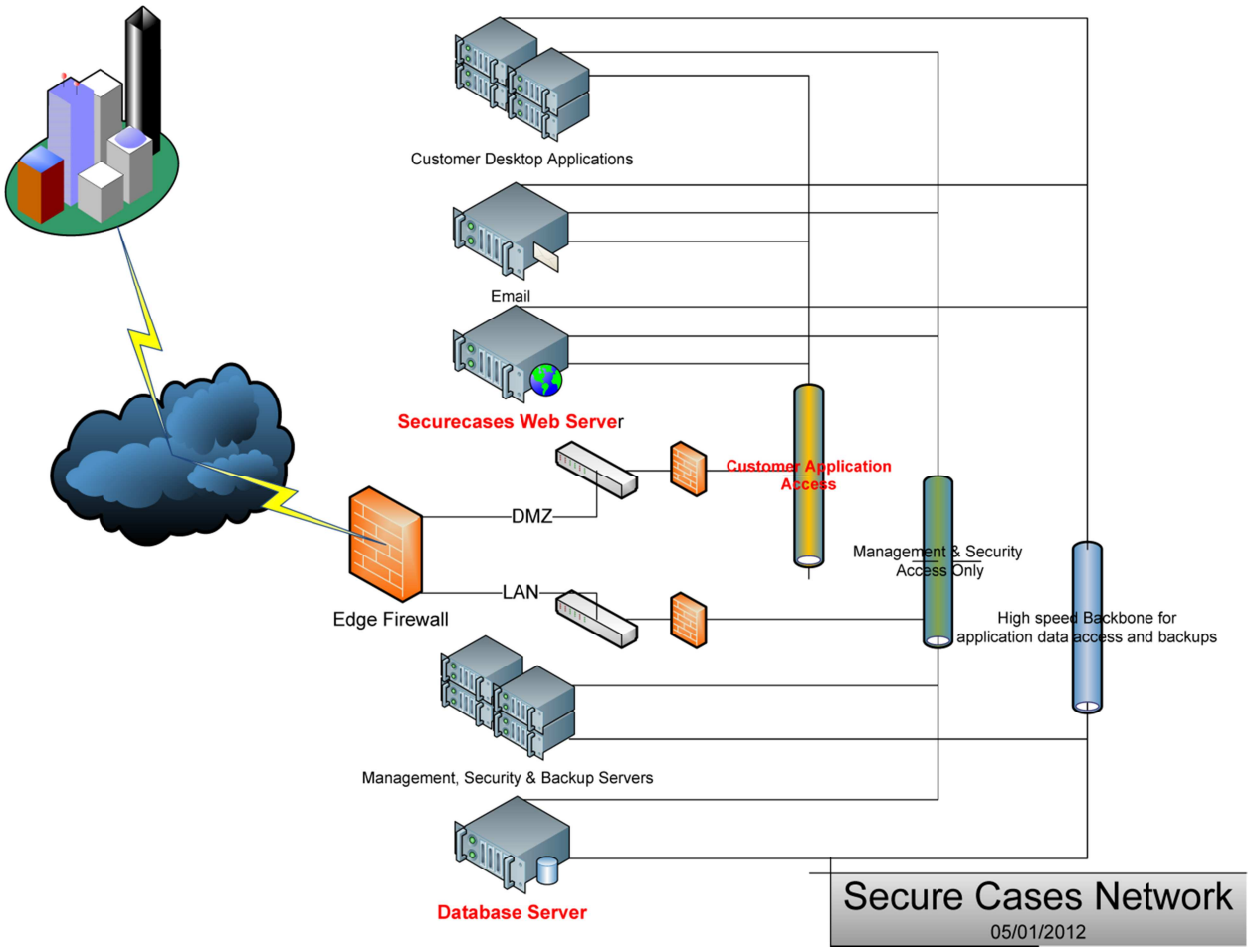
Communications

At the heart of every internet service provider's network there is a topology known as a SONET Ring. SONET rings, known as "self-healing rings," use two or more transmission paths between network nodes. To put this in English, imagine that rather than having a single telephone line or cable running from the street to your house, that instead, the cable encircled your house and each phone in your house had a line that went to a different location in the circle around your house. You could cut one of the telephone lines to the circle around your house, and you would still be able to communicate because of the connections by the remaining telephones.

The data center that houses the Secure Cases application is strategically located on top of SONET rings for three (that's right, 3 circles around us) different communications carriers and we are connected to all three. Since 2000, the data center has never lost communication.

SecureCases Network Diagram

As you can see from the SecureCases Network diagram traffic from the internet is immediately divided into Customer Application traffic versus management and security traffic and routed separately across two distinct networks. Additional firewalling then controls which customers have access to what applications.



The management and security traffic network is strictly limited to data center management personnel and SecureCases developers.

You will also note in the diagram a third network completely isolated from the internet. The SecureCases database sever resides on this network, completely isolated, from internet traffic to aid in performance, and to further remove the data from any potential security vulnerability. Only those with a “need to know” have access to the data.

SecureCases security and redundancy

Data backup

The SecureCases database (a Microsoft SQL Server database) is the heart and soul of the system. We take pride in the degree of protection we provide our customers' databases. In addition to being secured on a private network unavailable to internet traffic, the database is backed up every two hours. The last three backups are always available to be used on a duplicate database server in the event of data corruption or equipment failure.

Additionally each day a daily backup is taken and kept for a period of 5 days. This type of aggressive backup routine assures our customers protection for the valuable information they are collecting.

Monitoring

Each piece of equipment, each web site, each database and many other conditions are monitored by two servers dedicated to determining the "up" or "down" status (as well as in between states like "Hey, this server is running short on disk space"). Data center personnel are alerted in less than three minutes if there is a condition that needs a human response.

In Summary

The Secure Cases application is housed in an enterprise class data center with enterprise redundancy and security. No individual Secure Cases customer would have the resources to duplicate the environment. By providing the Secure Cases application as a service, our customers are able to take advantage of technology otherwise unavailable to them.

Acronyms

No technical treatise would ever be complete without a list of acronyms for those interested in some of the technology we use. So here it is:

Cisco Edge routers and firewalls (2 of each for redundancy)
Fortinet's Fortigate firewall (1 installed, 1 on stand-by)
Hewlett Packard Layer 2 switches (2 installed, 2 on stand-by in 100MB and 1000MB flavors)
Servers (50 and counting) manufactured by Intel and by IBM (we like the Intel servers the best)
Microsoft Windows Server
Microsoft SQL Server
Microsoft ASP.Net
Microsoft Active Directory
Microsoft DPM
Microsoft Exchange
Microsoft Forefront
SolarWinds IP Monitor
PRTG Bandwidth Monitor
Norton, and too many others to mention.