

Hosted Services: Benefits & Challenges

Matt Brunk

Hosted services are becoming increasingly important for my customers, but these services remain challenging. The struggle to move services from on-premise to off-premise somewhere in the cloud is just short of trying to sell insurance.

It takes more than passion to convince customers of my interconnect company that there are indeed benefits of using hosted solutions. The biggest challenge is how to leverage specific hosted solutions with the right mix of onsite systems and services to produce optimal results that meet or exceed customer expectations.

We started by implementing our own internal email security with a hosted solution from MX Logic more than a year ago. Immediately, we recognized benefits, but we needed to build our case and, in doing so, we implemented MX Logic's and others' solutions for our customers along the way.

We identified two recurring weaknesses that we see on customer sites. First is security—having a stateful firewall in place simply isn't enough. Second are the number of appliances and software solutions implemented in networks and on desktops. The appliances

always need patch control, and keeping the desktops current isn't always easy—and then the desktop solutions have a tendency to eat up too many resources on the end user's computer.

The drawback to onsite email security appliances is that email is getting more difficult to secure, and whatever hits your pipe has already used the bandwidth. The concept for hosted email security is simple—redirect all email to a hosted solution that only delivers clean email to your pipe.

Unlike insurance, the hosted service must provide reports, and this applies to any hosted solution—websites, forums, email servers, calendars, online help and other Web-based tools. The reporting function provides feedback, and it must provide key metrics to show the customer, by line item, the value of the hosted solution. MX Logic's portal is very simple to use and administer, and the reports offer enough clarity to adequately paint the picture; as a result, the value received is immediately perceived.

We've implemented email security for numerous customers, ranging from 1 to 500 users. In May 2007 we pooled three user companies' reports to show tangible benefits. Each customer seems to have very similar problems, and the results after each implementation yielded the same recurring benefits. Getting sites implemented ranged from extremely easy to complex.

What Goes Wrong?

First, it's really all about perception. The customer sees this service *as* a service, and no one is really convinced by the reports—they have to “see” the results.

The second hurdle that happens on every install—including our own—is that email isn't coming in. Either the MX (mail exchange) record change and/or the firewall settings on the site or host are wrong—or, the email isn't coming in because the system is in fact working.

Another contributing condition is the delay in propagating the MX record change. Fridays are always good for doing this, but the drawback may be inadequate support over the weekends in case there is a problem. ISPs can be a strange lot to deal with, as many are staffed with automated attendants, ARUs and voice mail with virtual workers.

ISP customer service levels need to be understood up front, in the planning stage, as does the feel for how they will respond to and work with the specific requests for changes on behalf of the customer. We've had one ISP to date that clearly refused to make any changes.

From the ISP's perspective, the benefit of using an email security system is that the email delivered to the customer will be clean and therefore less bandwidth will be used; also, the ISP will have less maintenance to perform on its own email server. One particular customer's IT staff is already seeking a new ISP because of the provider's refusal to lock down the firewall settings to only accept email from MX Logic and to refuse all other connections.

Along the same lines of hosted email and websites: Customers must be extremely careful to shake out the “hidden” ISP policies. Why would an ISP offer unlimited bandwidth and 1,000 user email addresses and then come back and say, “We can't handle your request because our policy only allows for 10 emails per month per user?” This particular ISP earned themselves a letter to their state attorney general's office for bad behavior.

The ISP's uptime guarantee or service level agreement (if they have one) is another must-have condition in writing. We also used the MX Logic tool that shows the number of server failures and percent of uptime to challenge ISPs not meeting three-nines availability as advertised.

What Goes Right?

Implementing a hosted email solution creates a virtual email firewall around the customer site. The effect is immediate: Customers always call to state they are not getting email—similar to, The phones aren't ringing.

After they get past the initial quieting of spam, we provide them with a daily report from the MX Logic portal. We do this for the first week, then go into monthly reporting. In a couple of days, they call back and are now satisfied with the new service. Spam pretty much disappears, save the 1 or <1 percent of messages that do get through. The kill rate of MX Logic at .9971 percent (as tested by Veritest) is quite adequate.

Evaluating Hosted Email Security

Key features and capabilities

- Technical Support (telephone and online) and hours/days provided

- In-House Expertise
- Reports
- Training tools
- Disaster Planning and Recovery
- User Tools
- Compliance
- Message Archiving
- Written Guarantee □

Matt Brunk is president of Telecomworx, a Maryland-based interconnect. His blog is at www.voiploop.com

Case Studies: Configurations, Problems And Solutions

■ **Customer #1**—Using hosted website, forums, online help, FTP.

Firewall security and client-based anti-spam/anti-virus software was not enough to keep PCs clean; there was too much spam and too many outbreaks of viruses.

Implemented MX Logic, moved MX record for domain from hosted website to MX Logic's hosted service.

Summary: This was a very low-risk project and we simply logged into the hosted Web server and redirected the MX (mail exchange) records for the domain to MX Logic. MX record changes can take hours to a day to propagate, so consider this whenever a change to the MX record is made.

Users downloaded the tool supplied by MX Logic for Outlook, which provides a button ("Delete As Spam") for when spam does get through. Clicking the button sends the message back to MX Logic for further analysis. Users receive customized reports at the end of each day detailing questionable messages.

■ **Customer #2**—Using hosted website

Firewall security and client-based anti-spam/anti-virus software was not enough to keep PCs clean. There was too much spam, as well as high maintenance on PCs and wiping drives.

We implemented firewall managed client that enforced anti-virus/anti-spam and moved MX record for domain to MX Logic hosted service.

Summary: The customer host scheduled the MX record change, which took two weeks for a simple change. All users started complaining Day 1 that their email was not coming in. Most of their traffic had been spam, now stopped, and their legitimate email traffic was less than entertaining. Users simply did not know how to react to not getting the volume of spam they had grown accustomed to.

PC maintenance is significantly down, to just minor repairs or changes of aging equipment.

■ **Customer #3**—Used dedicated email servers in the past, changed to a hosted solution and still had slow email, too many security breaches, too much spam, high maintenance on PCs. Customer prefers "virtual" approach and is not willing to take on more gear and appliances, which distracts them from their core business.

Implemented virtual email server and mailing list data-

base, and moved MX record for domain to MX Logic hosted service.

Summary: The virtual email server was upgraded within a month of the first implementation to accommodate more burstable bandwidth. Bounce-back messages and the error logs from the virtual server were critical in determining user issues vs. system/network issues. Most were user issues, and since they had no track record of the past, they didn't know how to effectively do mass-mailings using their email without being flagged as spammers themselves. The email database is MajorDomo, a freeware package that is good but requires a degree of skill and understanding.

Using different mail lists is a good tool, but it can go awry. The basic concept is that the user creates a list, "Remote Workers," for example, and then adds members' email addresses to the list.

But in this case, what the customer staff did was add other LIST names as members, which created an email loop. When one user sent a message to the LIST (Remote Workers) the message kept repeating over and over again since one of the members on the LIST (Remote Workers) was another LIST (Managers); and in that other LIST (Managers) was a member of Remote Workers.

The host detected a high traffic volume, shut down the server, and by the time they discovered the problem, the customer's domain was flagged as a Spammer. It took several weeks to get the domain removed from the blacklists and all the LISTS checked and modified.

With the hosted solution, maintenance of PCs decreased significantly. In the past, using mailing lists created an email dependency with the field workers. Changing to using a secure email list was painful and the mistakes noted above were more than a learning experience. The mailing lists had represented a means to communicate with these detached workers.

Compliance and understanding of how the mail database works will dictate better methods and best practices. Training and monitoring of changes showed that the customer technical staff didn't understand how to use the business tool, and employees had to rethink how they are using email and how to use the email list effectively□

A common threat identified in the reports are spam beacons. Spam beacons are tags embedded in HTML that give spammers the ability to confirm if their messages have been opened, indicating that the spam message reached a valid email address. The bad guys are constantly on the prowl seeking new targets and weaknesses in the systems, and this includes customer email servers—whether onsite or hosted. The servers are

exposed to extraneous traffic and security threats and require onboard security and/or another appliance to filter the email traffic.

For every issue in IT, networking and telecom, there always seems to be someone ready and willing to offer an appliance with a subscription-based software plan to fill the need. The hosted solution is great leverage since you can position the service between your networks

and/or other hosted services without the burden of more appliances, patch control and maintenance.

A hosted email security solution acts like another firewall designed just for email. This is a huge benefit, since firewalls and client software won't catch every possible security issue associated with the Internet. It's tempting to look at the report in Table 1 and discount the need for Customer #1 and #2 (i.e., the

TABLE 1 Benefits Of Enhanced Security

	Month	Viruses Blocked	Spam Beacons Blocked	Invalid Email Addresses Blocked
Customer #1 (5 users)	May	3	572	13,210
	June	0	374	7,177
	July	34	286	7,907
Customer #2 (25 users)	May	0	569	5,087
	June	6	537	4,833
	July	15	704	6,112
Customer #3 (475 users)	May	1,286	2,712	20,337
	June	15	3,208	19,792
	July	39	2,721	18,685

smaller customers) to have ongoing protection against viruses. Historically these customers, among others, may show no viruses blocked during one month, or may have low block rates.

But the real danger is the temptation of some customers to develop a false sense of security and conclude that the service is no longer needed. This is errant thinking. Appliances and software firewalls use signatures and rely upon updates to identify viruses and malware, so if you discontinue the service, you're not protected against new exploits.

(Arguably, there is no such thing as "real time updates," since a new exploit must first be discovered, then the anti-virus software must be changed or tweaked to identify the new method or signature that creates the attack. Nevertheless, regular updates are critical to keeping protection up to date.)

You can see the volume of spam that hits your network when you look at the reporting console under "invalid email addresses." Spammers use scripts to hit every possible email address and address scheme.

The email security portal also allows another countermeasure by using the policies to set and adjust email security in how invalid email receipts are handled. Accepting delivery and silently discarding invalid email messages doesn't really send a message to the spammers, but denying delivery doesn't discourage them, either. The only real way to dampen the spammers is to gather enough evidence and sue them.

Concerns And Considerations

Does a hosted email security solution negate the need to have local anti-virus/anti-spam clients? The short

answer is no, and the long answer is the same—no.

From a pure management perspective, hosted services are viable and relieve many responsibilities from the customer, but they do create new concerns and considerations.

Proceed with caution when using hosted solutions for Web applications, email servers, and beware of the many allures of not harboring equipment onsite. There are many twists in the offered services and understanding the true cost of doing business is often elusive. Instead, what I would run to, and do as an immediate action item on any network, is procure an email security hosted service, because you will reap more benefits faster. It will be challenging with larger user populations, but the change is worth the exercise, and the benefits should outweigh the pain.

As shown in Table 3, productivity benefits are realized from users not having to go through their email messages, discerning spam and then deleting it. We assumed 5 seconds as the value of time. Even if it's one second, that's an improvement worth obtaining.

Summarizing, the benefits of hosted email security center on realizing improved security, reduction of band-

width used at the customer premise and user productivity gains:

■ Hosted email security acts like an additional firewall customized for enterprise email.

■ Reduction in bandwidth usage has a positive ripple effect, as does reducing the amount of time that users waste to determine if an email message is spam.

■ In all cases, we have seen reduced PC maintenance (repair, clean, rebuild).

Deploying the MX Logic solution produced immediate results, but it's imperative that users/customers understand that when making changes to records, time is needed for the change to propagate across the Web.

■ Finally, remember that once the change to the hosted service is complete, the result is that things often seem "too quiet." Most customers react the same way—are we still getting email? But this is a better reaction than, "When can you come out to fix our network and PCs that are laden with viruses and malware?"

The Future

In November 2005, in "Clean Pipe vs. Dirty Pipe" I reported at VoIPLoop.com what Broadwing was doing with the innovative "fingerprint sharing" technology which uses Peakflow SP, a product of Arbor Networks. According to Arbor Networks, fingerprint sharing technology and the Fingerprint Sharing Alliance were developed by Arbor to provide a framework for dynamically sharing network anomaly details, or fingerprints, so that providers can consistently protect one another and their customers from today's lightning-fast-distributed threats.

TABLE 2 Bandwidth Reduction

	Month	Spam Rate % Blocked	Total Bandwidth (Mbps) to MX Logic	Total Bandwidth (Mbps) to Customer Site	Net Bandwidth (Mbps) Savings
Customer #1 (5 users)	May	89.9	160.7	16.23	144.47
	June	57.4	83.8	35.7	48.1
	July	56.2	85.5	37.44	48.06
Customer #2 (25 users)	May	78	163.6	35.99	127.61
	June	77.7	171.5	38.24	133.26
	July	79.1	126.8	35.84	90.96
Customer #3 (475 users)	May	42.6	579.2	332.46	246.74
	June	45.3	384.5	210.32	174.18
	July	42.7	438.8	251.43	187.37

TABLE 3 Productivity

	Month	Spam Messages Blocked	Time (seconds) Used by User to Review & Delete	Time in Hours Saved
Customer #1 (5 users)	May	13,220	66,100	18.36
	June	7,920	39,600	11
	July	8,633	43,165	11.99
Customer #2 (25 users)	May	5,825	29,125	8.09
	June	5,428	27,140	7.54
	July	6,729	33,645	9.35
Customer #3 (475 users)	May	22,519	112,595	31.28
	June	21,758	108,790	30.22
	July	20,237	101,185	28.11

Convergence seems to be on everyone's mind as companies continue to buy up other companies to bring about better integrated solutions. It will take many

baby steps to get where we're going. For example, we're seeing Sonicwall purchase backup data, VPN and email solutions, strengthening their line.

Eventually, maybe we'll see the same with hosted solutions—providers and ISPs willing to take on the venture. The role of the ISP and host will become more important as the services and applications are blended, rolled out and then converged.

Whatever ends up hitting the converged pipe must be clean. Keeping the network—LAN or WAN—clean today is akin to watching the dog chase his tail—it's never ending□

Companies Mentioned In This Article

- Arbor Networks
(www.arbornetworks.com)
- Broadwing (www.broadwing.com)
- MX Logic (www.mxlogic.com)
- Sonicwall (www.sonicwall.com)