Sandbox and Secure Email Gateway
Perfect Partners

Email has long been a preferred attack vector for Cybercriminals and nearly all mid to large businesses use a Secure Email Gateway (SEG). However, today’s Advanced Persistent Threats (APTs) are specifically crafted to bypass traditional security techniques. This is why leading Secure Email Gateways continue to evolve to deliver additional levels of protection.

Specifically, the latest secure email gateways combine a number of newer technologies—such as real time inspection of URLs directly on the hardware along with sandboxing as a separate but integrated extension. These complement the traditional combination of whitelists and blacklists, sender and recipient verification, IP and URL reputation, content and object inspection, and more.

Together a Secure Email Gateway and Sandbox form a powerful tandem to thwart sophisticated threats and are perfect partners for following three main reasons.

Diagram 1: Secure Email Gateway and Sandbox Working Together

Benefits
- Reduced risk of a compromise and data breach
- Simpler to deploy and manage than point products or separate systems
- Ability to truly deploy “inline” without slowing the business
Reason #1: Email is the TOP vector for targeted attacks
If we look at common patterns of advanced attack we see that, along with exploit of vulnerabilities, email is often the initial entry point attempted by Cybercriminals. In fact, according to Verizon’s 2014 Data Breach Incident Report, email attachments were the number 1 vector by a wide margin (78%) for Cyber-espionage. At FortiGuard Labs, we commonly uncover the following attack lifecycle while investigating emerging threats.

Step 1: Reconnaissance and Incursion
Sophisticated cybercriminals typically start with reconnaissance on the target organization. They then often craft a clever email, with a malicious link (or file) in it, and send the email to targeted recipients. This is where your antispam/antiphishing solution seeks to block the email. But if it doesn’t: the email goes to the target, whom the attacker hopes will click on the malicious link (or file).

Step 2: Establish Communication and Begin Attack
If the target clicks on the link, traffic will go out to a website to establish communication. This is where your web filter may block the traffic but if it doesn’t: that malicious website site starts to attack your organization.

Step 3: Attempt to Exploit and Enter
The malicious website will usually launch exploit attacks at the target to gain access to the system. This is where your intrusion prevention system (IPS) attempts to block the attack, but if it doesn’t: a tunnel is opened and malicious code delivered.

Step 4: Malware Installation
With malicious code seeking entry, ideally your anti-malware will protect you, at the gateway or client device itself. But if it doesn’t the attacker gets executable code into your system.

Step 5: Lateral Movement and Data Exfiltration
Once the malicious code is running, it usually looks to access credentials, move laterally in search of sensitive data and collect/stage it within your organization. But in order to complete its mission, it needs to exfiltrate that data out to a command & control server. This is where your application control, IP reputation, botnet and other protections come into play. If they don’t block this traffic: You are breached.

Your Secure Email Gateway traditionally includes many of the mentioned technologies to help thwart advanced attacks- antispam, antiphishing, embedded URL inspection, anti-malware and more.

Further, it should be complemented by a Next Generation Firewall, including Firewall, IPS, Application Control, Botnet Detection and more.

This is the classic security model and provides critical elements of protection to prevent attacks by acting on what is known.
Reason #2 Sandboxing is a Natural Complement to SEG Technologies

Unfortunately, we don’t live in a black and white world, where everything is known to be either good or bad. Email senders, email messages, email content…they all run the spectrum.

Yes, we have whitelists of known good senders and blacklists of known bad senders.

Yes, we have known good message structures and known bad email campaigns.

Yes, we have known good URLs for safe sites and known bad URLs for malicious ones.

And yes, we have known good code verified by various methods and known bad code and code families that have been previously identified.

But the world of email in particular is also full of grey-compromised systems that send legitimate mail from users by day and unwanted messages at the behest of bot herders by night, compromised sites that are 99.9% legitimate but have had iframe or other malicious code inserted without permission of the site owner and so forth. Not to mention new servers and sites set up, as well as messages and code crafted, as part of custom campaigns that are completely unknown. This grey has been proven to harm organizations large and small, in critical ways these past few years.

Fortunately, sandboxing has emerged as an excellent way to conduct further inspection on payloads in this grey area. Specifically, objects like attachments and URLs that represent a potential risk to the organization are placed in a safe, isolated environment that replicates end user operation.

In this environment, you can run code, observe it and rate it based on its activity rather than attributes.

So when you consider the use of these technologies all together—safelists and blacklists for known good or bad, heuristics and reputations for suspected good or bad, and sandboxing for those things not yet known or suspected—you can see how they deliver protection across the full continuum of code you might encounter.

Reason #3 Email is the Best Protocol for Sandboxing

But while Sandboxing is a critical technology to uncover APTs, it is both processor intensive and time consuming. Remember, this approach looks at the full run-time execution of not only the initial object or URL but also subsequent downloads and communications. On average, the time required for full sandbox analysis takes 1 minute or more, not the seconds or microseconds required of inline security products used in production environments. As a result of this potential latency sandboxing is generally deployed out of band to detect advanced attacks.

However, remediating the detected attack does take time and effort, so it’s better when possible to prevent such attacks from ever being delivered.

This is why deploying sandboxing as an integrated extension of your secure email gateway offers better protection even when integrated firewalls can pass the same objects from SMTP traffic to a sandbox. Specifically, because SMTP is a “store-and-forward” protocol, users rarely notice delays in message delivery which makes a policy of quarantine and hold for sandbox rating possible. As a result, organizations can now truly block advanced threats inline.
Conclusion

As a result of the sophistication and sheer damage that can result from today’s advanced threats, organizations are looking to complement traditional security technologies - that act on the known (or highly suspect) good or bad - with those that can explore and classify the unknown.

The most common technology considered for that purpose today is sandboxing. And it is increasingly available as an integrated component of existing infrastructure rather than a stand-alone solution operating independently. Integration between your Secure Email Gateway and Sandbox makes perfect sense given:

- Email is arguably the most common early stage vector of attack for advanced threats.
- Sandbox classification of the “unknown,” complements established email security technologies for the known.
- Its “store-and-forward” nature allows the time needed for additional sandbox inspection “in-line” so together they can prevent APTs from reaching an end user.


The Fortinet Solution

Fortinet’s FortiMail delivers a powerful set of email security technologies that consistently earn it top marks in independent third party testing. These include:

- IP Reputation: a real-time rating of email senders
- Compact Pattern Recognition Language (CPRL): proactive identification of malware families
- Embedded URL Inspection: a cloud-query to check links within messages
- Various sender and recipient verification techniques
- FortiSandbox Integration: for additional inspection to identify previously unknown threats.

FortiSandbox is a new advanced threat detection appliance which demonstrated 99% effectiveness during the NSS Labs Breach Detection Systems Group Test.

Powered by FortiGuard Labs expertise, FortiMail and FortiSandbox, as well as FortiGate, work hand-in-hand to prevent known threats and threat classes, detect previously unknown attacks and respond with automated mitigation.

For more information, read “Playing Safely in the Sandbox” http://www.fortinet.com/resource_center/whitepapers/fortimail-playing-safely-sandbox.html