All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Firewalls are alive and well: here's why

Many years ago, Gartner declared "Firewalls are Dead", but some 20 years later (give or take) they are still reporting on "next-generation" firewalls. Why is that?

Right to the answer

Firewalls provide an economy of scale by substantially reducing the input sequences and noise that can contact interfaces. Let's break that down:

- **Economy of scale:** Whether a single firewall is used at the border to a network area or firewalls are placed on every endpoint, they provide an economy of scale because the configuration and management of the firewalls can be unified and centralized. This provides both an economy of scale and a point of risk aggregation for common mode failures.
- **Reducing input sequences:** As a fundamental, a firewall reduces the total set of input sequences that can get from one side to another side. While imperfect in terms of eliminating all attack sequences, it can eliminate many of the distant mechanisms for exploiting weaknesses in the proximate network environment. That means that the existing weaknesses are not directly exploitable from a distance.
- **Reducing noise:** When used at network boundaries, a single firewall can eliminate a large portion of the possible traffic at one point, reducing the noise level in the 'interior'. That translates into less proximate bandwidth usage and interference, fewer traffic items to log and track, and reduced load on intrusion and anomaly detection systems. Less noise means better signal to noise ration means reduced false negatives and false positives. (it's complicated, but for lots of reasons).
- **Contact interfaces:** Firewalls protect by limiting contact with network interfaces. Every interface and every service operating on every interface introduces the potential for harm from outside influences. The fewer accessible interfaces, the fewer the potential input sequences that could cause harm. This isn't just about flawed code that allows bypass of controls or unauthorized remote access. It's about availability, accountability, transparency, custody, use control, and integrity as well. Reducing or eliminating unnecessary contact produces lots of savings.

The claims against firewalls

But firewalls are ineffective against… lots of things. Indeed, and most windows don't stop rocks or bullets or flashes of light or external surveillance. But they do stop wind and water.

- **They don't block all the interfaces:** Yes, there are interfaces without firewalls. Like sound and video input and output. And there are also doors, chimneys, and drains.
- **They only block some of the traffic:** Yes, they don't stop traffic authorized to pass. Neither do windows.

- **Attackers go around them easily:** Yes, the attackers use Trojan horses and viruses that pass through or within authorized traffic. And people walk through doors.
- **Mobile devices aren't sitting behind corporate firewalls:** Actually, they can be, if desired (via VPNs for example), and mobile devices can have firewalls configured on them as well.

Really, the claim against firewalls is that they only do what they do. And that is true, of everything that does anything.

But they are not effective today!

Attackers have learned to avoid firewalls rather than try to directly attack them. First they gain access through some other method and then, once on the interior network, they act as an insider and run **free**.

- **Free** in the sense of being able to directly attack interfaces of systems in proximity to the once(s) they have gained access to.
  - But for networks implementing zones, subzones, or temporal microzones, the proximity is again limited, to the zone, subzone, and temporal microzone available at any given time.
    - Which is to say, network segments without firewalls in place.
      - Which is to say, **we can make it even harder with MORE firewalls**.

Why do attackers do that?

Because firewalls work!

Attackers have to use more complex indirect processes because firewalls prevent their exploitation of simple and direct attack methods. Which is to say, firewalls are working.

So why do people urge eliminating firewalls?

It seems a fundamental of security that nobody really wants it.

- We only get security because we believe we need it.
  - We would rather not have to have a lock on the door, but since people will come in if there is no lock, if we don't want them in, we need to add a lock.
    - But they can still break a window! Yes they can…
  - We don't want animals coming in or wind blowing doors open, or we wouldn't have handles you have to turn to get in.

Effective security becomes transparent and automatic, at which point we don't notice it, at which point we don't understand its value, so we eliminate or reduce it, until something bad happens. Then we (officially) wonder how that could have ever happened?!?!?

Conclusions

Firewalls are not dead. They are effective. But they are not perfect or the complete solution to all of your problems. You should eliminate firewalls when you eliminate windows. And when the wind and rain come in, you should not be surprised.

