# IT security battle has changed ground

By Michael Xie

1 Feb 2016

The world moves swiftly; the IT security world even more so. Just a couple of years ago, securing the enterprise would basically consist of protecting an organisation from external intruders. Today, the battle has changed ground.


©ginasanders via 123RF

Education efforts from industry players have created higher levels of IT security awareness in the business world, and more firms have implemented basic security measures that can thwart direct attacks effectively.

This development is forcing hackers to up their game by figuring out alternative ways to get their hands on valuable enterprise assets. One new strategy that is becoming more common across the world is for hackers to gain entry to a corporate network by targeting its weakest points. Such points can include an unsecured employee mobile phone, or a workstation with limited access to corporate data.

These weak points typically reside in low value segments of the corporate network. Once the hacker breaks in and gets a toehold, however, he can often navigate to other more valuable parts of the network - which tend to be much more rigorously protected from external attackers - quite easily.

## Lateral movement

This 'lateral movement' modus operandi proves to be effective most of the time because many organisations do not isolate different segments of the network from one another. Moving from segment to segment is usually a breeze once hackers get into the network.

A few trends will make such attacks from within the organisation more common in the coming years:

• The increasing adoption of employee-owned mobile devices in enterprise environments. These are often poorly secured and provide a weak point of entry into the organisation for hackers.
• The exponential growth of IoT devices. Early and even current versions of these devices are not designed with security in mind, and are very tedious if not impossible to secure properly.

• Advancement in hacking techniques.

Traditionally, organisations deploy fire-walls at the perimeter of the network for protection. Edge fire-walls label all external traffic (i.e. Internet traffic) as untrusted, while designating all intra-network traffic as trusted, and handle them in two distinct ways. There are no grey areas, no ambiguity.

## Line has blurred

With the rise of attacks originating from weak segments of the network, the line delineating trusted and untrusted traffic has blurred. Merely deploying fire-walls at the edge of the network is no longer adequate - organisations need to re-architecture their network such that internal fire-walling can restrict malware flow between different segments of the organisation.

According to research firm Forrester, enterprises have built strong perimeters, but well-organised cyber criminals have recruited insiders and developed new attack methods that easily bypass their current security protections. Security and risk professionals today must make security ubiquitous throughout the network, not just at the perimeter.

Forrester advocates the zero trust security model, where the network is securely segmented, and all traffic is inspected and logged. With such a model, the information flow between an engineer and his/her marketing colleague seated next to each other, for example, will no longer proceed unchecked. Because these two employees are assigned to different network segments and an internal segmentation fire-wall (ISFW) is in place, proper policies will be applied and logs will be generated for any traffic traversing between the two departments.

ISFW comprises two kinds of technologies - policy-based segmentation that identifies a user's parameters, and dynamically and consistently enforces a security policy controlling the user's access to enterprises resources; and firewall segmentation that divides up the internal network to enable traffic analysis, logging and full security control.

## Multiple touch points

An ISFW does not replace the edge fire-wall. Instead, an ISFW provides multiple touch points within a network in order to provide security between existing network boundaries, or create entirely new segments inside of existing network boundaries. It also improves visibility by letting IT management see all layers of the network in one pane of glass.

Depending on the level of security needed between each network segment, the types of protection enabled will vary. Once a fire-wall is deployed into each segment of an enterprise network, its policy, logging and various modern detection features can help identify and quarantine users that have been compromised. Also, the fire-walls would make it much harder for hackers to do reconnaissance and discovery even if they have started to make their way inside the company network.

ISFWs should work in synchronisation with one another, leveraging threat intelligence and be complemented by advanced persistent threat (APT) detection solutions like sandboxing and endpoint security solutions so that actions can be taken to identify compromises and quarantine them as soon as they are discovered.

Enterprises' traditional objections to putting a fire-wall in front of each network segment have been around performance and price. Because intra-network traffic volume can be many times that of Internet traffic volume, not many fire-walls have the capability to handle the workloads without significant latency. Those that can handle it, when deployed in large numbers to cover each network segment within the enterprise, can make the cost prohibitive for many organisations.

## Attainable solutions

Today, however, attainable solutions exist. Modern fire-walls that leverage custom ASIC chips can be fast enough to handle internal fire-walling and be cost effective at the same time.

Some may recall that per-port security was all the rage a few years ago, until implementation hurdles put an end to that promise. Current ISFW technology is a step towards reviving that promise. As technologies in switching and access port security evolves and performance improves, we will be able to combine them with ISFW to reach that goal.

The concept of internal segmentation fire-walling has put the network security industry on the cusp of an exciting era. Firms that want to take their operations - and their business - one step ahead of the competition should take advantage of it.


ABOUT THE AUTHOR

Michael Xie is founder, president and chief technology officer, Fortinet