Firewalls: on-premises or in the cloud?

Introduction

Firewall devices, guarding internal networks from the Internet, have been a key element of network security for over two decades. Over these years, firewalls have developed in sophistication, functionality and performance—but until recently they remained physically bound to the premises of the networks they protect.

Recent years, however, have seen the emergence of Internet-located firewalls, which operate remotely from the networks they protect. These security services go by various names, such as cloud-based firewalls, security-as-a-service, and cloud security. The breadth of functionality these services offer is variable. For example, some provide very specific services, like spam filtering or virus scanning; while others offer a broad Unified Threat Management (UTM)-like service. What they do have in common, though, is that some or all of the traffic to and from the client's premises passes through the firewall provider's cloud-located equipment, where it is examined and filtered.

The cloud-based approach to network security is making a strong play in today's market, and attracting a good deal of interest. This paper considers the drivers behind cloud-based security, and examines the reasons why on-premises firewalls will long continue to have a strong market presence.

Cloud-based security services

Proponents of cloud-based security services cite the following perceived benefits:

1. Scalability – the cloud service can scale to meet the client's needs.
2. Availability – cloud providers build redundancy into their service architecture.
3. Ease of upgrade – the service provider can add functionality to the service without the client needing to lift a finger.
4. Lower Total Cost of Ownership (TCO) – there is no capital outlay for equipment, and no direct cost for staff with network security expertise.
5. Simpler management – the cloud provider carries out management tasks.

In the next sections, the value of each of these benefits is considered and assessed, in relation to the on-premises alternative.

1. Perceived benefit: Scalability

The scalability of a cloud security service refers to two operational aspects—increasing bandwidth and adding new sites.

Bandwidth

In the cloud security service model, bandwidth can be provisioned at whatever level the user requests, and the bandwidth turned up or down as the user's need change.

When using on-premises hardware, the hardware must be replaced by a higher-performance model if bandwidth requirements increase significantly.

However, the reality is that organizations' Internet bandwidth does not increase frequently, so it is typically some years between the occasions where a firewall must be replaced. Furthermore, the upgrade process doesn't have to be highly expensive or disruptive. If the new device is sourced from the same vendor as the previous one, the configuration can be copied across.

New sites

With a cloud security service, adding protection for a new site—for example, a new branch office—is just a matter of adding the new configuration into the cloud provider's system. No new hardware needs to be installed.

Although an on-premises approach to security does require a new piece of hardware to be installed at each new site, the act of installing a firewall device is not highly onerous, and the process of configuring it is of a similar magnitude to the task of configuring a new site into a cloud service.

Key points:

- Upgrading to higher-performance hardware occurs infrequently, and need not be an expensive process.
- Installing firewall hardware at new sites is no more labor-intensive than adding new sites to a cloud-based security service. In both cases, the security profile for the new site needs to be designed and configured.

2. Perceived benefit: availability

Cloud providers utilize virtualization and multi-site hosting to achieve both high uptime and immunity to localized outages.

However, the uptime of modern network hardware is also very high. Mean times between failures are typically in the order of 10 years. Combining units into redundant pairs can easily offer five nines of uptime.

Key point:

- The uptime of a cloud service is not significantly higher than a service based on on-premises hardware.

3. Perceived benefit: ease of upgrade

Service providers bring new functionality online with no action required by the customer.

Owners of on-premises hardware do have to install new software, and reboot, to introduce new features into their hardware. This does require some work on their part, but is a routine activity,

In both cases, any but the simplest new feature will require some configuration work to operate to the customer's requirements. Configuration is typically a much more substantial task than loading a new software release.

Key point:

- Utilizing new features is not a zero-cost process, even with a cloud service.

4. Perceived benefit: lower TCO

Cloud-based services are paid for on a subscription model, with possible extra fees for activities such as configuration changes, adding new sites, or upgrading bandwidth.

The costs for on-premises security are different:

- Capital cost for the hardware.
- Annual service contract and subscription fees.
- IT staff costs.

Because they are so different, cost comparisons between the two approaches are difficult to estimate. Despite this, there are a number of points that can be considered in relation to these costs.

Although the capabilities of firewalls have increased sharply, their prices have not. In fact, the competitive nature of the firewall appliance market puts a strong downward pressure on prices. Moreover, even if a site does not have an on-premises firewall, it still needs a router of some sort as its gateway. So, the decision to use a cloud security service does not remove the need to invest in gateway hardware. The cost differential between a Next-Generation Firewall and a well-featured, high-performance router with capabilities for Quality of Service, Dynamic Routing, detailed logging, redundancy options, fallback to 3G/4G connection, and more, is as low as a few hundred dollars. As a result, the capital cost savings of moving security to the cloud are not necessarily significant.

The annual service contract and subscription fees for a firewall device can be compared to the subscription fees of a cloud security service. The subscription fees for a firewall device are typically per device, whereas those for a cloud service are frequently per seat. As such, for any given comparison, the size of the organization is often a significant factor, and there is a cutover point at which the size of the organization makes the cloud service cost much less attractive than the cost of the firewall's annual subscription fees.

IT staff costs are a more difficult matter to analyze. Subscribing to a cloud security service is often promoted as effectively outsourcing network security skills to the provider's set of dedicated experts. These experts are envisaged as poring through security logs, looking for evidence of suspicious activity—an expensive activity to bring in-house.

Whilst it is true that cloud security providers do employ security experts who investigate suspicious activity, it is equally true that firewall vendors have access to teams of experts who are examining reports of suspicious activity from a broad range of sources. These experts quickly pick up new threats at large in the Internet, and rapidly provide blocks to those threats, which the firewalls download as pattern file updates, possibly several times per day.

The question then, is whether the presence of an on-premises firewall requires the presence of an on-premises security expert? The answer to this will vary from one organization to the next. There are a number of alternatives to bringing security expertise completely in-house. For example, monitoring of on-premises firewall logs can be contracted out to a security management service, or an existing in-house IT professional can upskill to perform a base level of monitoring, and have access to an outside consultant to deal with more complicated cases.

Key points:

- Hardware firewalls provide extensive features and high performance at very reasonable prices.
- Cloud-based security services do spread the cost of high-value expertise over multiple clients, but other expert out-sourcing options exist.
- Because of pricing models, the subscription fees for cloud-based services can greatly exceed those for hardware-based security

5. Perceived benefit: simpler management

When a security service is provided in the cloud, it is the cloud provider that carries out tasks like configuration backups, software upgrades, recovery from device failures, provisioning the protection of new sites, and other management activities.

While these tasks may in the past have been a significant overhead for those with their security devices on-premises, this is no longer the case. Intelligent solutions, such as Allied Telesis Management Framework™ (AMF) automate all of these tasks. Furthermore, since this automated network management is under the customer's control, there is no need to rely on an external party to carry out these essential tasks correctly.

AMF ensures that the complete configuration, operating system and licensing information of every unit in a network—including units located at remote locations—are backed up at a user-selected regular interval. The framework also provides zero-touch replacement of failed units—a factory-fresh replacement can simply be plugged into the network, and the network will reconfigure it as a clone of the failed unit. This capability is equally as available at remote sites as it is at the central site. Detailed configuration

Key point:

- Intelligent network frameworks like AMF can automate a lot of the management of on-premises firewalls

Drawbacks of cloud-based security

Cloud-based security has its drawbacks:

1. Losing ownership of security assets.
2. Unpredictable latency.
3. Vulnerability to discontinuation of the service.
4. Variability of data rate.

1. Losing ownership of security assets

The greatest risk associated with moving security to the cloud is the fact that it relinquishes the control of valuable security assets —encryption keys, passwords, and policies. No matter how reputable or careful the security service provider is, once these assets are operating in the cloud, somebody else controls who has access to them. Guarding these items is central to maintaining security —once they are compromised, so is security.

Key point:

- Security assess are highly valuable; losing control of them is risky.

2. Unpredictable latency

At least some of the components of a cloud-based security system will be shared between multiple clients. Therefore, a high load from one client can use a disproportionate amount of the shared resource, and reduce the access that other clients have to the resource. As a result, traffic from other clients will be queued, waiting for access to the shared resource. This manifests itself as increased latency in the traffic as it passes through the security service.

With dedicated on-premises hardware, the owner of the hardware has exclusive use of its resources

Key point:

- Sharing resources means variable performance.

3. Vulnerability to discontinuation of the service

If the service provider goes out of business, or decides to discontinue or significantly alter their security service, then this causes significant issues for their customers:

- Migrating to a new service requires a costly process of translating the existing configuration into a system which likely has a different configuration paradigm.
- It is difficult for the customer to verify that the service provider has completely erased any of the customer's security assets that were in their possession.

Key points:

- Service providers may stop providing their service at any time.
- Migrating to a new service provider may prove difficult, disruptive and expensive, and result in lost security information.

4. Variability of data rate

When security is provided in the cloud, then most, or all, of the Internet traffic for a protected site must pass through the cloud service. Therefore, the full path between the protected site and the cloud service must provide an end-to-end bandwidth equivalent to the bandwidth at the site's point of connection to the Internet. That is, if the site has a 500Mbps connection to the Internet, and can therefore exchange data with the Internet at 500 Mbps per second, then a consistent forwarding rate of 500Mbps is required between the site and the cloud security service. The Internet, however, is a shared resource, that forwards on a best-effort basis. As such, guaranteeing bandwidth on arbitrary paths across the Internet is not possible.

Key point:

- Data forwarding across the Internet is inherently unreliable and unpredictable.

Benefits of an on-premises firewall

Having a firewall device located in the physical network provides some benefits that a cloud-based service cannot bring:

1. Internal network security.
2. End-to-end VPNs.
3. Defense in depth.

1. Internal network security

Security is not entirely about controlling what happens at the connection to the Internet. Organizations commonly have internal security requirements—policies to protect data in one section of the organization from leaking to other sections; containment of malware infection; demarcation between guest-accessible network resources and employee-accessible resources; and collection of audit information on internal data traffic.

Moreover, scrutiny of traffic within the network is an increasingly important component of the defense against advanced persistent threats.

The volume of traffic that would need to be delivered to a cloud service to enable it to match the internal security capacity of on-premises hardware is quite impractical.

Key point:

- On-premises firewalls can provide firewalling of internal data, which cannot be feasibly achieved by a cloud-based service.

2. End-to-end VPNs

The purpose of a VPN is to ensure that data exchanged between the endpoints is subject to a specific security policy—a particular level of encryption, authentication, key re-origination rate, replay protection and so on—throughout its journey.

An on-premises firewall ensures that the VPN endpoints are at the points where the data enters and exits the customer's site. With a cloud-based security service, data must be sent to the provider's site—perhaps as plain text, or maybe in some service-defined form of encryption – before it is encapsulated into the VPN. This rather negates the nature of a VPN as emulating a dedicated connection between the end-points.

Key point:

- Using an on-premises firewall allows VPNs to protect data throughout its entire journey across the Internet.

3. Defense in depth

An optimal security strategy involves multiple layers of defense that are close to the assests being defended. Having on-premises firewalls at all sites in a multi-site network, in conjunction with security features within the LAN infrastructure, such as DOS defences, hardware filters, and client authentication, provides just this—layered defense, close to the assets.

An on-premise firewall in fact provides multiple layers of defense by itself, as it can apply security to internal traffic, as well as police communication to and from the Internet.

Combining a cloud-based security service with an on-premise firewall, of course, would be an ideal way to achieve multi-layered defense.

Key point:

- Relying on a security service located remotely on the Internet, and providing security for all sites from this one cloud-based location, does not provide the necessary depths of defense for optimal security.

Summary

While outsourcing network security to a cloud-based service can appear an attractive way to save money and reduce complexity, the reality is that there are compelling advantages to retaining on-premises firewalls.

On-premises firewalls provide many capabilities that cloud-based firewalls cannot. Security can be managed between departments or sites that may not traverse the cloud, and it can be applied in a layered approach to provide defence in depth. On-premises firewalls also ensure that information about, and responsibility for, security policies and cryptographic key material remains within the organizations that the firewalls protect. For these reasons and many more, firewalls will continue to be deployed on-premises rather than in the cloud.

Visit http://www.alliedtelesis.com/solutions/netsecurity for more information about network security, and how Allied Telesis can meet your security and threat management requirements today.

About Allied Telesis

For nearly 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Management Framework™ (AMF) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and "things"—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis**.com

Allied Telesis™ NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

C613-08017-00 RevA