Comparison of selected cloud firewalls based on provider-relevant criteria

A recommendation from the Institute for Internet Security
The Institute for Internet Security - if(is) is an innovative, independent, scientific facility of the Westfälische Hochschule ("Westphalian University of Applied Sciences"). In addition to research and development, we are a creative service provider in the field of Internet security.

Since the official opening in May 2005, the young and creative research team has rapidly transformed the institute into a leading source of Internet security expertise. Our aim is to make the Internet a more trustworthy and secure place.

Executive summary of this document

The newest generation of cloud firewalls and anti-malware solutions harbor great potential for varying target groups (telecommunications, Internet service & managed security providers). In this comparison we present various producers and their solutions and identify the extent to which they can effectively utilize and further develop the new potential offered by cloud services. Within the comparison, cloud elasticity, performance and scalability are weighed against the cost efficiency of these services.

The extensive research on the individual firewall and web security providers shows what the latest generations of their solutions are capable of. Clear winners and product recommendations emerge in the individual areas of the various target groups.

It has also been possible to identify a trend: a clear move away from appliances in the direction of cloud services. This is facilitated by the continuous improvement in bandwidths and latency times.
The challenges

In the digital world there is no such thing as unimportant data. The number of IT devices in use is on the increase, and a variety of different IT systems are employed. On top of that, nowadays a company's IT systems don't end neatly at the perimeter anymore nowadays. Boundaries that were once clear are becoming increasingly blurred by mobile devices, cloud computing and IoT. This massively increases the demands on modern IT security solutions. That is why new concepts are required to detect and effectively ward off the numerous methods of attack. The scope of functionality offered by firewalls has steadily increased in recent years. Today, stateful inspection, and port and content filter firewalls have long since left the third and fourth OSI layers (IP address and port) and established themselves on the application layer. But one important factor remains intact: the performance of the security solution. Aside from pure the analysis of all data packets, it is of course also necessary to process and forward them with the least possible delay. As such, traditional firewall appliances on the perimeter of a company can quickly become bottlenecks. That is why protection on the perimeter remains a compromise between performance and security.

The Future

Already smart watches, tablets, smartphones, IoT devices and notebooks all contain large amounts of sensitive data requiring protection. In future the number of IT devices per Internet user will increase, and the effort required for protection will increase at a similar pace. In the process IT security solutions must become more powerful, user-friendly, lower priced, more maintenance-free, reliable and innovative. If the trend continues numerous households will in future possess large amounts of complex Internet connectivity. Sustainable digitalization cannot succeed without adequate IT security!
Solutions

Today, scalable cloud firewalls are an adequate solution because the virtually unlimited computing capacity in the cloud means they can integrate numerous security and analysis functions without compromising performance.

Even technologically highly complex malware attacks in the cloud can now be detected and effectively warded off - attacks which today’s classic antivirus solutions wouldn't stand a chance with. Because, “antivirus is dead”, as was claimed in the Wall Street Journal May 2014 by the senior vice president for information security at Symantec. Instead of improving, this situation has since become even more critical.

The market for malware is very lucrative and a lot of effort goes into the constant development of malware itself. The secret of success for sandbox solutions is the fact that current anti-malware software cannot offer adequate protection anymore.

Here, the solution for millions of households can only be an anti-malware solution at the network access point, which, with the help of all the potential and resources in the cloud, not only prevents the transport, but also the communications of malware. With this approach even persistent malware can be disarmed.

Responsibility for anti-malware filters at the network access point can only be assumed by telecommunications companies, Internet service providers, or managed security service providers.

To make products available for the mass market they require very special firewalls in the cloud.
Criteria of Cloud services

With increasing bandwidths and ever more widespread cloud services, more and more IT security producers are offering cloud-capable firewalls. These cloud firewalls are used for various purposes. In the enterprise environment such firewalls are used in private clouds, to take virtualization of the networks one step further. Telecommunications and Internet service providers utilize these cloud firewalls to provide their customers with a commercial service. Since scalability and cost are what matter most, along with the standard set of next-generation firewall features that all providers here supply, these are our main criteria. This is where it becomes evident which solutions are economically and functionally viable for use in the mass market.

The evaluation of various producers of cloud firewall products is done in a quadrant system, in which each producer is ranked based on relevant criteria.
Criteria of Cloud services

Costs

Tiered cost structures make it more difficult to establish a simple price structure for customers. These are also a legacy from the era of firewall appliances - a time when the hardware itself automatically limited the number of users. Through the simple virtualization of these appliances, they inherited the old licensing systems, eradicating the innovative pay-as-you-go approach of the cloud.

For the use of cloud firewalls, the right approach is to simply merge supply and demand. Fixed prices per active user in a fluid cost model are customer and end-user friendly. Ideally, all that should be calculated here is the time in which the service was used.

The graphic depicts how traditional firewall licenses always license the „peak“ of users, whereas a cloud service lies on the use-curve and only calculates what was actually used.
Criteria of Cloud services

Scaling

In the case of central services, the scaling is a decisive criterion. Software systems that are used by millions of people require a way of automatically allocating additional resources. Here, with virtual resources the cloud technology replaces the established appliances of the traditional firewall producers. Scaling isn't accomplished anymore by expanding existing appliance structures, but rather must be performed by the system itself. When demand increases, more virtual resources are used.

As such, it is no longer necessary to buy new appliances or replace existing ones.
Criteria of Cloud services

Utilization of cloud resources

Clouds make their resources available to the virtualized systems in the form of virtual hardware. This means that, just like on a hypervisor running locally, a virtual machine in the cloud receives certain virtual resources and can work with precisely these whilst in operation.

But a cloud system is much more. It should be capable of adapting to environment variables such as rising/dropping numbers of users or more/less required bandwidth, and then reacting „elastically“ even while running. This is typically accomplished with the use of sub-instances within a cloud framework. Here, an orchestration instance itself can allocate/release virtual resources, so it can also start/delete new sub-instances.

Working with these cloud resources should be as economic as possible, because in cloud environments, in particular, free resources are needed for other services and shouldn't lie around unused. High-performance use of available cloud resources is essential for cost-efficiency in cloud firewalls. Aside from that, compatibility with a large number of cloud providers is a deciding factor for cloud environments that have already been established. Cloud instances are virtual machines which should generally support all common hypervisors, such as VMware, Xen, KVM and HyperV.

Cloud management platforms (CMP), such as OpenNebula for example, should also be supported. These are also necessary for combining heterogeneous computation resources and facilitating joint management and monitoring.

Commercial public cloud providers, such as Amazon Web Services (AWS), Azur, and others, should also be supported.
Criteria of Cloud services

Elasticity

Within virtual environments and ideally also in a cloud platform the system itself should decide how much virtual resources are required and then allocate them in real time, but also release them again when they are no longer needed.

This way, real time demand can be reliably satisfied. Elasticity helps implement need-based services, simply and in a user-friendly way.
The quadrant system

In a Cartesian coordinate system, the selected cloud firewall providers are plotted as coordinates based on the relevant criteria. With these coordinates an additional quadrant system was inserted near the achieved values. These quadrants characterize the individual providers in levels of suitability for the mass market in the cloud firewall area.

The axes
The X-axis denotes cost-effectiveness. In addition to costs per end-user, here the license model and the cost-efficient use of cloud resources is depicted. The Y-axis uses the scalability and performance of the individual cloud firewall solutions as criteria. This reflects the properties known in the cloud as „elasticity“.

Selection criteria for cloud firewall providers
Eight producers qualified for classification in the quadrant system. They are all active internationally and have at least one firewall product line in their portfolio. The overriding criterion here is the cloud usability and not the firewall functionality itself, which means even producers from the area of routing were included.

The information gathered originated from interviews with the individual producers, and from their websites, presentations, trade fairs, conferences and brochures.
Check Point

Check Point has headquarters in Tel Aviv, Israel and San Carlos, California. They are one of the world’s largest providers of IT security, with a broad portfolio in the area of next-generation firewalls, endpoint security, and mobile security.

Among others, Check Point offers virtualized versions of its appliances for:

Private Cloud

Supported are Cisco ACI, VMware NSX and OpenStack. The primary goal of these installations is to filter internal traffic between the virtual machines (east-west traffic).

Public Cloud

Here, Amazon Web Services (AWS), Microsoft Azur, Google Cloud and VMware vCloud are supported. Installations in the public cloud make it possible to protect and filter the services and machines outsourced to the public cloud, and expand them with secure VPN functionality.

Data center

Network function virtualization (NFV) support is extremely important for operators of data centers. By integrating vSEC products in an NFV environment the firewall is also excellently suited for use with software-defined WAN and vCPE installations.

Check Point is the number one choice when offering commercial firewall cloud services for major companies and enterprises. But the price and the complexity of the high-end technology makes Check Point unsuitable for other target groups.

Strengths

- Market leader in the area of enterprise firewalls
- Very good management solutions for the administration of extensive enterprise firewall installations
- Largest R&D resources in the firewall market

Weaknesses

- Cloud products are virtualized appliances and not optimized for elasticity
- Typical tiered licensing is offered
- The Sandblast sandbox solution does not perform as well as that of direct competitors
The providers in detail

Zscaler

Zscaler originates from San Jose, California, and is purely a provider of cloud security. Gartner lists Zscaler with more than a 50% market share in the global cloud-based secure web gateway (SWG) market.

Zscaler’s products run on its own Zscaler cloud, which, according to the company itself, is the world’s largest cloud security platform, with more than 100 data centers around the world.

Zscaler is also represented globally by more than 1000 points of presence, making it the dominating cloud security provider.

In addition to typical firewall-as-a-service/secure web gateway, Zscaler’s portfolio also includes sandboxing, DLP, and bandwidth management solutions. But all of these are tied to the Zscaler cloud product.

Zscaler publishes its Zscaler cloud availability status at: https://trust.scaler.com

Strengths

- Market leader with >50% of global market share in cloud-based SWG market
- Inspection of SSL/TLS web traffic
- Global Zscaler cloud network with more than 100 nodes in 30 countries

Weaknesses

- No on-premise solution without use of Zscaler cloud
- The Zscaler app, VZEN Virtual Proxy, has been available since December 2015 and still has weaknesses
- Tied to US legislation
Secucloud

Secucloud is active worldwide as provider of high-availability, cloud-based IT security solutions and has its headquarters in Hamburg, Germany. The purely cloud-based IT security products and services, which were conceived and developed from the outset exclusively and specifically for cloud environments, offer an integrated, uncompromising high-security and performance approach. The Elastic Cloud Security System here combines diverse security systems in the ECS² architecture with a global security cloud infrastructure.

The Elastic Cloud Security System (ECS²) product is suitable for use in both the private as well as the public cloud and is always used white-labeled as on-premise solution by telecommunications and Internet service providers.

An additional product is currently in the introduction phase. The marketplace solution (MPS) is offered in the form of public cloud security as a service, and is aimed at resellers in the area of SMEs that are looking to offer their own (white-labeled) firewall-as-a-service.

Private Cloud

ECS² supports virtually all hypervisors such as VMware, Xen, KVM, etc. and can also be run with OpenStack and OpenNebula.

Public Cloud

ECS² supports public cloud providers such as Amazon Web Services and Google.

The MPS can even be hosted in the public cloud, or used as service in the form of a ready-made solution, similar to Zscaler.

Strengths

- Sole genuine virtual on-premise solution with cloud base
- Cloud licenses allow very low-prices on mass market
- Automated scalability/elasticity

Weaknesses

- Small market share in global cloud security market
- Secucloud is a young enterprise
- Lack of optimizations in products for enterprise security use
The providers in detail

Cisco

Cisco comes from San Jose in California and features various cloud products in its portfolio. The Web Security Appliance (WSA) is also available as virtual appliance. The firmware of the appliance has been virtualized on a hypervisor. It is identical to the firmware of the appliances, so it is not aimed at cloud use.

Cloud Web Security (CWS) is purely a cloud-based web service. It has been on offer since 2016 and allows the central administration of various Cisco hardware (or virtualized) appliances.

Made available via the cloud as web proxy, Cloud Web Security provides distributed companies with security and control for the Internet connection. Users are protected at all times, regardless of location or device used. This is because the solution utilizes Cisco’s global threat intelligence network, applying functions to protect against threats.

Private Cloud

In the private cloud the virtual appliances of the Cisco WSA can be used to control east-west traffic, but also to protect the Internet interface of the private cloud.

Public Cloud

The latest product available from Cisco for the public cloud is called Umbrella, and was derived from the acquisition of the firm OpenDNS. Here, providers can sell DNS security, which is based on the Cisco network in the cloud (similar to Zscaler).

Aside from that, through the Cloud-Lock product Cisco also offers a CASB (Cloud Security Access Broker) service.

Data center

In Cisco’s broad portfolio many products can be found which are ready for security in the SDN and NFV areas.

Strengths

• Extremely widespread in the entire enterprise network environment
• A market leader in the IT security area
• Very broad portfolio of network and IT security products

Weaknesses

• Cloud service has only been on the market since 2016 and is still in an early phase
• Virtual appliances are not designed for cloud properties
• No automated scaling for changes to user numbers
The providers in detail

**Juniper**

Juniper Network has its headquarters in Sunnyvale, California. The focus of Juniper IT security products is strong on routing, because Juniper has its origins in this business and only later moved into the IT security market.

The SRX firewall series is supplied in 28 different hardware variations, but is based in each case on the company’s own JunOS operating system. This firewall solution is also available as virtual appliance.

The vSRX is a VM version of the firewall, whereas the cSRX is a container version of the firewall and takes a micro-service approach. By using Docker as container management solution it is possible to run flexible and highly scalable deployments of the cSRX even with SDN and NFV.

**Private Cloud**

On VMware or KVM the virtual vSRX can make a firewall available as virtual machine to separate and filter networks/zones.

The vSRX is also available in Amazon Web Services Marketplace and can protect private cloud resources in connection with the AWS VPS in particular.

**Public Cloud**

With cSRX container firewalls, service providers are provided with a way to serve larger numbers of security service customers than would be possible with simple virtual machines.

**Datacenter**

Juniper products have long supported data center virtualization with SDN and NFV. Here, integration with Contrail, Opencontrail and other third-party solutions is offered.

**Strengths**

- Hardware delivers high data throughput rates
- Wide distribution of offices worldwide
- Software-defined networking has been fully supported for a long time

**Weaknesses**

- Firewall features announced late
- Lagging behind with new public cloud support and support for virtualization
- Have been losing share in IT security market for years
The providers in detail

Palo Alto Networks

Active purely as IT security producer, Palo Alto Networks has its home in Santa Clara, California. With its innovations in the areas of application control and intrusion prevention systems, Palo Alto played a decisive role in the definition of the term next-generation firewall.

The firewall product line comprises 19 models, with its top model providing a maximum throughput rate of 200 Gbps. With the support of VMware, Palo Alto provides its customers with a way to virtualize its appliances (VM series).

Private Cloud

In private cloud environments as well as in the VPC of the Amazon Cloud the virtual VM series of the Palo Alto firewall can establish a segmentation between own systems (east-west traffic) based on existing licenses (BYOL = bring your own license).

Public Cloud

For the public cloud of a service provider the VM series of the Palo Alto firewall can act as Internet gateway in the classic, but virtual, sense. As opposed to WAF (Web Application Firewalls), however, the VM series inspects all traffic on the application and user levels, as is also the case with the hardware appliances.

Data center

With the VMware NSX support of the VM series, Palo Alto also satisfies the requirements of an SDDC (software defined data center).

Strengths

• Market leader in next-generation firewall enterprise segment
• Supplied innovative next-generation firewall features long before the competition
• Aside from Check Point, the most widely used enterprise firewall solution

Weaknesses

• Virtualized firewall appliance supports far fewer hypervisor systems than the competitors (in particular a Microsoft Azure implementation is lacking)
• As enterprise firewall producer, too expensive for small and medium sized enterprises. Even in the enterprise market Palo Alto has one of the highest prices per protected gigabit.
• With its „Traps“ endpoint solution Palo Alto hardly has any market share and cannot replicate its enterprise firewall success in the endpoint market
**The providers in detail**

**Fortinet**

Fortinet comes from Sunnyvale, California. This producer of firewalls has mainly hardware appliances in its portfolio. With its UTM and enterprise firewalls, Fortinet can be found in companies of all sizes. As producer of firewall appliances based on special hardware, Fortinet supplies a virtualized version of its firewall firmware which, because it has to make use of virtual interfaces of standard hardware, delivers only average performance.

**Private Cloud**

Fortinet supports all current virtualizations such as VMware, Citrix Xen, KVM and Microsoft Hyper-V, for securing private clouds with a virtual Fortinet appliance. Here, the focus is on internal VM communication, which can monitor traffic with transparent VDOM also on layer 2, for example in the same broadcast domain.

**Public Cloud**

In the Amazon and Microsoft public cloud, Fortinet’s virtual firewall appliances can be run with tiered licenses, just like with the hardware appliances.

**Strengths**
- Appliances deliver higher throughput rates than those of the competition
- Hardware is praised in test reports
- The price/performance ratio of the appliances dominates the market

**Weaknesses**
- Virtualized appliances don’t deliver the same performance head-start which the special hardware appliances do
- No availability of licenses designed for cloud use and no automatic scaling
- Virtual appliances are bound to fixed virtual hardware levels
The providers in detail

Allot / Optenet

Allot has its headquarters in Israel. With the acquisition of the company Optenet, they added hardware-based web filters to their portfolio. Originally in the IP traffic steering business, Allot appliances only offer basic firewall functionality.

With its web security products, Allot offers a cloud service that is based on hardware appliances, not virtual resources.

Private Cloud

Allot products are aimed at both enterprises and providers as customers, and Allot appliances can also be used in this context to supplement and monitor the private cloud.

Public Cloud

The Allot web filter can also be offered by providers as public cloud service, but in the provider network it is based on the familiar hardware appliances.

Strengths

• In the enterprise segment the special hardware appliances supply high throughput rates
• As company listed on NASDAQ, Allot is a major firm in the cloud security market
• With its roots in routing it is already prepared for SDN and network function virtualization

Weaknesses

• No complete filter options for SSL/TLS traffic
• Because of the hardware appliances, scaling can only be done on hardware blocks
• Price/performance isn’t on the same level as the security cloud competition
Conclusion

In order to continually make good use of the Internet in the future, innovative protection of IT end user devices is a challenge that must be mastered. Already today the fear of blackmail and identity and data theft is inhibiting many businesses and the general public from using IT devices that offer Internet connectivity.

In the examination it is necessary to differentiate between two different types of products:

Cloud firewalls for securing cloud resources and services

Here one mostly finds virtualized appliances of the traditional appliance producers. To achieve virtualization here the existing operating system of the current firewall appliances is simply started on a hypervisor (such as VMware, Xen or KVM), thus replacing the real hardware with virtual hardware.

Cloud firewalls for securing large numbers of devices via the cloud

Right from the outset producers such as Zscaler and Secucloud designed their products for operation in cloud environments, so they can utilize advantages such as performance and elasticity perfectly for their needs, and are thus capable of addressing the mass market. As such the products are ideally suited to protecting a multitude of different devices (mobile devices, IoT) from the cloud.
if(is) Recommendations

if(is) recommendation for the consumer market

In our opinion, the kind of innovative protection that is required is supplied by Secucloud.

To be able to protect millions of users simultaneously in the most flexible way possible, the excellent elasticity of the Secucloud ECS² cloud firewall is a key function.

Special developments of business features such as SSL interception, deep packet inspection (DPI) and others make high-end features fit for widespread use. Taking SSL inspection as example, Secucloud offers a solution that uses targeted reputation and certificate checks to detect dangerous SSL traffic, without having to fully break it open.

With a scheme of payment according to resources used, it is possible for operators of the ECS² cloud firewall to offer a cost-efficient, flexible and future-oriented protection mechanism. Even without inherited systems and legacy systems the cloud firewall is capable of making a key contribution to the security of the Internet.

Since the subject of trust plays a special role in the choice of IT security solutions, the Secucloud ECS² cloud firewall from Germany retains a special advantage here, too.

if(is) recommendation for the MSSP market

Leading the field of traditional firewall producers are Palo Alto and Check Point, both in the virtual as well as in the appliance-based enterprise segment. Because of their proliferation and size, these producers have a reputation in the market that is virtually impossible for other producers to match.

Despite its roots in appliances, Check Point in particular, is seeing extremely strong development in cloud use. Wide distribution by Amazon Web Services (AWS) and Azur is facilitated by advanced integration in the infrastructure and automatisms of these public cloud providers.

With the Amazon Elastic Load Balancer, Check Point is virtually infinitely scalable within the resources of the AWS. If operated on their own cloud platform, however, this would not be possible.

As such, Check Point is the clear favorite in managed security service provider (MSSP) business. An established and renowned but also innovative enterprise solution, which however should be set up by a service provider.
if(is) Recommendations

*if(is) recommendation for the enterprise market*

Standing out as market leader in the cloud secure web gateway segment for business use is Zscaler. According to Gartner, the easy-set-up enterprise protection clearly dominates in this area, with more than half of the global market. Features such as full SSL interception, DLP and sandboxing are aimed narrowly at business customers, as such technologies are unusable in the consumer market.

Current services, such as optimum collaboration with Microsoft Office 365, are the reason why business customers should choose Zscaler with its holistic cloud concept.

With Zscaler’s cloud intelligence and sandboxing concept, even enterprise needs such as anti-ransomware are satisfied.

Because of the pure Zscaler cloud resource use, the price/performance ratio is better than with all the appliance-based firewall systems.

Prof. Dr. (TU NN) Norbert Pohlmann
Head of the Institute for Internet Security – if(is)
Neidenburger Str. 43
45897 Gelsenkirchen