Barracuda Web Application Firewall Qualification Questions

Why a Barracuda Web Application Firewall

The Barracuda CloudGen Web Application Firewall blocks application layer attacks directed at websites and API's that are published to the internet. Attacks blocked by the WAF include those recognized by the OWASP Top 10, application DDoS and automated bot attacks. Simultaneously, it provides superior protection against data leakage. Complementing its protective feature's you can benefit from strong authentication and access control capabilities and detailed logging for analytics.

How to spot an opportunity

- Looking to move their applications into Azure.
- Looking to host a website in Azure.
- They already have infrastructure in Azure and are looking to build new applications.
- They have a small number of applications in Azure but are reluctant to move their IT infrastructure over due to unfamiliarity/uncertainty of the cloud.
- A company that works in a high compliance industry (finance, government, healthcare, ecommerce).
- Customer inquiring how to ensure their applications in the public cloud are secure.
- Customer unsure if there are any current vulnerabilities within their environment.

Pains that they may be dealing with

- Want increased visibility of the traffic into their websites/ cloud infrastructure.
- Moving legacy applications that may not be compatible with cloud features.
- Cloud environment is outgrowing the ability to manage security with native tools.

Conversation starters - Web Application Firewalls

QUALIFYING QUESTIONS	EXTENDED TALK TRACK
Are you already protecting web-facing apps? How are you securing your network?	What type of solution organizations are using is a great question. How much time and energy is spent maintaining the rulesets, gathering logs, and ensuring the health of your cloud infrastructure?
What workloads are you moving to the cloud?	If you are moving any sites or services accessed over the web then you may want to consider how they can be secured.
How much IT resource do you spend today on protecting your cloud, and is it too much?	Today's organizations are lean – they simply don't have extra resources, despite how important security is. The less time you have to devote to managing these solutions, the better – so the solution needs to be easy-to-use, highly automated, and nearly invisible.
Are you aware that all WAF's are not equal?	Compared to some entry level WAF's the most secure WAFs are designed using something called a Reverse Proxy. In this design, the WAF receives the web browsing request and only sends the safe traffic onto the web servers. This is instantaneous (users don't see it).

QUALIFYING QUESTIONS	EXTENDED TALK TRACK
Doesn't Azure provide something to secure my web-facing apps?	Microsoft offers an optional Web Application Firewall or WAF in Azure. It is an extra cost, and it provides some basic web-facing application protections, but has limitations.
What doesn't the WAF in Azure do for me?	The challenge is that many websites need different levels of security on different pages. As the Azure WAF provides only one ruleset you will likely have to reduce security for some pages in order for others to function. Dedicated WAF's not only provide tools to detect these differences but allow you to customize in the right places.
Are there any specific functionalities you require?	For example maybe you have been using TMG to change the websites name between customers and your servers and need a replacement or you have lots of redirects to send traffic to different places. Maybe you need to authenticate your users in a different way.
Why is a Reverse Proxy the best way to go?	Reverse Proxies inspect data in BOTH directions – so not only does it prevent incoming attacks, it can prevent outgoing data leakage (either accidental or intentional). Much better than placing WAF software on the web server.
Would you be interested in a solution that's easy to use and highly effective?	The Barracuda WAF is the most popular 3rd party WAF in Azure for a reason – it performs well and it's highly cost-effective. We also have a program which can get your web applications under Barracuda WAF protection at even more competitive prices than you'll find on the Azure marketplace. Can we schedule a demo?

Reasons why they need Barracuda

- Top 10 Microsoft Global ISV partner in Azure
- First Microsoft certified partner in Azure
- Gold Certified partner
- Long history of supporting customers running in the cloud (i.e. shortly after Azure went live)
- Expert solution architects to assist with demo, design, POC & best practise
- Flexible pricing models – BYOL or PAYG

For Barracuda Solutions on Microsoft Azure

Please go to the Solutions pages on barracuda.com/programs/azure to look at the case solutions.

Common Web Application Firewall use cases *(plus required license)* on Microsoft Azure

OWASP Top 10+	Load Balancing	Advanced Bot Protection	DDoS	Malware + ATP
Protecting custom apps from SQL injection, cross-site scripting, web scraping, bot protection.	Load balancing with persistence for highly secure and scalable application infrastructure	Machine Learning protection service for bot attacks	Protects against application layer distributed denial-of-service (DDoS)	Protects against known and Zero Day threats
Included in BASE License	*Included in BASE License*	*Additional ABP License required*	*Additional DDoS License required*	*Additional ATP License required* *Must be on 2 core instance and upgraded license (Level 5)*

Product Choice

Sizes and product choice

Small (approx. > 100Mbps – 1 core)	Level 1 *(No malware possible)*
Medium (approx. > 200Mbps – 2 cores)	Level 5
Large (approx. > 400Mbps – 4 cores)	Level 10
X-Large (approx. > 800Mbps – 8 cores)	Level 15

Licenses

Base

Additional Licenses

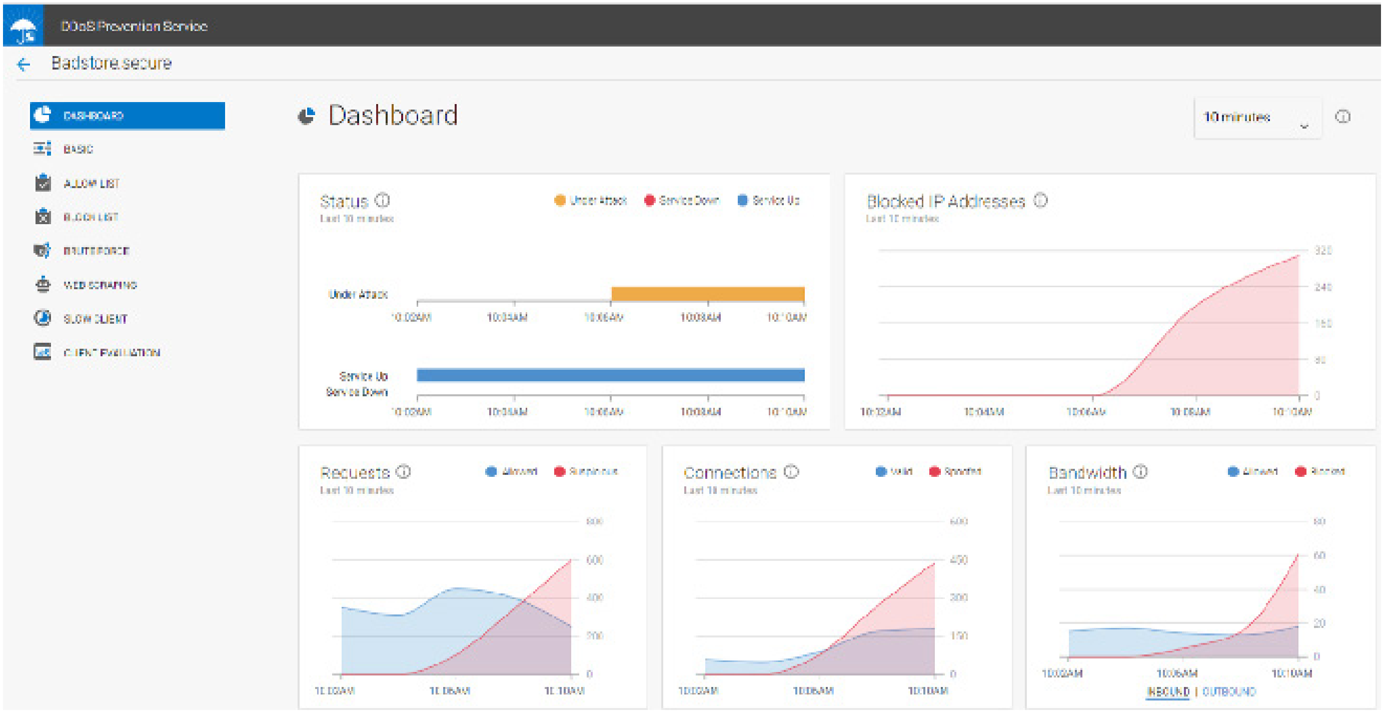
Advanced Threat Protection & Malware
DDoS (optional on all sizes)
Advanced Bot Protection (optional on all size)

Qualifying Questions Q&A - Security in the Cloud

QUALIFYING QUESTIONS	EXTENDED TALK TRACK
What kinds of web apps, website, or mobile apps do you provide?	Everybody's using the web – why not, it's easy and free. From web applications to website features to mobile apps, companies direct consumers and their own employees to the web. But there's risk, and many companies aren't aware of the significance, because hackers (except for ransomware) never announce themselves..
What types of information get entered using your web apps, website, or mobile apps?	If you're doing commerce on the web, you're collecting personally identifiable information or PII – and that's valuable to hackers. You might not think what you're collecting is valuable, but you're wrong. Did you know in the US, the National Parks System used to have reservation forms on its website that required just a name and phone number – it got hacked and sold to telemarketers.
Do you only provide content on your website?	That may preclude you from a data hack – but not from an attack. Your website can become the unwitting host of attacks due to something called SQL injection – code tricks to cheat your database into providing more data (and it's easy to do).
How are you using the cloud today?	Everybody's in the cloud in some manner – from just experimenting to leveraging providers like GoDaddy to setting up their own VMs in the cloud. It makes sense – the cloud is low-cost, highly reliable, and very low maintenance. (Microsoft script for converting hosted to cloud)
What are your future plans?	Most companies look to move websites (web applications) first – after all, if you already run your VM in a data center then it's not any harder to operate in a cloud – in this case, Azure. Most workloads can be moved without modifications and there are other benefits. (Microsoft script for converting hosted to cloud)
Are you aware of the benefits of the cloud?	For example, the flexibility of the cloud will allow you to start take advantage of the new serverless services to deliver your websites and mobile app services. These can provide reduced maintenance, quicker delivery times and potentially for a lower cost.

Qualifying Questions Q&A - Workloads in the cloud

QUALIFYING QUESTIONS	EXTENDED TALK TRACK
If you're currently using a hosting provider, how much do you know about their security?	Hosting companies may add web security on top of their hosting, sometimes inclusive, often for an additional monthly fee. But do you know how effective that is? How quickly can you recover from an attack, would they help you?
Do you know about the Microsoft Azure Shared Responsibility Model?	All cloud providers follow something called the Shared Responsibility Model. In it, Microsoft guarantees its cloud will be reliable and secure, but they don't guarantee YOUR security. In other words, they can't guarantee that your data won't be hacked or your web-facing sites attacked. This is because they don't control what you and your users do with the cloud.
Have you experienced a web attack?	Nearly ¾ of organizations have experienced some type of web attack. Many are minor – but worse, once a hacker has succeeded with a smaller successful attack, they will mount a more serious one using the same vulnerabilities. It's rarely an if but a when, especially if you gather any data.
How long do you think it would take you to identify and respond to an attack?	Organizations typically don't detect an attack until days, often weeks afterwards. If an attack is solely to siphon off data, it may not be noticed for months, as the attackers will want to remain low-key and siphon off as much data as possible. Obviously compliance regulations need to be considered.
Do you rely on logs and alerts to understand when attacks occur?	Both logs and alerts are invaluable, but you may not have access to them quickly enough to detect something in progress or to spot abnormal behavior. You could benefit from an alert when attacks reach a threshold.
What do you think will be the impact of an attack?	Aside from ransomware – which is typically delivered via email and results in an almost immediate lockdown and ransom payment, web attacks have other impacts like defacement of your web pages. They are hugely damaging to reputations and in many cases lead to regulatory fines as well.
Do you believe you are completely protected from attacks when running in Azure?	This is a common misconception. Azure only guarantees a secure network or infrastructure; they consider it the customer's responsibility to secure what they place in the cloud.
Do you know what the typical attacks that occur against web-facing applications (and mobile apps) are?	The following are all typical attacks: OWASP Top 10 (an annual list of the top malware attacks), SQL or software injections, DDoS (denial of service), and advanced persistent threats. The goal of each is to penetrate the web app and use it to gain access to data or your infrastructure.



Web Application Firewall product details

BWFICAZ001a	BARRACUDA CLOUDGEN WAF FOR MICROSOFT AZURE ACCOUNT LEVEL 1	0.00
BWFICAZ001a-v1	1 year license	5141.40
BWFICAZ001a-p1	1 year Premium Support (2,3,4)	1126.40
BWFICAZ001a-dd1	1 Year DDoS Prevention Service	1542.20

BWFICAZ005a	BARRACUDA CLOUDGEN WAF FOR MICROSOFT AZURE ACCOUNT LEVEL 5	0.00
BWFICAZ005a-v1	1 year license	6526.30
BWFICAZ005a-p1	1 year Premium Support (2,3,4)	1433.30
BWFICAZ005a-a1	1 Year Advanced Threat Protection	2638.90
BWFICAZ005a-dd1	1 Year DDoS Prevention Service	1958.00

Resources and success stories

Please go to the resources pages on barracuda.com/programs/azure/resources for more information.

For more information on the Barracuda WAF in Azure please go to barracuda.com/products/webapplicationfirewall/models/5

For a free scan for web application security flaws such as those on the OWASP Top 10, including SQL injection, cross-site scripting and others, please go to bvm.barracudanetworks.com

Barracuda®
Your journey, secured.