Frequently Asked Questions about Edgewise / ZWS

Marc Doughty - 2023-04-21 - Comments (0) - Servers and Services

Q. What can I expect on the day my service is ‘Edgewised’?

A. Hopefully nothing at all! The rules we are enabling are based on real-world activity of your service, as observed by the agents on the servers. Activity that has been happening while the policies are built is what is permitted by the policies.

Q. Do I need to work with ISG if I need to make changes to my service?

A. Possibly. Since Edgewise monitors activity to create rules, it’s likely that expanding to additional hosts, software upgrades, or additional integrations with other services will require us to modify the rules or temporarily suspend enforcement for re-evaluation.

Q. Does Edgewise monitor traffic?

A. No. Edgewise does not intercept traffic, it collects information about the nature of the ‘sockets’ opened by applications on servers. It sees ‘connections’ not ‘content’.

Q. Does Edgewise protect from malware?
A. Only tangentially. Edgewise uses hashes of binaries to determine their differences from each other. The hashes are compared to a database of known malware, and it can reduce the surface area that malware in the environment could attack laterally, but it should not be considered equivalent to an ‘anti-malware’ product.

Q. Can I use Edgewise to limit my service to a specific set of users or computers?

A. Not at this time. Edgewise is being deployed to ‘microsegment’ servers within the datacenter from each other.

Q. Will Edgewise slow my service down?

A. It should not. Edgewise permits or denies applications from creating connections, which is less resource intensive than inspecting traffic. It is normal for the agent to consume a small amount of CPU and memory, but impact should be on-par with other systems management agents.

Q. I’m trying to do something that used to work or something new but the connection is being denied even though there’s no firewalling. Is this Edgewise?

A. ISG and Systems Administrators in CIS should be able to determine if Edgewise blocked an activity if you provide the hostnames and time you experienced difficulty. Typically, we can tune the rules in just a few minutes. In more serious cases, we can put all policies into learning mode again, or suspend the agent on individual hosts.

Q. How do I get help if I suspect Edgewise is involved in an issue I am having?

A. Quick questions can be answered and adjustments made by contacting the Operations Center or ISG staff. Tickets in Deskpro are preferred for tracking more complex issues.

Q. What is the process for onboarding a new service?

A. The process is just like it’s always been. Because Edgewise is on the hosts that CIS provisions, you can build your service out normally. Once it is ready for use, we can start drawing perimeters and policies around it with Edgewise.