**Cisco Umbrella Secure Internet Gateway (SIG) Firewall Options to Protect Your Enterprise**

**Michael O'Connell:** Good afternoon. This is Michael O'Connell. I'm a Senior Security Architect with Aspire Technology Partners. In our last podcast, we talked about Umbrella SIG, which is Umbrella Secure Internet Gateway. Today, what we're going to focus on is Secure Internet Gateway firewall options, what are they and we're going to expand deeper into these firewall options and functionality.

**Michael O'Connell:** What is the difference between a switch, a router, a standard firewall, and a SIG gateway that we're referring to today? Well, very simple, the difference between these feature sets are a switch connects multiple computers or mobile devices together into a local network; a router connects separate networks allowing them to communicate and route between one another; a firewall, in the legacy traditional format, is a security device. It puts up a barrier between the local network and the public internet.

**Michael O'Connell:** In today's threat vectors in the world, you'll see everybody say, "Oh, I have this as a firewall. I have this is a firewall." Well, what SIG does, and the next generation, is to secure internet gateway firewall. What that is, is a cloud-delivered firewall. It gives you the visibility and control for traffic that originates from the request, no matter where they are. So, a branch office, remote locations, it allows me to get a single pane of glass to cloud-deliver policies and simplify management.

**Michael O'Connell:** Are there different types of firewalls? And, briefly, what are some of the things that each does? So, if you talk legacy, where you're looking years back and you're coming from a traditional standpoint, there was really five different types of firewalls. There are different names depending on who, what vendor you're speaking to. From an overview perspective, we'll go into this.

**Michael O'Connell:** The first was kind of a packet filtering firewall. What is that? It's an in-line, fast and efficient, to process the actual information packets. So, it enables complex security policies to filter through inexpensive minimal impact on your network. However, what it wasn't good at doing was securing configurations correctly. Lack features like user authentication logging.

**Michael O'Connell:** Then, you have what's known as a gateway firewall or circuit level, which sits on the edge of your network. That provides privacy for data passing in and out of your private network. So, anything going into your internet. So, that was really the edge ten plus years ago. That's how the firewalls came into play. So, that protected your organization from a circuit level. What it didn't do is, it didn't do any content filtering. I couldn't do anything with other firewall technologies.

**Michael O'Connell:** Then, we go into the application-level gateway, so the application level firewalls. So, what do they do? They simply are able to detect and block attacks not visible at the OSI model network. It protects user's anonymity so the public internet doesn't see who your internal users are. What can't they do? Well, they can affect network performance, very heavy processing overhead.

**Michael O'Connell:** Now, we start getting into what's known as the firewalls today. So, you have a stateful inspection firewall. A lot of times you look at like Legacy Cisco ASAs or other certain vendors, Layer 1 through 4 firewalls. And what do these do? They block types of attacks that exploit protocol vulnerabilities. They operate with fewer open ports. They reduce your corporate attack surface. They're capable of blocking [inaudible], types of denial service or DoS attacks. What is the disadvantage? A lot of skillset is required to securely configure these. They do not support all authentication connections. Can, honestly, be a lot of high processing overhead.

**Michael O'Connell:** And then, now, what we get into - that's been prevalent in the last five plus years - is the next-gen firewall, NGFW. And what does that do? Well, that gives me everything that I've spoken about, really, that so far the first four, traditional firewall functionality, adds the IDS/IPS - What's IDS? Intrusion Detection. What's IPS? Intrusion Prevention - and advanced threat malware scanning and other analytics. It gives me the full capability of monitoring network protocols from a datalink all the way to the application letter. So, you're talking Layer 2 to Layer 7 of an OSI model. And substantial logging capabilities to protect your organization. So, if you're looking at firepower or other devices, they're the next-gen firewalls.

**Michael O'Connell:** What's one thing that SIG and SIG firewalls offer that is an advantage also on top of that last layer, that next-gen firewall? Well, we can still do the Layer 2 through 7. The full IP port protocol and application locked down from a SIG Advantage or a SIG Essentials firewall. The difference between the two is, I can centrally manage.

**Michael O'Connell:** Essentially, I answered the question a little complex. It's five, but I'm going to go six/seven as the types and number of total firewall options. So, when you're thinking about today's firewalls and looking in it or discussing SIG, whether it's SIG Essentials or SIG Advantage's, what are some applications that come to mind today? And something that SIG Essentials or SIG cloud firewall, cloud-delivered firewall or CDFW, can deliver and protect your organization with?

**Michael O'Connell:** Well, if you're an organization that's starting to have a presence or already has a presence and an Azure, or an AWS, or a Google Cloud, or any Cloud infrastructure per se, SIG gives you the ability to very easily protect and give you cloud access security broker. So, on top of my standard two through seven files, I can protect my organization and see what's going in and out of those virtual infrastructures, aka cloud infrastructures. Something that's not on premises.

**Michael O'Connell:** When I'm looking at SIG, when you're talking about an application level, I give visibility not only to my corporate organization or my remote users per se, but I'm also a cloud-based architecture.

**Michael O'Connell:** Is there a particular prescription? Or what's the firewalls that we recommend to each individual organization? Well, every organization is going to be different. With COVID and the way the world has been affected, everyone knows the landscape has changed for the workplace. One thing that you want to look at is, is there a full office presence like there was two years ago or six months ago or what's the plan moving forward?

**Michael O'Connell:** If your business functionality and landscape has changed, one of the advantages of looking at a SIG Essentials or SIG Advantage packages, no matter where the organizations had it whether that's 20 branch offices, a hundred branch offices, maybe two offices, maybe no offices, you're going to have continual firewall protection.

**Michael O'Connell:** Now, if you are going back into an office and you have a full-on only office present, no VPN connection, then, yeah, a traditional next-gen firewall can handle all the applications you need. But with today's devices connecting from anywhere in the world, whether that's a Starbucks, traveling, any of the web traffic coming in and out, you want to look and try to diversify your organization, protect your company and your distributer locations and users no matter where they're at.

**Michael O'Connell:** The biggest thing is companies need to address security in a foursome, no matter where. That's where your go with SIG. What do I mean about that? Well, with SIG, whether it's a SIG Essentials or SIG Advantage, you're looking at two different versions of the firewall. So, I'll kind of go into detail there.

**Michael O'Connell:** SIG Essentials is the entry for the secure internet gateway cloud firewall. What does that give me? Well, that gives me full on web filtering. It gives me the full customization of creating blocks and allow lists. But what that also gives you is, it gives you a direct [inaudible] and other feed-based AV integration and Malware defense for your organization.

**Michael O'Connell:** When I start talking about firewall perspectives in a SIG Essential, I'm creating Layer 3, Layer 4 policies. I'm blocking specific IPs, ports, and protocols. What's the difference between the Essentials versions and the Advantage? The one that I'm going to recommend? Well, in the Advantage version, you're getting deep in protecting for outbound traffic using Application Layer 7 policies with an IPS built on.

**Michael O'Connell:** In both versions, you're going to get the standard firewall IPSec Tunnel termination, whether it's an IKEv2, IKEv1. If you want to build tunnels, you have full capability. The other additional add-on to this, you talk about a SIG Advantage and the prescription, that's kind of the full package. So, you get the DNS level protection, you get the remote agent protection, no matter where they're at. But you get the firewall Layers 2 through 7.

**Michael O'Connell:** What you get also is a data loss prevention in-line inspection. So, what does that mean? Anything that's web or cloud application traffic for sensitive data is going to prevent your organization from a loss with a SIG Advantage. A lot of those firewalls I spoke about earlier are not going to do DLP out of box and out of default. You may have had a separate product. With a look and exploration into the SIG options and your cloud-delivered firewall, you can manage that from anywhere in the world. You do not need to be in your corporate office.

**Michael O'Connell:** As an architect and an engineer from background and many, many years in this, it's very nice to be able to manage this no matter where I'm at very quickly. If I need to make a change, I can make a universal change very quick and deploy it to fix the security vulnerability or something in my organization.

**Michael O'Connell:** Are you using multiple vendors in your organization from a staffing perspective, from a management, in order to lockdown security policy sets and obtain a solution and a desired income to block and protect your organization? Do you have to log into three, four, five different vendors? Maybe one or two even. Are you using multiple different products to accomplish multiple different solutions? Would that be easier and more manageable to maintain under a single pane of glass? The other one is, do I got to log in? Do my engineers and do my team have to log into each site location?

**Michael O'Connell:** If I have a security vulnerability or something happens to my organization, does it take my team five, six steps to get everywhere protected? Or am I able to do it from the same single pane of glass? Can I build customizable policies very quick and deploy them globally? Are you using, maybe, a legacy layer early on, Layer 1 through 4 firewall? And are you using maybe a Layer 4 through 7 to do anything from a Layer 3, Layer 4 firewall log on activity to block devices to application visibility and control? Would you be interested in combining those layers together?

**Michael O'Connell:** Then, the final thing is, how about an advanced IDS and IPS feature set. Do you have one built in? Again, is that built on multiple vendors? Or are you using different things? And more importantly - and this is the last thing I'll mention - from scalability, do you have to go ahead and put out the actual assets to buy new hardware at each site moving forward?

**Michael O'Connell:** With the dynamic office changes, if things continue to change, would you like a dynamic scalable option with SIG and a cloud-delivered firewall where you have threat intelligence, you have your Layer 3 through 7 visibility and customizable from a single pane of glass?

**Michael O'Connell:** I've gone through a lot of different options and discussions in regards to SIG firewalls, and what are the different options of firewalls, and what are the different versions of your next-gen compared to SIG Essentials and SIG Advantage. If you're interested and if you want to have the conversation, that we absolutely would love to, I recommend contacting marketing@aspriretransforms.com. Once again, that's marketing@aspiretransforms.com. We would be happy to put you on one of our cyber security architects, including myself, to discuss your next-gen firewall options, discussing the SIG options in your organization.