**Benefits of Cisco Umbrella Secure Internet Gateway for Your Enterprise**

**Michael O'Connell:**  My name is Michael O'Connell. I'm from Aspire Technology Partners. My role here with Aspire is a Security Solutions Architect, and I have over 14 years of network and network security implementation experience.

**Michael O'Connell:** Today, we're talking about Umbrella SIG, also known as Cisco Umbrella Secure Internet Gateway. So, what is Secure Internet Gateway? Secure Internet Gateway is going to give your organization a higher level of protection from a single-source solution.

**Michael O'Connell:** Organizations are facing a difficult dilemma right now, growing telemetry and threat landscapes creating an ever-expanding attack surface, everybody being remote, COVID entered into everybody's daily life, organizations have changed the way that their workforce and landscape works. The average person may not be in the office full-time, five-days-a-week, 365 days out of the year anymore. There's a more hybrid landscape.

**Michael O'Connell:** With Umbrella SIG, you can cut complexity, reduce risk exposure, and improve network performance with a single cloud-delivered service that deploys easily and scales according with your business.

**Michael O'Connell:**  We talked a lot about the security posture for an organization. What benefits would Umbrella SIG and what is the security posture for an organization? So, with what I was mentioning before, with the hybrid workforce, there's, basically, a dark spot in the current workforce organization to see what's going on with your assets if they're not inside your corporate organization.

**Michael O'Connell:** From a security posture overview, the visibility that Umbrella and SIG, specifically, is going to give you is to protect internet access across your network devices. No matter if they're in a branch office, whether they're at a Starbucks, whether they're traveling, whether they're in your corporate office. Or they're what we consider roaming users, so if they are at home or they go from multiple different locations.

**Michael O'Connell:** Cisco Umbrella, specifically with SIG, is going to give you additional layer of security and allow you to protect your organization. That gives you the ability to block requests to malicious and unwanted destinations before that connection is even established. You're guaranteeing and protecting your corporate assets from malicious activity no matter their location.

**Michael O'Connell:** SIG kind of dives a little deeper into that. What SIG, Secure Internet Gateway, is going to give you is, it gives you advance secure web gateway full proxy functionality. That gives me the ability to content filter by category specific URLs. That gives me the ability to scan all uploaded and downloaded files for malware using Cisco Secure Endpoint, formerly known as Cisco AMP Engine, and third-party resources.

**Michael O'Connell:** That gives me a backend integration into Cisco threatgrid that will analyze my suspicious files, unlimited samples in your organization. It gives me the ability to block certain downloads of file types if I have a remote user that's not VPN'd into my organization. I'll be able to block an executable file from being pulled down and ran on that remote device. So, from a security posture overview, that gives me a single pane of glass protection no matter where they're at.

**Michael O'Connell:** Umbrella SIG can complement your existing organization's infrastructure in several ways. Number one, it can be added as an add-on specifically just for your remote user. So, if you're coming from a legacy firewall appliance, for example, maybe a Layer 1 to 4 appliance. It's not doing the Next Generation IDS/IPS functionalities. Maybe you don't have URL features. Maybe you're not able to see what is going on your remote users. Cisco Umbrella SIG can be implemented side-by-side with your existing architecture.

**Michael O'Connell:** There's a couple other use cases too. If you have a remote site, for example, maybe you have a device, maybe you have a device that's end-of-life, end-of-sale, it's been sitting out there, "You know what? I don't have any kind of next-gen protection at that." Cisco Umbrella with a round or tunnel to a cloud infrastructure can simply replace that end device firewall and I can manage everything from a pane of glass.

**Michael O'Connell:** So, there's different use cases for each individual organization. But Cisco Umbrella has multiple different options with SIG that you can go ahead and swap them out interchangeably. There's features, for example, in SIG Essentials as compared to SIG Advantage, different license levels that you can go ahead and get very deep.

**Michael O'Connell:** One thing that's changing in the security landscape, for example right now, everything's going to SSL decryption. Any site, for example, in a lot of legacy infrastructures, you don't see what's encrypted on an HTTPS site. You can't see what the user is doing in there. With Cisco's Umbrella SIG full proxy, I can do full or selective SSL decryptions to further protect the organization from hidden attacks and time-consuming infections.

**Michael O'Connell:** For a couple use cases for why Umbrella SIG would directly benefit your organization, so we had a deployment that I was engaged in, and what they needed to do was go PCI and PII compliant. With Cisco Umbrella SIG, you have Data Loss Prevention enabled. What does Data Loss Prevention or DLP do? It analyzes sensitive data in line to provide visibility and control over sensitive data leaving your organization.

**Michael O'Connell:** So, maybe I have an organization that we did. They have social security numbers. They had billing information. So, that's PII, that's Personal Identifiable Information. That needed to be stopped to make sure that that cannot leave the organization. That is not to be uploaded to Dropbox or third-party organizations. So, utilizing Umbrella SIG, we were able to stop that and protect the organizations and the employees from transferring data outside the corporate threshold.

**Michael O'Connell:** Another example is, I had a deployment where there was a use case for several branch offices. It was more of a grocery chain. And they had multiple different storage with end-of-life, end-of-support, Layer 1 through 4 firewalls. What were they were looking to do? Well, they were looking to streamline their employees and their IT staff investments. They want to make better use of their organizations time.

**Michael O'Connell:** So, what are they able to do? We were able to bring Umbrella SIG cloud-delivered firewall to their infrastructure. I helped them to deploy it, get it set up. Inside there, their IT staff was then able to make it very simple. The deployment is very simple. The management and reporting is all through a single pane of glass. The engineers, at that point, can simply deploy multiple customizable policies whether it's via IP, port, protocol, the application, or IPS all from a single pane of glass. I can push you to eight different remote sites at a simple click. I don't need to go back and log into each individual one, and go through and do the same process over and over every individual time.

**Michael O'Connell:** The nice thing about this also, is, with the Umbrella SIG cloud-delivered firewall options, you get full layers, seven application visibility and control to identify thousands of applications and block or allow them. Also baked in is Cisco's version of SNORT. The new SNORT 3 technology, which is their new version of the IDS/IPS signature-based detection agent is built into the Umbrella SIG platform. We were able to go ahead and simplify and reduce the IT overhead for that deployment specifically.

**Michael O'Connell:** So, one thing that I'm enthusiastic about this, and what I've heard back from customers after migrating to an Umbrella SIG is, number one, it gives me full visibility. I have the Telos Integration and SNORT 3, so I get a higher level detection. For example, my engineers and the company's engineers are asleep through the middle of the night, there is a malicious threat, bad actor on the other side of the globe. Telos is going to automatically update their cloud-delivered firewall. So, they're not going in there. Engineers aren't being woken up.

**Michael O'Connell:** But more importantly, you have the backend and appliance capacity to talking to that Cisco Telos threat intelligence. So, that's going to give you the ability to detect and block more threats dynamically without tying up your engineers and their hours. A lot of organizations do not have one engineer that's just going to sit in the firewall 24/7, 365.

**Michael O'Connell:** The biggest thing we hear back in the early adoptions from the Umbrella SIG immediately from an organization is, "Well, it streamlined everything. My engineers are freed up to do additional tasks. They're not just doing one job. I don't need one engineer just to be the firewall guru anymore. Now, I can have him or her do multiple tasks because the simplicity and reporting in Umbrella SIG are very easy to deploy."

**Michael O'Connell:** So, if you're interested in learning more and seeing a proof of concept, also proof of a value of Umbrella SIG, Aspire Technology Partners is a four-time Cisco master partner, we can directly work with you and build you out a POC environment. We can go to a full demo with you. We would simply contact marketing@aspiretransforms.com, and we can set you up immediately to schedule a POC. And I'd be more than happy to walk you through the integration and the overview of Umbrella SIG in your infrastructure.

**Michael O'Connell:** So, I'd like to thank you all for joining me today. Once again, my name is Michael O'Connell with Aspire Technology Partners. If you're interested in learning more about Umbrella SIG, please feel free to contact Aspire at marketing@aspiretransforms.com. Thank you very much.