Video - Fundamentals of ISE (5 min)

I remember my first security policy. So simple. Good stuff on, bad stuff off. Over the years, however, defining good and bad as gotten really difficult. So one policy quickly became two, then 10, then more and forget about just defining these policies, I need to enforce them as well. Now there's compliance and the need to prove I'm secure. On top of all that, everyone's bringing in his or her favorite Wi-Fi device and expecting full network access. Keeping up with this stuff takes time, people, and money, not to mention how I translate policy terms like location, users, devices, and applications into geek speak like IPs, MACs, ACLs, ports, and 802.1x. Enough! An answer for us.

The Cisco Identity Servers Engine or ISE is an identity-based policy platform that enables compliance, enhances security, and streamlines operations. Its unique architecture lets you gather real-time contextual information about users and devices to proactively enforce governance policy across the entire network infrastructure. When you think about it, how could all this be attempted otherwise? As the central policy component for Cisco's TrustSec Solution, ISE is the single source for policy definition, control, and reporting. So, you want to be on my network?

Let me show you the tool set. Triple A. Authentication, authorization, and accounting. Hey, what's your username and your password? Cool. Now let me give you access to just what you need and by the way, I'm logging this whole session just in case. Posture. Is this device clean? Carrying any suspicious applications or viruses? No? Profiler. You say you're a printer, but now you act like a web camera? I'm going to show you the door. Out! And now, guest management. Just need temporary access? No problem. You get just enough access, but when your time is up, it's up. And automatically. Nice thing for me, I don't even have to set you up as a guest. All that's handled by the person who wanted you to visit

Now many of you are saying to yourself right now, self, this sounds just like Cisco NAC and ACS. And you're right. That's where it starts. ISE combines the functionality of both, but with simpler deployment and common management. Moving forward, ISE will extend more deeply into the network, into the data center, and the application stack. The Cisco Identity Services Engine is the single source of truth for end points all across the network.

Now, there are really just two packages to understand here. The base package is all about authentication, ID, and guest services like what you find in Cisco ACS and NAC Guest Server. The advanced package adds profiling and posture services into the mix. A deeper more intelligent analysis of anything requesting access. NAC Appliance and Profiler, they'd be your reference points here. And anticipating your next logical question, no, this does not mean end of life for NAC or ACS. Every network is different. ICS is for those of us who want to consolidate policies in an 802.1x framework. If that's not you because say you want a choke point that's in line, or maybe you're just looking to authenticate a network device admins or something. Well, existing NAC or ACS products? They're going to be a better fit.

Now speaking of fit, you have three different hardware appliances to choose from, as well as a VMware-based and virtualized appliance. And because Cisco's shipping on the same hardware used by NAC and ACS today, there's a built-in level of investment protection. Always a good point to make to the bean counters, right? Now unlike other solutions, Cisco ISE has the ability to run specific functions at critical points in the network. For example, a pair of ISE appliances for administration, maintenance, and troubleshooting, and logging, and a high availability configuration. This could be located centrally, but with distributed appliances for making policy decisions as close to the user or device as possible communicating to your Cisco network infrastructure for enforcement. This is a really important design point to call out here. Cisco ISE works with your existing network devices, switches, wireless controllers, VPN concentrators, to balance the workload and keep enforcement as close to the end point as possible. If you have legacy gear in your network, no worries. ISE can make enforcement work with these as well. Now this example was a large network design simply to illustrate the flexibility available.

You can still get tremendous value from just two of these things. Redundancy, right? Start small, add capacity through additional appliances or extra licenses whenever needed. All right. Our assault on complexity continues now with a simple interface including things like a centralized dashboard with hotlinks to more details, flexible filtering of your active session, drag and drop re-ordering of rules, reusable objects. ISE uses state of the art widgets to make page-hopping and crazy scrolling a thing of the past. You're just going to love the clarity ISE provides here. Visibility into what just happened, when it happened, who or what was involved and how it was taken care of. We all know that complexity is the enemy of good security. This is why the ISE dashboard and the reporting tools, the live logs, are so robust and valuable.

So there you have it. Cisco Identity Services Engine. Single point of truth restoring visbility and control to the edge of your network. Enough already, huh? Why don't you check it out for yourself? For more information, visit cisco.com/go/ise.