Who In The World Are You?

Peter Silva, 2011-07-06

Steven Wright has said, '*It's a small world, but I wouldn't want to paint it.*' The world is getting smaller with today's 24/7 global marketplace. Businesses have offices and employees around the world to serve the needs of the organization's global customers. Those users, whether they are in a branch office, home office or mobile need access to critical information. Data like corporate information, customer information, sales information, financial information, product information and any other sources of business material is important to be able to make smart enterprise decisions. Without access to this data, poor decisions are made and the business can suffer.

The recent breaches, especially the intrusions tied to the RSA compromise, has put identity and access management in the spotlight. Once upon a time, users had to be in the office connected to the network to access corporate applications. IT organizations probably knew the user was since they were sitting at a desk; organizations knew the type of device since it was issued by IT and the business applications were delivered quickly and securely since it was from an internal local area network. Then, users needed access to that same information while they were away from the office and solutions like VPNs and Remote Access quickly gained acceptance. As adoption grew, so did requests for access above and beyond the normal employee. Soon partners, contractors, vendors and other 3rd party ecosystems were given access to corporate resources. Employees and partners from around the globe were connecting from a barrage of networks, carriers and devices. This can be very risky since IT might not know the identity of those users.

Anonymous networks allow users to gain access to systems via a User ID and password but they cannot decipher exactly who the user actually is; an employee, guest, contractor, partner and the like. Anonymous networks do have visibility at the IP or MAC address level but that information does not equate to a user's identity. Since these networks are unable to attribute IP to identity, the risk is that information may be available to users who are not authorized to see it. There is also no reporting as to what was accessed or where a specific user has navigated within a system. Unauthorized access to systems is a huge concern for companies, not only pertaining to the disclosure and loss of confidential company data but the potential risks to regulatory compliance and public criticism. It is important that only authenticated users gain admission and that they only access the resources they are authorized to see. Controlling and managing access to system resources must be based on identity. A user's identity, or their expressed or digitally represented identity can include identifiers like: what you say, what you know, where you are, what you share, who you know, your preferences, your choices, your reputation, your profession or any other combination that is unique to the user.

Access can mean different things - access to an intranet web application to search for materials, access to MS Exchange for email, access to virtualized Citrix, VMware or Remote Desktop deployments, access to a particular network segment for files and full domain network access as if the user is sitting in the office. The resources themselves can be in multiple locations, corporate headquarters, the data center, at a branch office, in the cloud or a mix of them all. When users are all over the world, globally distributed access across several data centers can help solve access and availability requirements. Organizations also need their application and access security solution in the strategic point of control, a centralized location at the intersection between the users and their resources to make those intelligent, contextual, identity based decisions on how to handle access requests.

Residing in this important strategic point of control within the network, the BIG-IP Access Policy Manager (APM) for BIG-IP Local Traffic Manager (LTM) along with BIG-IP Edge Gateway (EGW) provide the security, scalability and optimization that's required for unified global access to corporate resources for all types of deployment environments. The ability to converge and consolidate remote users, LAN access and wireless junctions on a single management interface and provide easy-to-manage access policies saves money and frees up valuable IT resources. F5's access solutions secures your infrastructure, creating a place within the network to provide security, scalability, optimization, flexibility, context, resource control, policy management, reporting and availability for all applications.

ps

Resources:

- The IP Address – Identity Disconnect
- Lost Your Balance? Drop The Load and Deliver!
- Identity Theft: Good News-Bad News Edition
- F5 Friday: Never Outsource Control
- Is OpenID too open?
- F5 Friday: Application Access Control - Code, Agent, or Proxy?
- Audio White Paper - Streamlining Oracle Web Application Access Control
- The Context-Aware Cloud
- Be Our Guest

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com