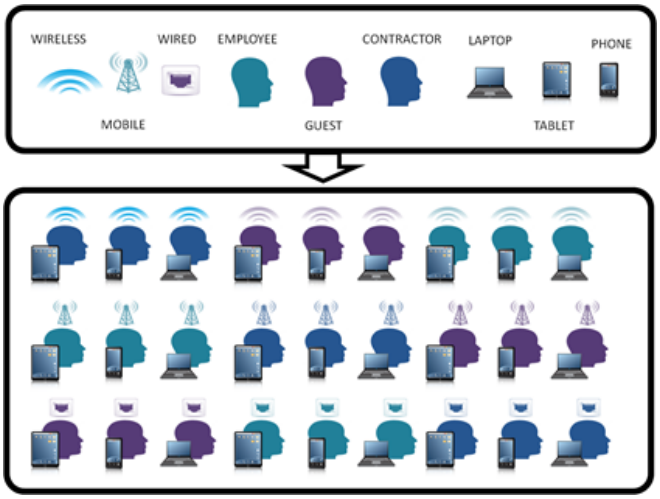
Complexity Drives Consolidation

Lori MacVittie, 2012-05-03

The growing complexity of managing more users from more places using more devices will drive consolidation efforts – but maybe not in the way you think.



Pop quiz time. Given three sets of three items each, how many possible combinations are there when choosing only one from each set? Ready? Go.

If you said "27" give yourself a cookie. If you said "too [bleep] many", give yourself two cookies because you recognize that at some point, the number of combinations is simply unmanageable and it really doesn't matter, it's too many no matter how you count it.

This is not some random exercise, unfortunately, designed to simply flex your mathematical mental powers. It's a serious question based on the need to manage an increasing number of variables to ensure secure access to corporate resources. There are currently (at least) three sets of three items that must be considered:

1. User (employee, guest, contractor)
2. Device (laptop, tablet, phone)
3. Network (wired, wireless, mobile)

Now, if you're defining corporate policy based on these variables, and most organizations have – or would like to have - such a level of granularity in their access policies, this is going to grow unwieldy very quickly.

These three sets of three quickly turn into 27 different policies.

Initially this may not look so bad, until you realize that these 27 policies need to, at least in some part, be replicated across multiple solutions in the data center. There's the remote access solution (VPN), access management (to control access to specific resources and application services), and network control.

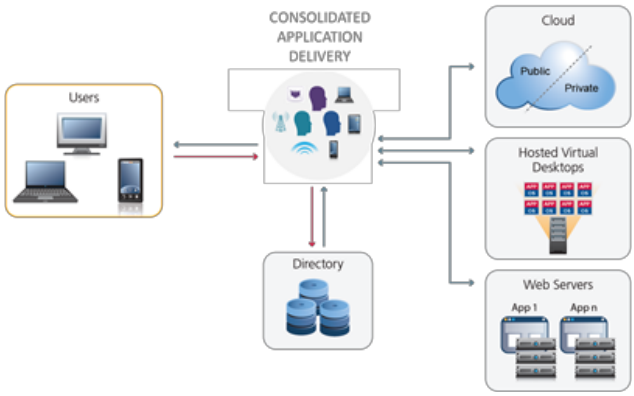
Complicating even further (if that was possible) the deployment of such policies is the possibility that multiple identity stores may be required, as well as the inclusion of mobile device management (MDM). On top of that, there may be a web application firewall (WAF) solution that might need user or network-specific policies that tighten (or loosen) security based on any one of those variables.

We've got not only the original 27 policies, but a variable number of configurations that must codify those policies across a variable number of solutions.

That's not scalable; not from a management perspective and certainly not from an operational perspective.

SCALING ACCESS MANAGEMENT

One solution lies in consolidation. Not necessarily through scaling up individual components as a means to reduce the solution footprint and thus scale back the operational impact, but by consolidating services into an operationally unified tier by taking advantage of a holistic platform approach to (remote) access management.



The application delivery tier is an increasingly key tier within the data center for enabling strategic control and flexibility over application delivery. This includes (secure) remote access and resource access management.

Consolidating access management and secure remote access onto a unified application delivery platform not only mitigates the problem of replicating partial policies across multiple solutions, but it brings to bear the inherent scalability of the underlying platform, which is designed specifically to scale services – whether application or authentication or access management. This means dependent services can scale on-demand along with the applications and resources they support.

A consolidated approach also adds value in its ability to preserve context across services, a key factor in effectively managing access for the volatile environment created by the introduction of multiple devices and connection media leveraged by users today. It is almost always the case in a highly available deployment that the first component to respond to a user request will be the application delivery controller, as these are tasked with high-availability and load balancing duties. When that request is passed on to the application or an access management service, pieces of the contextual puzzle are necessarily lost due because most protocols are not designed to carry such information forward. In cases where component-component integration is possible, this context can be maintained. But it is more often the case that such integration does not exist, or if it does, is not put to use.

Thus context is lost and decisions made downstream of the application delivery controller are made based on increasingly fewer variables, many of which are necessary to enforce corporate access policies today. By consolidating these services at the application delivery tier, context is preserved and leveraged, providing not only more complete policy enforcement but simpler policy deployment. This is why it is imperative for application delivery systems to support not just specific applications or protocols, but all applications and protocols. It is also the driving reason why support for heterogeneous virtualization and VDI platforms is so important; consolidation cannot occur if X-specific delivery solutions are required.

As the number of devices, users, and network medium continues to expand, it will put more pressure on all aspects of IT operations. That pressure can be alleviated by consolidating disparate but intimately related services into a unified application delivery tier and applying a more holistic, contextually aware solution that is not only ultimately more manageable and flexible, but more scalable as well.

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