

## Limiting what contractors can do on the network

Contractors definitely represent a unique security challenge. Unlike typical guests, who are there for just a short time and need only Internet access, contractors - especially long-term contractors - are much closer to employee status.

The problem, of course, is that they're not employees. So for regulatory reasons, or for just common sense reasons, you can't give them wide-open access to your entire enterprise network. Yet in nearly all cases, they have to be on your LAN to do their jobs.

In my industry, auditors are a great example - they need to access several financial systems, and they're on-site for as long as a month at a time. In hospitals, the service technicians that come in to work on the x-ray machines and other medical devices are a great example of this issue. Similarly, lots of companies have outsourced portions of their IT functions, such as managing blade servers. Very often, those third-party contractors end up at your facility for years, with a company business card, desk and email address.

But it's not appropriate for these workers to be able to access your company's source code or other intellectual property, your financial data (unless they're the auditors), or future product plans. Often, these workers move from company to company within the same industry, so their ability to relay information to a very interested competitor isn't hard to fathom.

To limit contractor access, I relied on the trusty network segmentation tools of virtual LANs (VLANs) and access control lists (ACLs) for years. But ultimately, the problems with this approach forced me to look for more automated tools.

First, the staff time needed to set up and maintain VLANs and ACLs just got out of hand. Any time there's a move, or a new contractor joins the group, IT needs to ensure these settings are up to date. Having the logical separation essentially hard-wired into the physical design adds a lot of complexity.

Second, some environments just can't use VLANs and ACLs. I have seen many environments with the use of shared PCs. They all need to see different applications and resources, and since they're accessing them from the same PC, port-based segmentation just wouldn't work there.

Third, and probably most alarming, people figure out ways around these security measures. Even if they don't steal their buddy's username and password, they know if they log in from that friend's desk, they can get to IM or the Internet or some other resource their own PC doesn't let them access.

So what's a more secure and more automated approach? I've found that role-based access control is the essential ingredient for keeping up with the challenging contractor access problem. You'll need the flexibility to apply role-based controls in a couple ways to fully address the range of contractor types.

For your long-term contractors, look for a system where you can add them to your Active Directory or other identity store and have a network device enforce access policies based on their group designation within AD. If the security device can learn the roles automatically, and control the traffic directly rather than relying on an outside device like a switch, your access control will stay dynamic. If a contractor leaves, and his/her name is taken out of AD, he/she won't be able to get on the network at all. If another contractor moves desks, you won't have to update any VLANs or ACLs to limit where on the LAN he can go.

For your short-term contractors, consider leveraging a captive portal to provide access to a generic set of resources that are similar across your business groups. This tool lets you quickly provide access without needing to update the identity store before the contractor can start working. That shared login will still enable you to control access - what applications can they run, what servers can they reach. But you won't have the granular, per-contractor control or tracking that the AD approach provides.

This approach has the added benefit of applying controls without the contractors being aware of it. If you needed to update VLANs and ACLs every time they moved desks, they could easily assume that the network changes you were hurrying to complete were in place because you simply didn't trust them.

As you look to implement controls for contractors, make sure the security platforms you're considering offer the ability to automatically learn users' roles, a captive portal option, and a self-contained approach to enforcing policy so you can get out of the VLAN/ACL update game.