



## Case Study: Linking Support Engineers with Customer Networks

As one of the largest network equipment vendors, Alcatel-Lucent's sales to global carriers often include service and support agreements. To provide such service, Alcatel-Lucent's teams of support engineers must access customer networks, and those customers want to be assured that their networks are being accessed with complete security. When it revamped its global support infrastructure in 2006, Alcatel-Lucent used NeoAccel's SSL VPN-Plus products to provide security while reducing costs and administrative overhead.

Prior to late 2006, Alcatel-Lucent maintained separate support organizations in various countries and global regions. It was up to local engineering teams to arrange for secure access to their customers, and there was no standard method of access among teams. This piecemeal approach led to unnecessary training and VPN client maintenance as well as widely varying security policies in use during customer network access.

In 2006, the company decided to streamline its support operations outside of North America, standardizing the method of access and enforcing one set of strict security guidelines for its engineers serving customers in Europe, the Middle East, Africa, and South America. With more than 100 engineers and customer networks located around the world, the right solution meant not only standardizing engineers' method of access, but also standardizing the location through which those networks were accessed. One of the first challenges was to simplify configuration and management.

"We didn't like having to distribute and configure VPN client software," said Atilla Akalin, team leader of Alcatel-Lucent's International Support Service Team. "We have dozens of engineers all over the world," he says, "and they're not always located in the same place or at the same machine. Our goal was to allow access from anywhere while making sure we met the customers' security requirements."

To simplify the process, Alcatel-Lucent planned to set up a secure "dial-in" room at its Istanbul, Turkey support facility. The room would house dozens of individual PCs, each of which would be connected to a specific customer network via an always-on terrestrial link. To gain access to a particular customer network, Alcatel-Lucent engineers would use a VPN connection to link to the dial-in room's network. Policies enforced through the VPN solution would then restrict access to specific customer PCs to only those engineers who were authorized.

On paper, the plan looked great, but other than the physical aspects of setting up the PCs, it hinged on finding the right remote access solution. The VPN solution had to:

- allow access from any remote PC
- support a wide range of connection speeds from T1 down to ISDN
- offer extremely high availability
- deliver granular access control so that each engineer's access could be limited to specific customer PCs
- offer clientless operation to reduce administrative overhead and complexity
- provide full endpoint security checks on client devices
- enforce centralized, identity-based policies

After reviewing IPsec-based VPN solutions from major vendors, Alcatel-Lucent selected NeoAccel's SSL VPN-Plus, and deployed the SGX-2400 appliance in the new dial-in room in early 2007.



“We selected NeoAccel SSL-VPN Plus because it enables secure and fast remote access without our having to distribute or configure clients,” says Akalin. “Since the secure tunnel can pass through firewalls and works from any network, this solution provided us an immediate and tangible productivity benefit by allowing our engineers to work anywhere.”

Using any standard web browser, support engineers can access the dial-in room from any PC on any network worldwide, and Alcatel-Lucent customers can be assured that the access is fully secure and restricted. “The SSL VPN-Plus access control policies allow us to restrict an engineer’s access to only the specific customer network PCs where he or she is authorized,” says Akalin.

Thanks to NeoAccel’s patented TCP connection handling technology, the user connections aren’t compromised by the use of SSL as they would be in other SSL VPN products. “Many of our engineers tell us that the performance and functionality they now get from remote locations looks and feels just like operating an application over the LAN,” says Akalin

To grant or change user access policies, Akalin’s team uses Microsoft Active Directory. Because SSL VPN-Plus integrates fully with Active Directory, network administrators must only add, change, or delete user records in one directory in one location, ensuring consistent security throughout the user base. “Our customers have granted us access to their networks in this way to facilitate support of Alcatel-Lucent equipment on their networks, but naturally they insist on the highest security,” says Akalin. “The SSL VPN-Plus solution gives us the global standardization, easy administration and granular access control that make this possible.”

Alcatel-Lucent has a global reputation for customer service plus a strong desire to maintain it while reducing costs and streamlining its operations. With NeoAccel’s SSL VPN-Plus, Alcatel-Lucent Turkey has streamlined the support that helps maintain that reputation.