Comments on SPUC IT Working Group's plan for South Pole Computer Security

You are correct to state that trying to ensure a consistent, secure software load on all machines at the pole is an impossible task. There will always be machines that are configured incorrectly or have particular combinations of software that introduce vulnerabilities. The goal should be to minimize the number of system disruptions caused by security breaches and to contain the effects of those that occur.

The major recommendation, that IPSec virtual private networks (VPNs) be established between the pole and CONUS is correct in spirit, but wrong in details.

IPSec VPNs work well for point to point encrypted links between sites that share a common administration. Because the links are set up permanently, the cryptographic keys need only be exchanged once. This can be easily be done manually. So multiple tunnels could be set up from institutions in CONUS to the pole, each being encrypted.

The end result, however, is much less secure than desired. This scheme makes south pole machines accessible on the local networks of the institutions in CONUS. Since these are usually university networks, they are probably not especially secure. This has just pushed the security problem from pole out to all of the participating institutions.

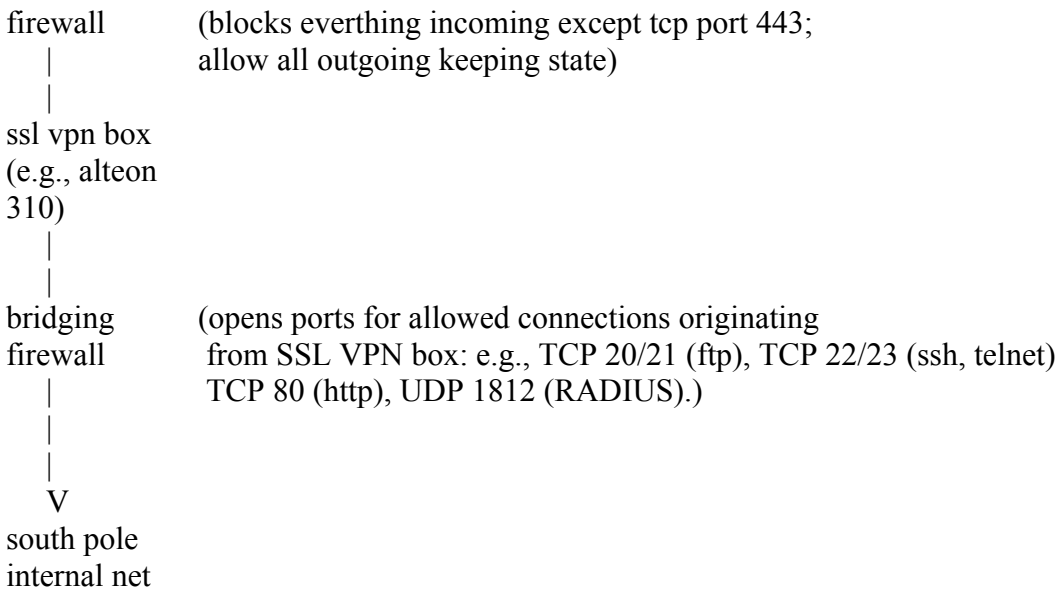
It is possible to configure IPSec VPNs so that they use authentication and encryption on a per-session basis. This seems to the goal of the SPUC IT WG recommendations. But these sorts of VPNs are a nightmare to configure. Who is delegated the responsibility for key management? A grantee institution? Raytheon? Who takes responsibility when a particular VPN client does not support the version of the key management protocol being used? IPSec itself is well standardized but the per-session authentication and key management are poorly defined, reflected in the morass of incompatible products available.

For the reasons mentioned in the last paragraph, most large commercial and government users do not use IPSec for their VPNs, but a simpler scheme called an SSL (Secure Sockets Layer) VPN. This uses the SSL security found in all web browsers to set up an encrypted link to an SSL VPN appliance. The VPN appliance does authentication, which can be password, RADIUS, LDAP, X.509 digital certificate, etc. It then presents a web page listing the services available to that user: FTP, ssh, telnet, etc. The user can immediately use any SSL aware application. Essentially any TCP based application can be tunneled through the SSL connection if browser supports Java applets.

The main advantage of this system is that every user already has an SSL client that is known to work: their web browser. It also allows per client customization

of available services (for instance, we may not want to give every user telnet or ssh privileges, but everyone can access read-only ftp directories to move data.) It also does something else important: authentication can be associated with users, not machines.

The architecture of this system:



This system will meet the goals for the pole network. Everything can be behind the firewall, blocking the vast majority of break-in attempts. The firewall and SSL VPN logs will provide information on the frequency and severity of break-in attempts. (At the moment, it appears that lack of information on the sophistication of attacks that the pole has faced has caused overreaction. Running all of the traffic through the firewall and regularly examining the logs will likely reveal that most attacks are simple-minded attempts to exploits obvious vulnerabilities). The "Demilitarized Zone" between the internal and external firewalls is also an obvious place to install an intrusion detection appliance, should that be desired.

Note also that the above system allows all outbound traffic; a stateful firewall permits replies to connections originated in the secure zone, but blocks all inbound connections not explicitly permitted. It doesn't affect outbound ftp, sending e-mail or web browsing.

There are additional changes that should probably be made to the south pole network. Bridging firewalls, which simply filter packets on an ethernet link, should be put between the administrative domains at the south pole. This means isolating the science network, Raytheon administrative network and government network. By doing simple sanity checks on packets in the local network, compromised

machines will not be able to infect the entire network. Additionally, each administrative domain (grantees, contractor and government) can craft policies that reflect the acceptable balance between security and ease-of-use.

Gregory Wright

Antiope Associates
18 Clay Street
Fair Haven, New Jersey 07704

(732) 345-0914
gwright@antiope.com