

# Multi-Site: Securing All the End Points

[PRINT](#)

November 19, 2007

By Matt Brunk

The multi-site deal for any dealer is alluring. What matters most is the level of detail that is taken to ensure that the care of all the customer assets isn't lacking. The success of using a newly built network hinged on the details and as my buddy often say's "the devil is in the details."

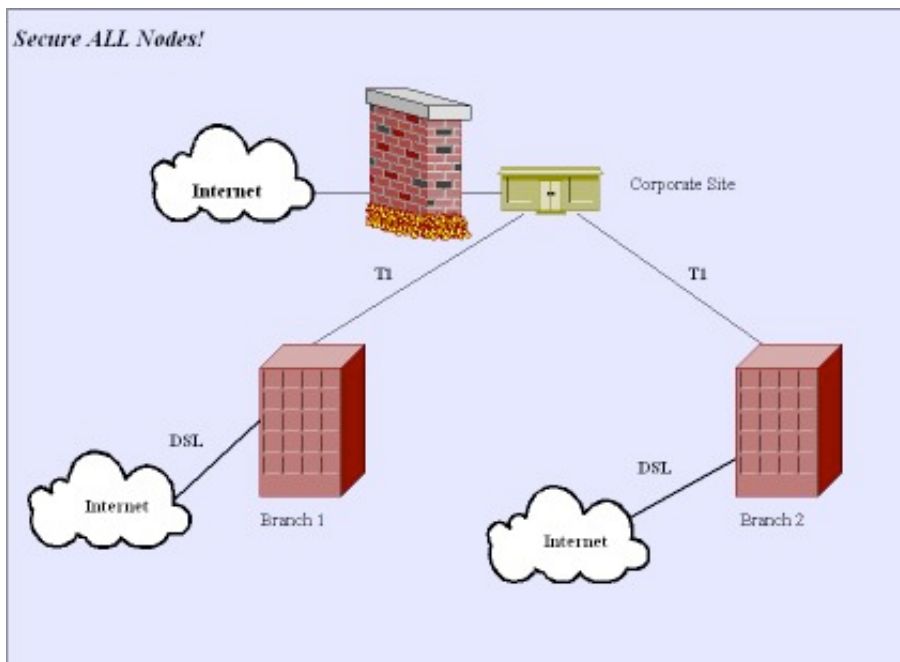


Not securing the end nodes invites unwanted traffic, compromises network integrity and potentially tests your patience.

Doesn't it makes sense to secure all nodes?

After having asked the router gods "did you secure the far end sites?" was the question dismissed. Perhaps they were having a bad day ruling their fiefdoms or maybe they just weren't paying attention.

The corporate site connects to each branch using a dedicated point-to-point T1. At each branch is another router connecting the T1 and a DSL used for backup. All Internet traffic is authenticated and routes through the corporate site, which also has a DSL used for backup routing and overflow in case the Internet T1 fails or becomes congested.



The corporate site firewall performs load balancing and overflow from the T1 to the DSL. The remote sites or branches while routed did have a hole by not being fire-walled. The threats entered via the backup DSL lines at the branch offices and would hammer the corporate site with malicious traffic. While corporate is still secure, the damage done could have been devastating for any number of reasons from weak intrusion protection to open ports or improperly programmed firewalls.

The malicious traffic showed up in the corporate site's firewall and yes, someone does read the logs- at least until we think we have everything nailed down. Without excuse, it does take a lot of time to review and act on customer logs. TMI (Too Much Information) plagues not just me. Two lessons are you still need to review the logs of the wares else you learn the hard way by burying your head in the sand which is to ignore

them. Then, be sure to secure ALL ends of the network. You don't need any malicious traffic traversing your multi-site network to test your security or your luck. Even if corporate is/was 100 percent secure, why would you want to invite this traffic on your network?

## Comment on this Article

[Click here to comment... \(Show/Hide Form\)](#)

## Other Visitors Comments

There are no comments currently....

**Close Window**