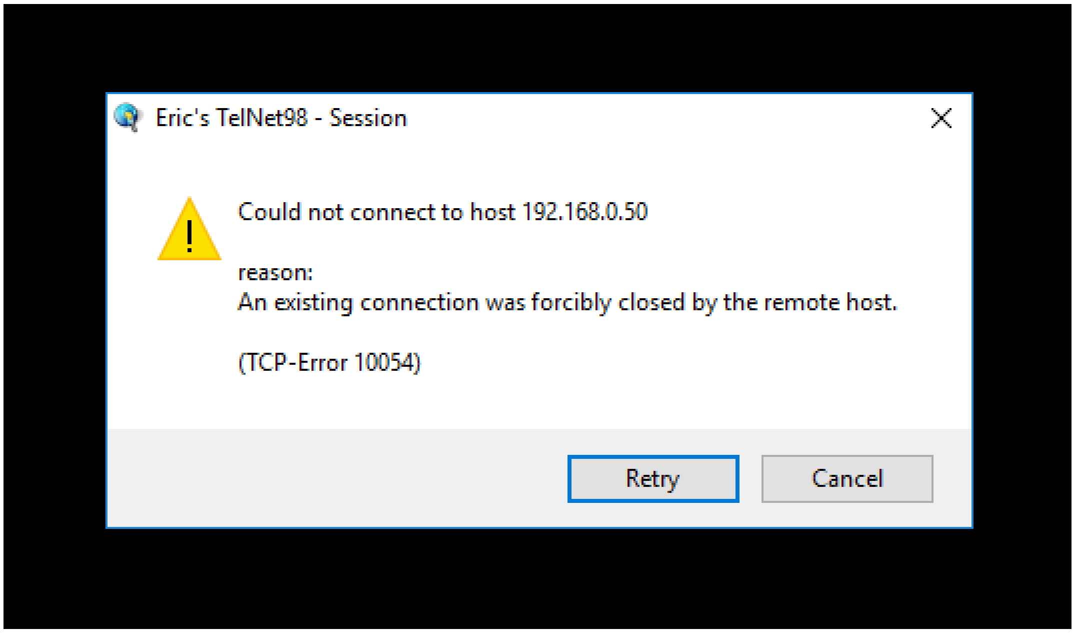
ONEIR SOLUTIONS

Giving Businesses A Competitive Edge™
Today and Tomorrow…

Technical Bulletin: Stop Unwanted Access into Your Oneir Solutions Server

A number of our valued Oneir Solutions customers still do NOT have adequate security for their Oneir Solutions server. There have been some recent examples that have come to the attention of our Customer Support team during the past week. One example is the error message shown below. This usually means that (since VMware is running) that the ssh daemon has been compromised or under stress. The attacks pretty much max out the number of ssh connections – when VMware is rebooted, it will allow a connection usually once and then not again.

This is one example where there hasn't been major damage to the server configuration or the company files with in Oneir Solutions.



Eric's TelNet98 - Session

Could not connect to host 192.168.0.50

reason:
An existing connection was forcibly closed by the remote host.

(TCP-Error 10054)

You need to ensure your security is locked down tightly...and not open to the wide world as was the case with these recent examples. Your Technical Support group needs to restrict access through your firewall/router so that only known computers, laptops and tablets can access the Oneir Solutions data. For Oneir Solutions to have access, we rely on you blocking out all other users at the router/entrance level to restrict ONLY to internal IP and should include our 2 static IP support addresses 204.10.243.52 and 72.38.179.194.

In the larger Oneir Solutions template we already have the security built in but the older ones do not – they rely on your Technical Support group blocking out all other users at the router/entrance level to restrict ONLY to internal IP.

If others are connecting directly to the Oneir server from the outside, you may consider making them part of the VPN so they are then part of the internal network.

This is a fairly serious problem if not addressed immediately. Hackers are not attacking any specific servers so do not take it personally. But if left to their devices, the hacker can create major catastrophic damage.

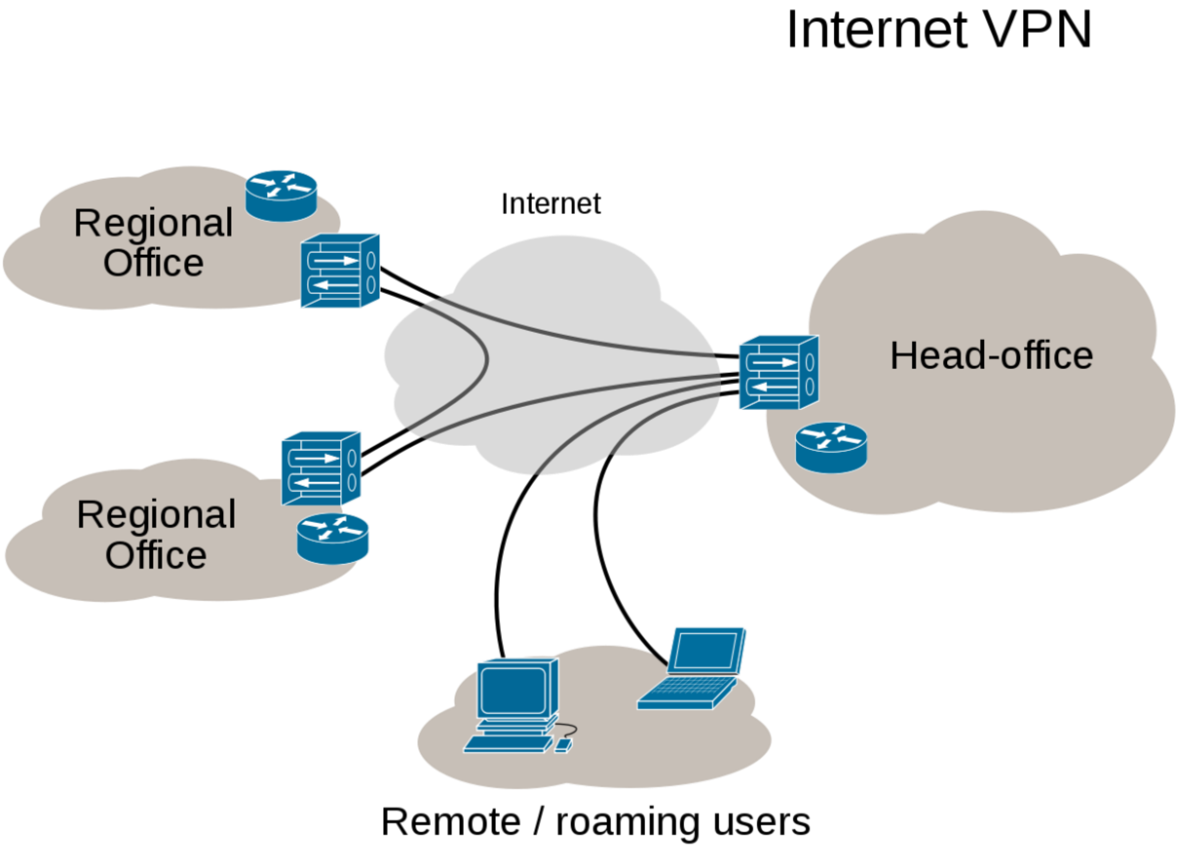
This brings up another issue; i.e. **Backing Up Your Company Data**. While your Technical Support Group is checking into your firewall protection, also have them verify that you have a backed up copy of the company data. Oneir Solutions provides a daily backup of your data every night. Please ensure that this data is being transferred to a secure area...preferably off site.

In computing, a **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Typically, your router can be configured to restrict access.   This is your first line of defense against intruders. So restrict access to only those external IP Address that you wish to allow access to your Oneir Solutions server. Setting up your router so that it is wide open is asking for easy intrusion into your server and its valued data.

Firewalls are often categorized as either *network firewalls* or *host-based firewalls*. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network.

A **virtual private network** (**VPN**) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network. Oneir Solutions access from your workstation desktops, laptops and tablets is expected to be set up on a VPN; either using a hardware appliance or software VPN.

Virtual Private Networks may allow employees to securely access a corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their wireless transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions.



A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains, so services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN). Designers have developed VPN variants, such as Virtual Private LAN Service (VPLS), and layer-2 tunneling protocols, to overcome this limitation.