Know Your Network

A New Administrator's Guide to Network Monitoring

Network Security

Your network is running fine, but is it secure?

Network Security is more than just making sure you have a good firewall installed on your network. No matter how secure you feel your network is, if you don't pay attention to what your employees are doing on and with the devices on your network, you may have a glaring hole in your security that could be exploited by someone with just a little knowledge of how to get in and cause damage.

The only 'completely safe' network is one that has no connection to the Internet and no modems anywhere on the network. The best you can do is make sure your major access points are secure as possible, and that the people that use your network are informed about the dangers of what is out there and what they can do to help.

Before you can put together a security strategy, you have to know about what the dangers are:

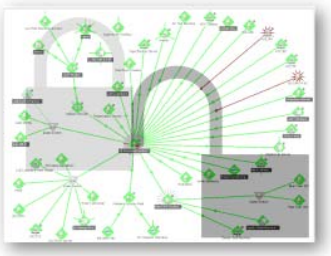
Denial of Service (DoS) - This sort of attack is where someone 'forces' commands on the server in such a quantity that the server can't keep up, ultimately locking it up.

Unauthorized Access - Password sharing, password hacking, someone forgetting to change their default passwords. There are many issues that would cause someone to gain access to your systems that shouldn't.

Destructive Attacks - When someone gains access to your network, they may have the ability to cause a lot of destruction. Data could be deleted, web sites could be changed, and viruses could be implanted.

Unauthorized Programs - Most administrators are very particular about what is running on their network. If someone is running an insecure server, a back door could be opened to the entire network.

Espionage - If you have sensitive data on your network, chances are there is someone out there who is trying to get it.



These are just a few of the problems that might be encountered. Fortunately, with the proper training, the proper tools, and the proper configuration, you can alleviate the potential for something devastating happening.

What to do

The following are a set of best practices that you can follow to reduce the risk of having an insecure network.

- Make sure data is where it should be.
- Publish security policies and procedures so that all employees can access them.
- Be certain that employees are oriented on the security policies.
- Keep virus definitions up to date on all of the computers on your network.
- Back up your data on a regular basis.
- Keep up to date on relevant security advisories.
- Make sure you know what is running on your network.
- Have personal firewalls enabled on all XP workstations.

The use of a network monitoring application such as WhatsUp Gold v11 can be a key part of your security procedures. While no software can handle every aspect of your network security, WhatsUp has some features that will help with several of the concerns you face while making sure your network is both operational and secure.

The following sections describe the features in WhatsUp Gold that you can use to make sure your network is as secure as possible.

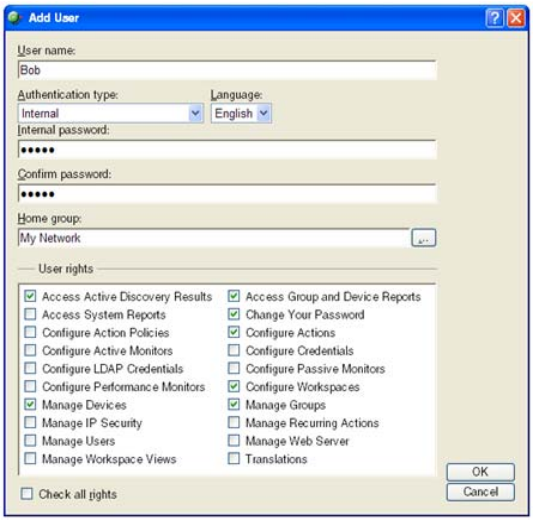
How WhatsUp Gold Can Help

Since the main job of WhatsUp Gold is that of network monitoring, your first task should be making sure that the devices on your network running your security protocols (firewalls, proxy servers, etc.) are set up on your device list. Once those devices are configured with the proper monitors and alerts, WhatsUp keeps track of their availability and performance.

Web Security

The WhatsUp Gold web interface is a direct look into your WhatsUp database. Therefore, it is important that you make sure whoever is logging in sees what they need to see and not things they do not. With the administrator login (which should be changed as soon as you install the application) you can create User Rights for specific users or classes of user that you create logins for. A class is simply a login that you distribute to people that don't have a named login of their own.

User rights can be set so that only specific people can make changes to your device configurations, add devices to your database, or even see specified device groups.



Through the web interface, you can select Configure > IP Security and only allow specific IP addresses to access your web interface, or block specific addresses.

Unauthorized Servers

As an unsecured server could open a back door into your network, you can set up Active Discovery to scan your network on a regular basis to see if specific types of servers are present. From the WhatsUp Console, go to Configure > Active Discovery, and create a scheduled entry with the Active Discovery wizard (click Add to begin.)

Once configured, you will be able to see if someone is running an FTP or HTTP server on their workstation. Use the Active Discovery Log report to view the results. It is a good idea to limit the use of this feature to perhaps once a day. Otherwise, it could slow down your network.

With this tool, you can also keep a daily track of which devices are running on your network. If one of these devices doesn't look familiar, you can track it down and see if it should be there.

SNMP Security

If you have SNMP (Simple Network Management Protocol) enabled devices on your network, it is very important that you change your community strings from the default 'public.' Once this is done, configure your SNMP credentials in WhatsUp Gold to get the most out of monitoring those devices.

Furthermore, your SNMP devices can be configured to send traps to WhatsUp Gold when someone tries to access the device with the wrong community string. You may not want to set this on all of your SNMP devices, but the most important of those could be set up so that you are alerted if someone tries to access it. The device generates an 'Authentication Failure' trap and sends that trap to your WhatsUp Gold machine.

More Information

For more information about how to use WhatsUp Gold, refer to the Getting Started Guide, and the application's online help. Both are great resources for configuration and solution information.

IPSWITCH WhatsUpGold