

# Blocking GoToMyPC.com Access with WatchGuard XTM

---

John M. Stengel, WCSP, WCT

5/7/2010

## **The Problem**

With businesses IT security growing companies are required to plug holes in their security infrastructure. Compliance and other regulations require auditing and logging of all activity. One major unmonitored area can be remote access to company resources. While this can be a productive way for employees to work it can lead to bigger issues.

Picture this, with remote access software you can transfer files back and forth between local and offsite workstations. These files brought into your company may contain Trojans, malware, or other threats. These files sent out of your company could be used against you or sold to a competitor. Employee and client sensitive data could be leaked and your company could still be liable for damages.

All information and activity logging while using remote access software may not be visible to IT administrators. Companies may have no way of tracking back what takes place during these remote sessions. This could leave companies vulnerable to risk and litigation.

It is the responsibility of companies to protect this information. The purpose of this document is to describe in detail how to prevent remote access to company computers using GoToMyPC.com with a WatchGuard firewall.

## **Why GoToMyPC.com**

Using a standard web blocking package such as WatchGuard's WebBlocker and Websense you have the ability to block access to Proxy sites. This will block access to sites such as logmein.com.

What makes GoToMyPC.com unique is that once installed it tries to go out various ports to make a connection. It doesn't connect to a typical URL rather to an IP address. The IP address it connects to can be one of any number they have built into the software. This makes controlling access by IP virtually impossible.

Additionally in our testing we observed that the agent tries to access the remote servers over a variety of ports such as 443 and 80. We were initially able to block the agent from working by adding a proxy to the SSL certificates passing through the channel. The issue with this was other valid sites also stopped working.

With a lot of testing and using the granularity of the WatchGuard Proxy policies we were successful in shutting this off. Not only are we able to stop it from working we can even send an alert that the user is attempting access to the software.

## **Environment**

To perform our testing we used a WatchGuard x750e running firmware 11.2.3. I do, however, think this will work in any version of Fireware.

In our environment we control access to outbound ports. We do not have an Outbound Any policy on our firewall so all outbound activity requires a rule. This is often referred to as Egress Filtering.

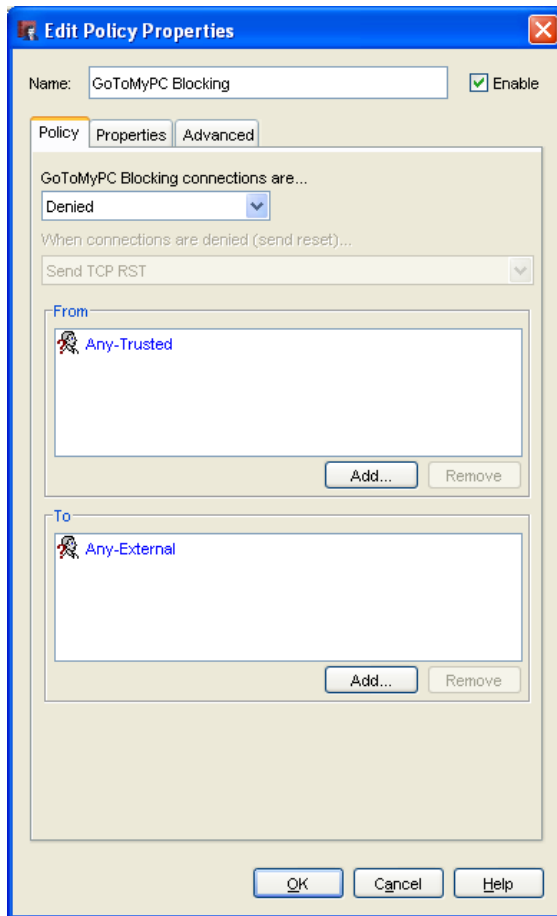
We use the WatchGuard WebBlocker, HTTP, and HTTPS proxies for web browsing.

## How to Stop GoToMyPC.com

The below steps are going to assume you are using HTTP and HTTPS Proxy Policies on your WatchGuard.

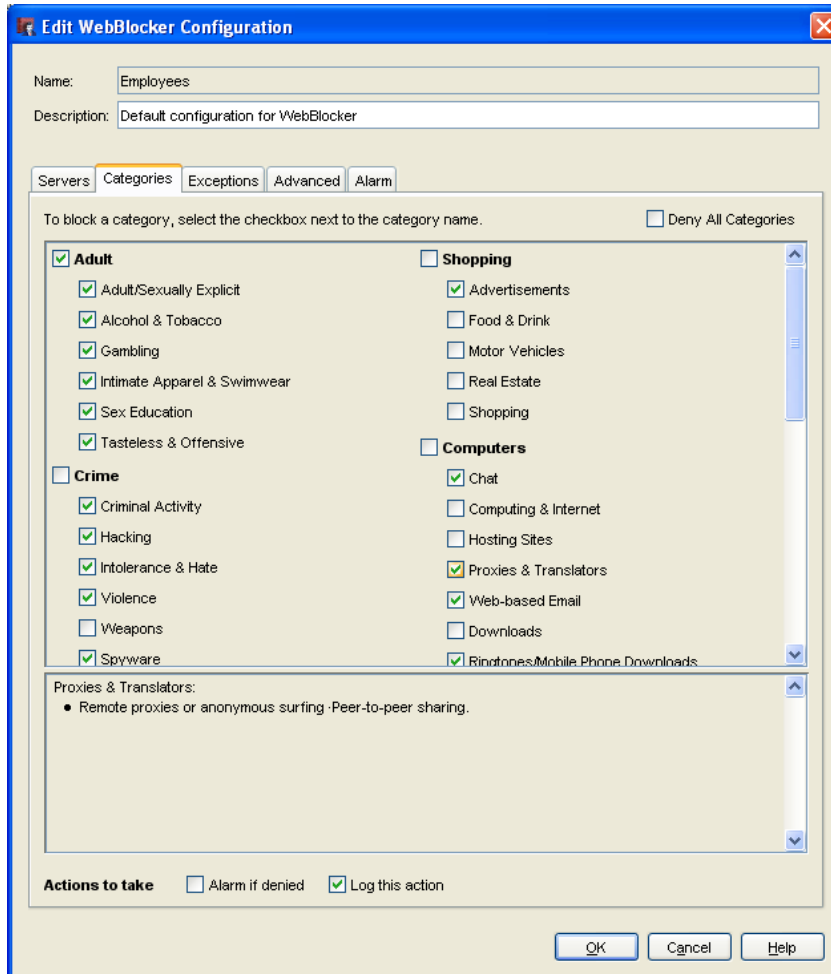
### Step 1 – Blocking Port 8200

- Create a new rule for TCP port 8200. The rule should be set to Denied, like below. This blocks access to the authorization request from the agent.



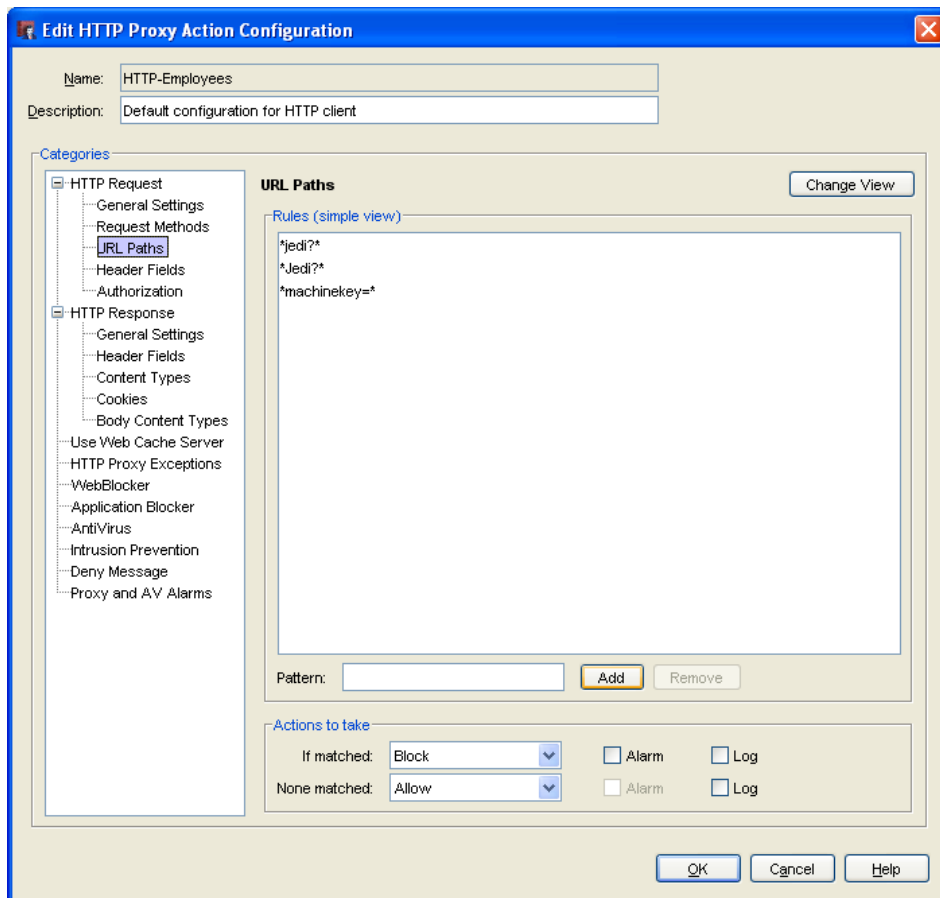
## Step 2 – WebBlocker

- If you have a license for WebBlocker it will add another level to your security. While you can still stop the agent without this, blocking access to the Proxies and Translators category will prevent them from even getting to the sites.



## Step 3 – HTTP Proxy

- This is the most important step. When the agent calls out to an IP address it has some behavior that we can monitor. First it calls a URL with the term **machinekey=** in the line. Next at the time of connection it calls a service with the phrase **jedi?** in the line. Using these two in the proxy policy we were able to block the traffic.
- In the screen shot below you will see that I added those terms to the URL Paths section under the HTTP Request portion of the policy. I added them as **\*jedi?\***, **\*Jedi?\***, and **\*machinekey=\***



- Now I set mine to block if they are accessed. Reason being is as an Administrator I want to know that my employees have the agent installed. What happens in this scenario is when the agent calls out they are added to my Blocked Sites list. They are then required to call the help desk for access to the internet. This alerts staff that the agent is installed and action can be taken by management.

## Wrap Up

Access to GoToMyPC.com is stopped. Nothing else is needed at the time of publication. The software may change overtime and we may need to adjust our logic.

## About the Author

John M Stengel is a WatchGuard Certified Trainer with JStengel Consulting ([www.jstengel.net](http://www.jstengel.net)). He works as a security consultant with companies in a variety of industries.

JStengel Consulting is a [WatchGuard](http://www.watchguard.com) Expert Partner and Certified Training Partner. Clients include retail, healthcare, schools, and government organizations.