Blocking Ultra Surf with NetSpective

Updated on 4/19/2012

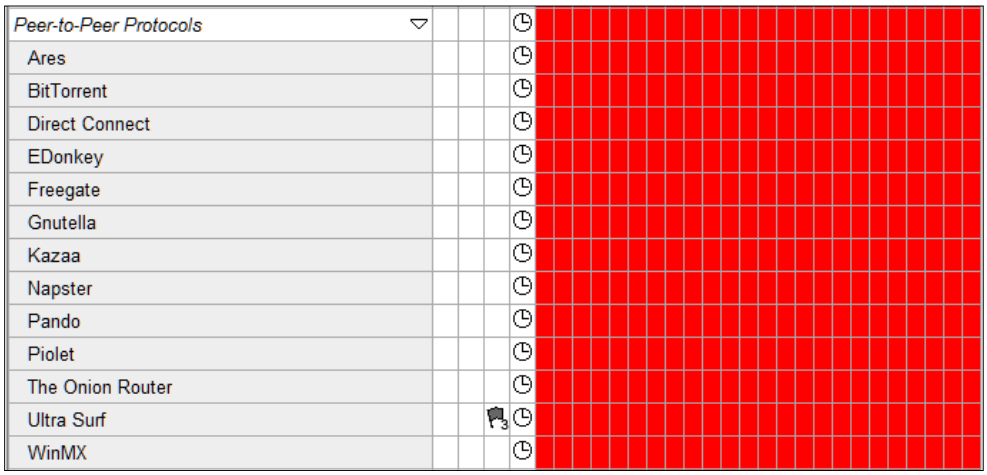
Ultra Surf recently made considerable changes within their product thereby making it harder to detect and block. In addition to the Ultra Surf activity on TCP, we have found that there are several servers using a new UDP-based protocol to international sites. Therefore, NetSpective's current TCP-based detection and blocking will need to be supplemented by firewall rules to block the new protocol going to certain international network zones.

The following is the recommended steps to effectively block the current release of Ultra Surf. All groups you wish to prevent Ultra Surf activity in should have these steps applied to them. Please be aware that a product like Ultra Surf is constantly changing since they are attempting to bypass web filtering applications.

1. **Configure NetSpective to block Ultra Surf's TCP-based traffic**

   From the Group Policy screen, under Peer-to-Peer Protocols, block Ultra Surf as category, indicated by the row next to it in red.

   Next we want to lock down the protocol. Click in the Flag field next to Ultra Surf to select Network Abuse Level 3. This will designate that Ultra Surf will be used for Network Abuse Detection.



2. **Configure NetSpective's Network Abuse Detection**

   We want to make sure that any user who tries to run Ultra Surf has their protocols shut down. In the Groups section, click on the group you want to prevent from using Ultra Surf. When presented with the Group Properties page, select the Abuse Settings tab. Under the Settings field choose "Level 3" and then check the Abuse Detection tab and adjust the settings to read the following:

   "If there are **5** Hits to 'Level 3' Categories in **1** minutes, lock down all **Activity** for **5** minutes.

This will prevent the workstation from being able to access the internet using any TCP-based protocol after we have detected the presence of Ultra Surf. As you get more experience with blocking Ultra Surf, you may choose to adjust the threshold hits, activity period, and lock down period to suit your needs.

3. Block UDP traffic to certain International Network Zones

The above steps will prevent TCP-based activity from the Ultra Surf client. However, Ultra Surf also uses a proprietary encrypted UDP-based protocol to proxy across certain servers. We have identified these servers to be in several zones, most of which are in Taiwan, that can be blocked at your firewall. Below is a list of network zones where UDP traffic should be blocked at your firewall:

Network Address	Network Mask
65.49.14.0	255.255.255.0
1.160.0.0	255.240.0.0
27.105.0.0	255.255.0.0
59.104.0.0	255.254.0.0
59.112.0.0	255.240.0.0
61.30.0.0	255.254.0.0
61.56.0.0	255.248.0.0
61.64.0.0	255.252.0.0
61.216.0.0	255.248.0.0
61.224.0.0	255.248.0.0
111.240.0.0	255.240.0.0
112.104.0.0	255.254.0.0
114.24.0.0	255.252.0.0
114.32.0.0	255.240.0.0
118.160.0.0	255.248.0.0
118.168.0.0	255.252.0.0
122.116.0.0	255.254.0.0
122.118.0.0	255.255.0.0
122.120.0.0	255.248.0.0
123.204.0.0	255.254.0.0
124.8.0.0	255.252.0.0

Network Address	Network Mask
124.12.0.0	255.255.0.0
124.218.0.0	255.255.0.0
124.219.0.0	255.255.128.0
125.224.0.0	255.248.0.0
125.232.0.0	255.254.0.0
175.96.0.0	255.252.0.0
175.180.0.0	255.252.0.0
203.64.0.0	255.248.0.0
203.72.0.0	255.252.0.0
210.58.0.0	255.254.0.0
210.60.0.0	255.252.0.0
210.64.0.0	255.248.0.0
211.72.0.0	255.248.0.0
218.160.0.0	255.240.0.0
218.187.0.0	255.255.0.0
219.80.0.0	255.254.0.0
219.84.0.0	255.252.0.0
219.91.0.0	255.255.128.0
220.128.0.0	255.240.0.0
221.169.0.0	255.255.0.0

We will continue to study the Ultra Surf protocol and will provide additional tech notes and software updates when needed. Please ask your support representative to be on the "*Ultra Surf Update List*".