Best Practice - How to Integrate External DNS Block Lists with the CloudGen Firewall

https://campus.barracuda.com/doc/32547/

The UI in Barracuda Firewall Admin provides the option of entering selected URLs into a list to be blocked at the time of resolving a domain into an Internet IP address. Usually, the list is fed by entries that are input manually. However, in certain situations, it is necessary to import lists that contain hundreds or even thousands of entries. This article describes how to integrate an external DNS block list with the CloudGen Firewall Caching DNS Service.

The integration leverages the same mechanism that can be accessed through the GUI at **DNS Interception > Intercepted Domains**.

This workaround will cause the Caching DNS Service to return NXDOMAIN instead of the official IP address assigned in the internal FQDN to the IP address translation table of the DNS system.

Prerequisites

It is recommended to create the block list file on a PC and transfer it to the firewall.

- You should be familiar with using file transfer tools like WinSCP for transferring files to the file system of your firewall.
- It is recommended to store a script in a dedicated directory, e.g., `/var/<mycompany>/scripts`, where <mycompany> must be replaced with your preferred name.
- You should be familiar with scheduling scripts. For more information, see How to Configure a Cronjob.

How to Integrate a DNS-Interception Block List into the Firewall

Integrating the DNS interception block list requires you to perform the following steps:

1. Create and transfer the DNS block list to your firewall.
2. Create the script file on your PC.
3. Copy the script file to your firewall.
4. Schedule the script file for execution.

Step 1. Create and Transfer the DNS Block List to Your Firewall

When creating a DNS block list, you must consider the following:

1. Use a raw text editor to create your DNS block list!
2. Do not save the block list in a file format like '.rtf' or any other non-raw file format!
3. Do not include any comments in the DNS block list! The comment lines in the following example are for illustration purposes only!

The following listing is an example of a DNS block list:

```
# Example of DNS block list
#
# head /root/small.dnsbl
0--foodwarez.da.ru
0-000.store
0-24bpautomentes.hu
0-29.com
0-lx.58411522.xyz
0.101tubeporn.com
0.code.cotsta.ru
000.abreubueno91.repl.co
000.gaysexe.free.fr
000.tf
```

Perform the following steps to get the block list into your firewall:

1. Create your DNS block list on a PC.
2. Save the block list under the filename `small.dnsbl`. Note: Do not use a different filename because the script below directly refers to this file name in the source code!
3. Transfer this block list file with your file transfer application to the firewall, and store the file under the path `/root/`. In the example below, the filename is `small.dnsbl` , and the full path name is `/root/dnsbl.small`.

Step 2. Create the Script File on Your PC

Perform the following steps:

1. Use a raw-text editor on your PC and create a new file.
2. Copy the content of the following script example into your editor.
3. Select a self-explanatory filename for your script, and append the file extension '.sh' to the file name, e.g., `activate_dns_blocklist.sh`. This file extension is necessary because the file is a script file and will be interpreted by the Linux shell interpreter.
4. Save the document.

```
#!/bin/bash

# Imports an existing DNS Blocklist into Barracuda CloudGen Firewall Caching DNS service

# Input file
DNSBL_FILE="/root/small.dnsbl"

ZONE_TEMPLATE="/opt/phion/modules/box/boxsrv/bdns/rpz.custom.zone.template"
TIMESTAMP_FILE="/tmp/dnsbl-zone.timestamp"
TMP_FILE="/tmp/dnsbl-zone.tmp"
CUSTOM_ZONE="/var/phion/run/bdns/rpz.custom.zone"


# Check if input file mtime has changed
check_file_changed() {
    local file_path="$1"
    # Check if timestamp file exists
    if [[ ! -f ${TIMESTAMP_FILE} ]]; then
        touch ${TIMESTAMP_FILE}         # Create timestamp file if it doesn't exist
    fi
    # Read previous timestamp
    local prev_timestamp=$(cat ${TIMESTAMP_FILE})
    # Get current timestamp
    local current_timestamp=$(stat -c %Y "$file_path")
    # Compare timestamps
    if [[ $current_timestamp -gt $prev_timestamp ]]; then
        return 0        # File has changed
    else
        return 1        # File hasn't changed
    fi
}


if check_file_changed ${DNSBL_FILE};
then
    echo "DNS Blocklist $DNSBL_FILE has changed"
    # Generate SOA record with current epoch time
    _UNIXSECS=$(date +%s)
    sed -e "s/<serial>/${_UNIXSECS}/" ${ZONE_TEMPLATE} > ${TMP_FILE}
    echo >> ${TMP_FILE}

    # Read hostnames from DNSBL_FILE and
    # convert to bind format
    while IFS= read -r line; do
        # Generate content line for each line in the file
        content_line="${line} CNAME ."
        echo $content_line
    done < "${DNSBL_FILE}" >> ${TMP_FILE}
    chattr -i ${CUSTOM_ZONE}
    mv ${TMP_FILE} ${CUSTOM_ZONE}
    chattr +i ${CUSTOM_ZONE}

    # Reload bdns
    /sbin/rndc reload

    # Update timestamp file
    echo "$(stat -c %Y ${DNSBL_FILE})" > ${TIMESTAMP_FILE}

else
    echo "DNS Blocklist $DNSBL_FILE has ** NOT ** changed. Exiting."
fi
```

Step 3. Copy the Script File to Your Firewall

It is recommended to host all user script files in a common directory of the file system of your firewall. Perform the following steps to create such a common directory:

1. Log into SSH on your firewall.
2. In the terminal window, go to `/var` by entering: `cd /var`
3. Create the common script directory and replace <myCompanyName> with the name of your company. To do so, enter: `mkdir ./<myCompanyName>`
4. On your PC, open the file transfer application and copy your script file to the directory `/var/<myCompanyName>/` . The full path of your script, based on the proposed script file name from above, is: `/var/<myCompanyName>/activate_dns_blocklist.sh` .
5. Go back to your firewall and check the presence of the transferred script file:
    1. Enter: `cd /var/<myCompanyName>` and replace <...> with your company name.
    2. Enter: `ls -la`

    ```
    [root@FW:/var/barracuda]# ls -la
    total 12
    drwxr-xr-x  2 root root 4096 Apr  5 07:23 .
    drwxr-xr-x 22 root root 4096 Apr  5 07:05 ..
    -rw-r--r--  1 root root 1854 Apr  5 07:08
    activate_dns_block_list.sh
    ```

6. Ensure that the file `activate_dns_block_list.sh` is present.
7. If the script is present, you must make it executable:
    1. Enter: `chmod +x ./activate_dns_block_list.sh`
    2. Enter: `ls -la`

3. The listing now displays the file as executable: `-rw xr--r--  1 root root 1854 Apr  5 07:08 activate_dns_block_list.sh`

Step 4. Schedule the Script File for Execution

The CloudGen Firewall provides multiple options to schedule a script for execution. You can schedule a script for daily, weekly, monthly, or yearly execution.

1. For more information, see How to Configure a Cronjob.
2. Perform all steps in the article, and at the location Step 1., sub-step 10, enter the full path name of your script: `/var/<myCompanyName>/activate_dns_blocklist.sh` .
3. Complete all subsequent steps.

Depending on your selection (daily, weekly, monthly, yearly), your firewall activates the DNS block list periodically, based on the content of your DNS block list at `/root/small.dnsbl` .