DNS Flood対策v10.1CMP対応版

ichiro, 2010-06-09

はじめに:
3年ほど前にDNS Flood対策として、DNSリクエストを制限するiRuleを紹介しました。1秒間であるIPアドレスから受信したDNSリクエスト数が制限値を超えた際、そのIPアドレスを「blacklist」に載せてしばらくの間そのIPアドレスからのDNSリクエストを廃棄するというルールでした。

当時、データ保存構造としてグローバル変数とArray変数しか存在しなかったため、タイムアウト方法や古いデータのクリーンアップをすべて「unset」コマンドを利用してルールの中で実施する必要がありました。

ではBIG-IP v10.1でCMPの時代においてはどのようなルールになるでしょうか。
CMPでは1台のBIG-IPの中に複数のTMMが動作し、グローバル変数が利用できない、複数のCMPを意識したプログラミングが必要、同じ動作を実現するのに難しいルールが必要になるなどの心配があるかもしれません。

しかし、実際にはその必要はありません。v10.1の「table」コマンドでは、優れた機能によってArray変数での実現が複雑だった動作が非常に簡単になり、以前のルールに比べて行数が半分ほどになります。

今回のルール紹介および分析で、皆様もぜひ「table」コマンドを使ってみましょう。

タイトル:DNS Flood対策v10.1CMP対応版

メリット:DNSリクエストを使ったDoS攻撃を防止します。

機能説明:
まず、以前のルールを見てみましょう。こちらにあります:
https://www.f5networks.co.jp/primemembers/irule/0709.html

以前のルールでは2つのArray変数を使いました。1つは1秒間の間に受信したリクエスト数を数えるカウンターとして使い、もうひとつは実際にブロックするIPアドレスを記録するblacklistです。

また、Array変数は時間を意識しない単純なテーブルデータ構造ですので、どちらのArrayも古いデータを削除するための処理をiRuleの中に記述しなければなりませんでした。そのため、当時のルールの中に現在時刻とArray変数で保存しておいたTimestampを引き算したり([expr {$currtime - $::blacklist($srcip)}])、比較したり($currtime ne $y)していました。

それに対して、v10.1においての「table」コマンドでは、時間を意識したロジックが非常にシンプルになりました。

tableコマンドのtimestamp機能についての説明は、下記のリンクを参照してください:
http://devcentral.f5.com/Default.aspx?tabid=63&articleType=ArticleView&articleId=2378
http://devcentral.f5.com/Default.aspx?tabid=63&articleType=ArticleView&articleId=2379

今回、DNS Flood対策v10.1 CMP対応版では、上記リンクに記述されているlifetimeとcreate timestampの機能を使うことによって、TMMが古いデータの削除を実施するため、わざわざiRuleの中で削除したり、現在時刻とtimestampを比較する処理の記述の必要がなくなりました。

このルールの動作では、DNSリクエストが到達した際(CLIENT_DATA)、blacklistに載っているかをチェックします。(載っていればdropしてルール処理を終了)

次に、DNSリクエストを送信したIPアドレスと現在時刻を使ってKeyを作成し、そのKeyでtableの中にリクエスト回数を記録します。(同時にkeyのlifetimeを2秒に設定します)

最後に、tableに記録されているリクエスト回数がmaxqueryを超えているかをチェックします。超えている場合、そのIPアドレスを別のkeyとして利用しblacklistのsubtableにエントリを記録します。また、blacklistエントリーのlifetimeをholdtimeに設定します。その後、必要なくなったIPアドレスと現在時刻で構造したkeyを利用したエントリーを削除します。

上記以外のtableおよびblacklist subtableのデータクリーンアップはlifetime機能でTMMが実施します。これでiRuleの行数を半分に減らすことができます。

tableコマンドは非常に便利なものですので、使い方を覚えておくと今後のiRule作成にとても役立ちます。

設定概要：
staticであるグローバル変数を設定します（RULE_INITで実施）：
static::maxqueryは2秒間での最大DNSリクエスト数。超えた場合はクライアントIPアドレスをblacklistに蓄積。
static::holdtimeはblacklistに載っているエントリーのlifetime。blacklistに記録してから設定した秒数を過ぎると、TMMがエントリを削除します。

【iRule定義】

```
when RULE_INIT {
   set static::maxquery 100
   set static::holdtime 600
}
when CLIENT_DATA {
   set srcip [IP::remote_addr]
   if { [table lookup -subtable "blacklist" $srcip] != "" } {
      drop
      return
   }
   set curtime [clock second]
   set key "count:$srcip:$curtime"
   set count [table incr $key]
   table lifetime $key 2
   if { $count > $static::maxquery } {
      table add -subtable "blacklist" $srcip "blocked" indef $static::holdtime
      table delete $key
      drop
      return
   }
}
```

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113