Netscreen Firewall DDoS Ayarları

Netscreen Firewall DDoS'dan Korunma Özellikleri

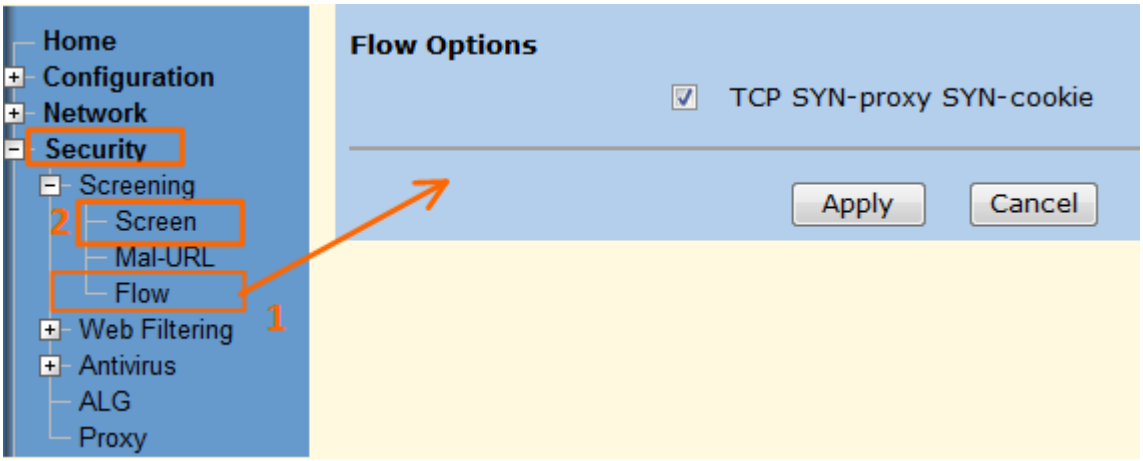
Erhan YÜKSEL <eyuksel@bga.com.tr>

11/22/2010

[Bu yazı Netscreen Firewall üzerinde DDoS saldırılarına karşı alınabilecek önlemleri anlatmaktadır.]

Netscreen Firewall 'da ddos protection - screen değerlerinin ayarlanması :

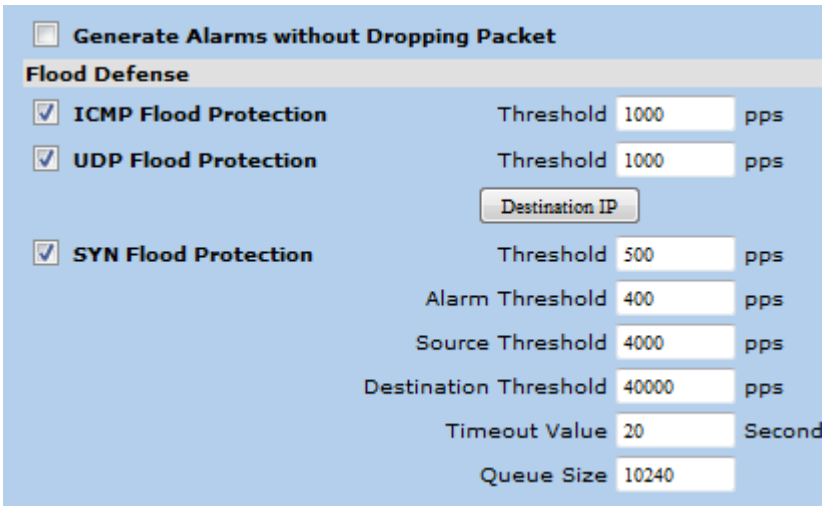
Netscreen de SYN-Proxy ve SYN-cookie de yapacağımız ayarlamaların aktif olması için öncelikle aşağıdaki menüden SYN-Proxy SYN-cookie korumasını aktifleştiememiz gerekir . Aksi halde SYN protection ile ilgili yapılacak ayarlamaların etkisi olmayacaktır.



2- "Flow Option" aktif edildikten sonra Screen menüsündeki seçenekler trafiğimize göre uygun hale getirmeliyiz. Trafiğimize uygun hale getirebilmemiz için trafiğimizi tanımamız gerekir. Yani normal şartlar altında tek bir source tan açılabilecek session sayısı , anlık icmp trafiği , anlık yeni tcp oturumu açma isteği sayısı gibi.

Netscreen firewalllarda ddos ayarları "zone" bazlı yapılır . UDP flood haricinde, korumaya alacağımız ip adreslerini belirtemeyiz. TCP SYN-Proxy SYN-cookie aktifleştirme işlemi tüm zone'lar için geçerlidir.

2. adımdaki screen değerleri ise zone bazlı yapılır.



Zone protection uyguladığımız zone'a gelecek olan paket değerlerini belirleriz . Uyguladığımız değerler zone'dan çıkan değerler için geçerli olmaz . Yani trust zone'a ayarları aktifleştirmeden

sadece untrust zone ‘da ayarlama yaparsak , trust’dan untrust’a giden paketler için herhangi bir koruma sağlanmaz.

Generate Alarms without Dropping Packet : Engelleme yapmadan sadece uyarı vermesi sağlanır.

Udp flood protection : Bir veya birden fazla kaynaktan bir hedefe giden udp paketi sayısını kısıtlar.

Destination IP butonu ile korunması istenen sunucların ip adresleri girilebilir.

İcmp flood protection : Bir saniyede gelebilecek icmp paket sayısıdır . Bu değer aşıldığında o saniye için gelen paketler firewall tarafindan bloklanır .

Bir sonraki saniyede deger sıfırlanır. Default değeri 1000 dir, default değerlerde iken birinci sn de 1200 icmp echo request gelmesi durumunda 200’ü blokalanır ikinci sn de 1400 icmp echo request gelmesi durumunda 400’ü blokalnır , üçüncü sn de 900 icmp echo request gelmesi durumunda ise bloklama olmaz . **Bu işleyiş diğer koruma mekanizmaları (SYN , UDP protection) için de geçerlidir** .

Firewall da icmp paketleri engellenmişse buradaki değerin bir önemi yoktur.

SYN Flood Protection :

Threshold : syn-proxy yi aktif etmek icin gelmesi gereken half-open bağlantı isteği (syn bayrağı set edilmiş tcp paketi) sayısıdır. (Yani üçlü el sıkışmayı tamamlamayan bağlantı isteği sayısı) .

Bu değer tüm istemcilerden gelen syn sayısı degeridir. Yani tek bir kaynak için belirlenen değer değildir. Bu değere ulaşana kadar gelen SYN paketler ile ilgili herhangi bir işlem yapılmaz , Netscreen tarafından korunan sunuculara doğrudan iletilir. Firewall ve sunucuda session açılmış olur.

Bu değerin düşük tutulmasi normal bağlantı yapmak isteyen kullanıcıların bağlantılarına zarar vermez sadece firewall'un syn-proxy olarak calismasina sebep olur. Netscaler gibi waf cihazlarında bu değer default 0 dır ve iptal edilemez, yani syn-proxy ilk syn den itibaren aktiftir. Bu değerin “0”(sıfır) olmasının iki temel etkisi vardır:

1- Üçlü el sıkışmayı tamamlamayan port scan taramalarında tüm portlar açık görünür.
2- Syn -proxy işleminde firewall göndermiş olduğu SYN+ACK paketlerindeki sequence number 'ları matematiksel bir işlem sonucu ürettiğinden işlemci yükü getirir . Bu değerin yüksek tutulması , firewall ve sunucunun session tablosunun dolmasına ve sunucunun performansının düşmesine sebep olabilir.

Alarm Threshold : Event bölümüne log düşmesi için gelmesi gereken SYN paketi sayısıdır.

Log düşmesi için threshold + Alarm Threshold değeri kadar syn paketi gelmeli. Yukaridaki değerlere göre event log düşebilmesi için saniyede 900 syn gelmesi gerekir.

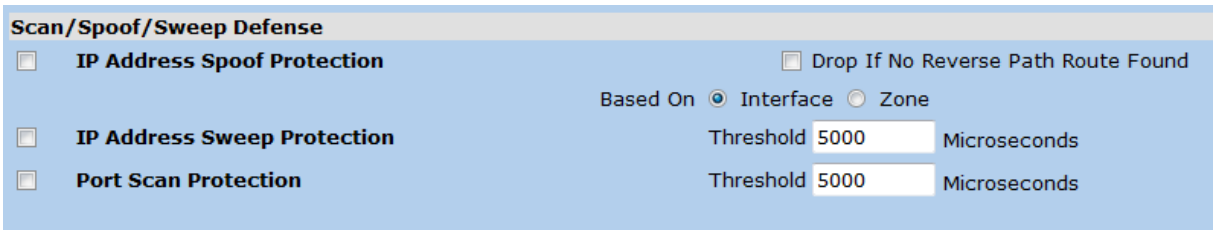
Source Threshold : Bir kaynak ip’den gelen herhangi bir hedef ip’nin herhangi bir portuna gelebilecek bir saniyedeki syn paketi sayısı . Bu değerin üstüne çıkılması durumunda istekler legal dahi olsa firewall tarafından engellenir.

Bu değer bir saniyedeki yeni baglantı isteği sayısını gösterir. İstemcilerden en fazla bağlantı isteğinde bulunanlar tespit edilmeli ve optimum değer buna göre belirlenmelidir . Yüksek tutulması durumunda saldırı anında "Queue size"ın dolmasına ve diğer bağlantıların kesilmesine sebep olabilir. Değeri yüksek tutularak synflood uyarısı geldiği anda düşürülebilir, fakat mesai dışındaki saldırılarda aksaklık yaşanabilir.

Timeout Value : tamamlanmamis oturum isteğinin kuyrukta bekleme suresidir. Bu surenin bitiminde session kapatılır , cevabi bu sureye kadar geciktiren legal isteklerin cevaplari da kabul edilmez. Max 50 sn olarak ayarlanabilir.

Normal durumlarda 20 sn Legal baglantilarin kurulabilmesi için fazlasıyla yeterli bir süredir. saldırı anında 3 'e kadar düşürülebilir. Normal şartlarda 3 sn syn+ack için uzun bir süredir.

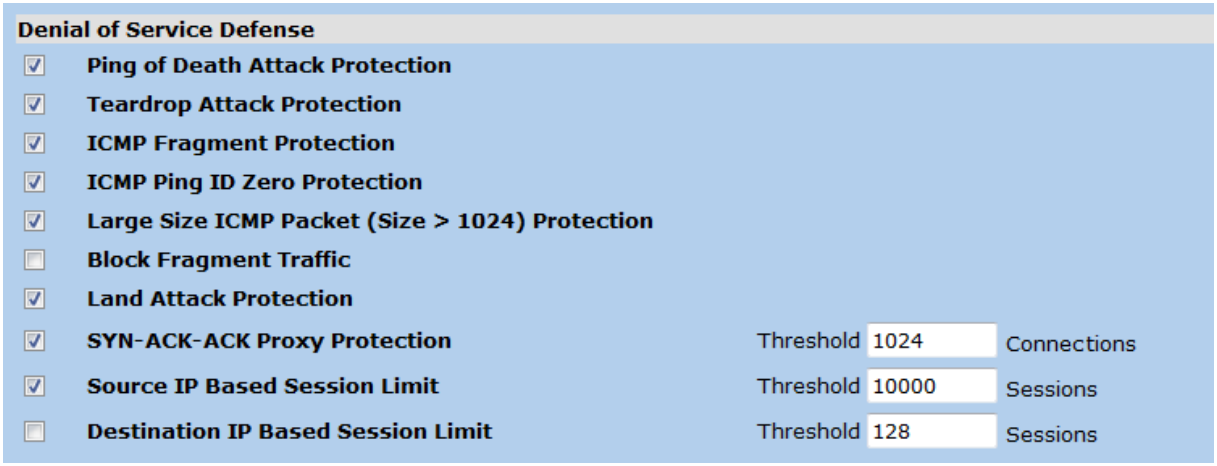
Queue Size : kuyrukta bekletilebilecek istek sayısı . bu değerin uzerine cikilmasi durumunda yeni istekler düşürülür. Threshould değeri aşıldıktan sonra gelen half-open istekler syn-proxy sisteminde tutulur ta ki buradaki değere ulaşılan akadar . Bir syn flood saldırısında yukarıdaki değer tablosu göz önünde bulundurulursa 10240 bağlatıya cevap verilir sonrasi red edilir



IP Address Spoof Protection : Firewall'un herhangi bir bacağından veya zone'nundan gelen paketlerin kaynak ip adresine yine firewall'un aynı bacağından erişilip erişilmediğini kontrol eder. Bu sayede bizden internete doğru spoof edilmiş ip adresleri ile çıkılması engellenmiş olur. Daha çok ISP ortamlarında kullanılması tavsiye edilir. ISP dışındaki yerlerde genelde kullanıcılar natlanarak çıktığından spoof işlemi işe yaramaz , fakat paketlerin internete çıkmasını dahi istemiyorsak bu seçeneği kullanıcılarımızın bulunduğu zone'da aktifleştirmeliyiz.

IP Address Sweep Protection : Belirtilen süre içerisinde aynı souece adresten 10 ip adresine gönderilen ICMP echo request paketlerinden hiçbirine cevap dönmemesi durumunda , aynı saniyedeki 11. ve sonraki ICMP echo request paketleri bloklanır . Bu değer 1 ile 1 milyon milisaniye arasında verilebilir.

Port Scan Protection : Belirtilen süre içerisinde tek bir kaynak ip'den tek bir hedef ip'nin 10 ayrı **kapalı** portuna SYN paketi gönderilmesi durumda o kaynağa ait 11. ve sonraki (tüm hedeflere doğru) SYN paketleri bloklanır.



seçeneklerin çoğunun seçilmesinde bir mahsur yoktur . Seçilmemesi gerektiği düşündüğüm 2 seçenek ise aşağıdakilerdir:

Block Fragment Traffic : Parçalanmış paketler her ağda olabilecek normal paketlerdir . Bu sebeple paketlerin bloklanması performans düşmesine ve paket kayıplarının artmasına sebep olabilir.

Destination IP Based Session Limit : Hedef ip adresi bazlı oturum sayısını belirler . Session doldurmaya yönelik bir saldırı gelmesi durumunda, legal kullanıcıları kesmemek için bu seçenek aktif edilmemelidir. Zaten saldırganın istediği de internete verdiğiniz hizmetleri servis verilmez hale getirmektir . Bu seçeneğin aktif edilmesi sonucu , çok az bir trafik ile sunucuları erişilemez hale gelmesi sağlanabilir.

Rakamsal Değer Gerektiren Seçenekler :

SYN-ACK-ACK Proxy Protection : Uygulama katmanında proxylik yapılan uygulamalara erişimi engelleyici saldırlardan korumak için kullanılır. Ftp gibi proxylik yapılan bir uygulamaya bağlanmak isteyen kullanıcı ile firewall arasında 3'lü el sıkışma tamamlanır, ardından firewall kullanıcıya login ekranı gonderir, bu aşamadan sonra kullanıcı login olmayıp yeni baglantılar açmak istemesi durumunda burada belirtilen sayı kadar oturum isteği göndermesine izin verilir. Sonraki bağlantı istekleri bloklanır. Rakamın çok yüksek tutulması , firewall'un proxylik yapabilecek oturum sayısının aşılmasına ve legal isteklerin gerçekleştirilememesine sebep olur . Kısıtlama kaynak ip bazlı yapılır.

Source IP Based Session Limit : Tek bir ip adresinden açılabilecek toplam session sayısıdır , bu sayının limitlenmesi ile session tablosunun dolması zorlaşmış olur . **TCP connection'ları spoof edilmiş ip adresleri ile yapılamadığından, saldırganlar gerçek ip adresleri ile gelmek zorundadır** , bir ip adresinden açılabilecek session sayısı da kısıtlanması durumunda, saldırganın session tablosunu doldurmak için daha büyük botnetler ile session açması gerekecektir. Büyük botnet ile gelinmesi durumunda bu değer düşürülmelidir. düşürülebilecek minimum sayıyı bulabilmek için sistemimize tek ip adresinden gelen max bağlantı sayısı bulunmalıdır. Buda networkümüzün normal zamandaki istatistiklerinin tutulmasına bağlıdır.

Netscreen den bu değerleri direk alamıyoruz fakat çeşitli analiz yazılımları ile aşağıdaki gibi rapor alınabilir :

```
-Session Overview Report-

Total Number of Connections:                    8301
The average Number of Sessions Per IP:          5.2872611465.

Top 5 Source IP addresses with the most connections:

Number of Connections - IP Address
1211.0    -    10.6.5.4
1126.0    -    10.3.2.1
1011.0    -    10.88.99.100
106.0     -    88.228.72.227
101.0     -    88.249.86.196

Top 5 Destination IP addresses with the most connections:

Number of Connections - IP Address
4533.0    -    75.5.10.15
86.0      -    172.25.0.5
64.0      -    212.175.40.157
48.0      -    10.9.8.7
45.0      -    67.205.67.14
```

Son olarak TCP/IP anormallikleri ile ilgili seçeneklerin aktif edilmesi var :

yukarıdaki seçeneklerinin tümünün seçilmesinde bir mahsur yoktur . Seçenekler herhangi bir tcp oturumunda olmaması gereken flag kombinasyonları ve durumları içermektedir.

NOT : Yukarıdaki değerleri en doğru şekilde doldurabilmek için normal zamanda network'teki trafiğifiği iyi analiz etmeliyiz . Max ve min değerleri belirlemeliyiz. Saldırı anında bu değerler nereye kadar çekilebileceğini belirlemeliyiz.