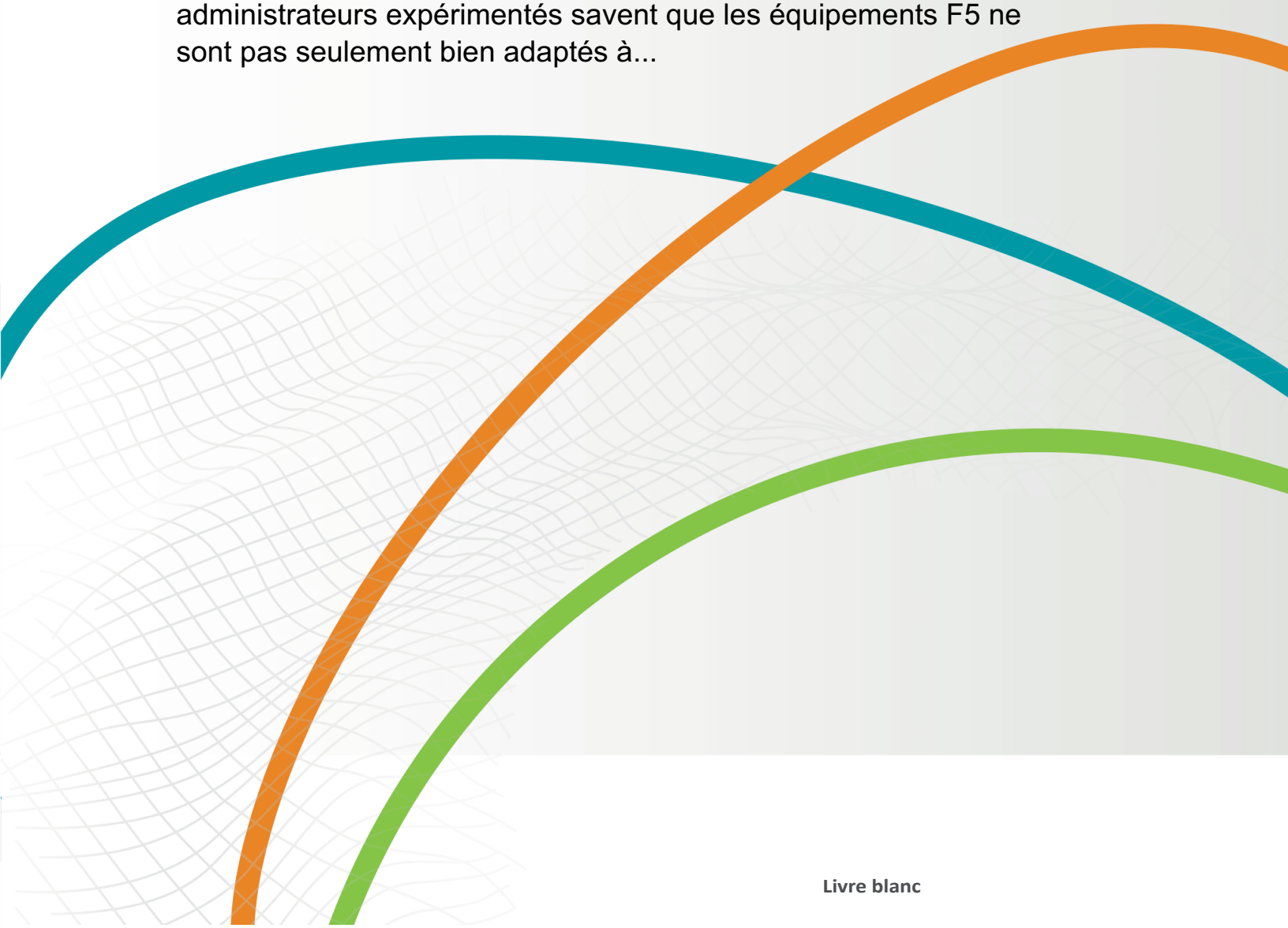
F5 DDoS Protection : Pratiques recommandées (Volume 1)

Le déni de service distribué (DDoS) est une préoccupation majeure pour de nombreuses organisations aujourd'hui, des marques de l'industrie financière de haut niveau aux fournisseurs de services. Les administrateurs expérimentés savent que les équipements F5 ne sont pas seulement bien adaptés à...



Livre blanc

1 Concept

Le déni de service distribué (DDoS) est une préoccupation majeure pour de nombreuses organisations aujourd'hui, des marques de l'industrie financière de haut niveau aux fournisseurs de services. Les administrateurs expérimentés savent que les équipements F5 sont non seulement bien adaptés à l'atténuation des attaques DDoS, mais qu'ils sont parfois les seuls à pouvoir atténuer certains types de DDoS. Ce que beaucoup d'administrateurs ignorent, c'est qu'une solution DDoS complète sur site peut être réalisée avec un complément de produits F5.

Une attaque DDoS peut être un engagement stressant où certaines parties du réseau ne répondent pas et où les équipements peuvent tomber en panne. Ce n'est pas le moment de planifier une défense - la préparation de vos applications réseau en temps de paix vous aidera grandement à atténuer l'attaque à l'avenir.

Ce guide suppose que vous disposez d'une solution réseau F5 et d'une solution de sécurité F5 en option.

Toutes les configurations, commandes et plateformes sont supposées être TMOS 11.3.0, sauf indication contraire.

Même si la plupart des informations techniques sont specific à l'équipement F5, certaines stratégies (comme l'utilisation de pools SNAT pour éviter l'épuisement des ports) peuvent également s'appliquer aux appareils d'autres fournisseurs.

2 Architecture résistante aux DDoS

Il est possible de construire un réseau de livraison d'applications qui soit résistant aux attaques DDoS. Cette section traite du travail qui peut être effectué avant une attaque pour rendre le réseau et les applications résilients.

2.1 Architecture recommandée par F5

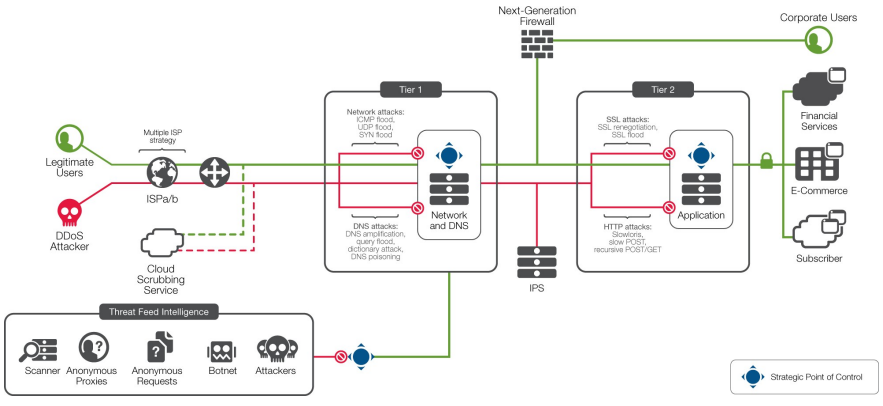


Figure 1 : F5 recommande une approche DDoS à deux niveaux.

De nombreuses organisations remanient leur architecture pour résister aux attaques DDoS. Pour de nombreux clients, F5 recommande une solution DDoS à deux niveaux, où le first (périmètre) est composé d'un firewalling réseau de couches 3 et 4 et d'un simple équilibrage de charge vers un second niveau de services plus sophistiqués (et également plus gourmands en ressources CPU), notamment la terminaison SSL et le Web Application Firewalling.

L'approche à deux niveaux présente plusieurs benefits :

- L'atténuation peut être isolée de manière à ce que les couches 3 et 4 soient atténuées au niveau 1, la protection des applications étant assurée au niveau 2.
- Les niveaux peuvent être mis à l'échelle indépendamment les uns des autres. Par exemple, si l'utilisation du WAF augmente, une autre appliance (ou lame) peut être ajoutée au deuxième niveau sans affecter le first niveau.
- Les niveaux peuvent avoir différents types de plateformes et même différentes versions de logiciels.
- Lorsque de nouvelles politiques sont appliquées au deuxième niveau, le first tier peut diriger juste une partie du traffic vers les nouvelles politiques jusqu'à ce qu'elles soient entièrement validées.

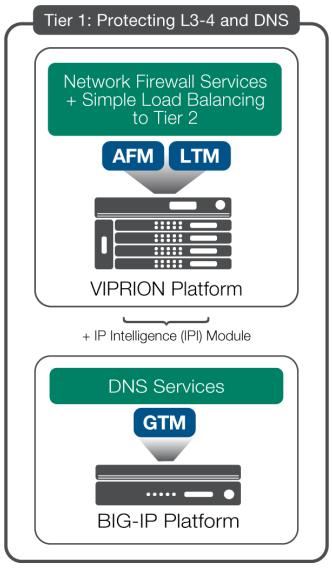
	Niveau 1Tier 2DMZ		
Composants F5	AFM + LTM	LTM + ASM	GTM DNS Express
Modèle OSI	Couches 3 + 4	Niveau 7+.	DNS
Capacités	Pare-feu réseau	Résiliation du SSL	
	Équilibrage de charge de premier niveau	Pare-feu pour applications Web	Résolution DNS
	Listes noires de réputation IP	Équilibre	
Attaques atténuées	Inondations de SYN	Slowloris	
	Inondations ICMP	Poste lent	Inondations UDP
	Paquets malformés	Apache Killer	Inondations DNS
	Flood TCP	RUDY / Keep Dead	NXDOMAIN Inondations
	Mauvais acteurs connus	Renégociation SSL	DNSSEC

2.2 Niveau 1 : Défense du réseau

Le first niveau est construit autour du firewall réseau. Vous avez Presque certainement déjà un firewall réseau (il peut s'agir ou non de F5) et une équipe firewall réseau (ou au moins un administrateur). À ce niveau, vous préparerez les défenses autour des couches 3 et 4 (IP et TCP). C'est là que vous atténuerez les SYN floods, les TCP floods et bloquerez les adresses sources lors d'une attaque DDoS.

Les sections suivantes s'appliquent à l'équipement du niveau 1, qu'il s'agisse du module firewall F5 AFM ou d'un équilibreur de charge F5 LTM devant le firewall réseau d'un autre fournisseur.

2.2.1 Choix des types de serveurs virtuels



Les organisations qui utilisent soit le firewall (AFM) soit l'équilibreur de charge (LTM) de F5 au niveau 1 ont le choix sur la façon de structurer leur configuration. Il existe quatre options pour définir un objet " d'écoute ". Bien qu'elles soient toutes des façons valables d'organiser la configuration, certaines présentent des atouts différents face aux DDoS.

- Les **serveurs virtuels full-proxy** sont les serveurs virtuels standard dans une configuration F5. Ces auditeurs établissent une connexion réelle avec chaque client entrant avant d'initier une connexion secondaire au serveur. L'acte même de terminer et de valider la connexion du client fournit un large éventail de protection avant même que le deuxième niveau ne soit invoqué.
- Les **serveurs virtuels de transfert** sont plus rapides et protègent toujours contre les pannes SYN, mais n'offrent pas le même niveau de protection que les serveurs virtuels full proxy.
- Les **serveurs virtuels Wildcard** permettent de **découpler les règles de firewall du serveur virtuel d'application**. Cela permet de créer une règle qui dit "pour toute adresse fournissant des services FTP, appliquer ce jeu de règles, cette politique de mise en miroir et cette politique de NAT source."
- Les **domaines de route**, qui isolent les sous-réseaux IP dupliqués dans des tables de routage logiques et séparées, sont courants dans les environnements des fournisseurs de services. Alors que les domaines de route n'apportent que peu ou pas de benefit concernant le DDoS en soi, ils peuvent être utilisés comme des chevilles sur lesquelles accrocher des politiques de sécurité de couche 4.

Figure 2 : Les serveurs Wildcard sont une option au niveau 1

```
ltm virtual ws_ftp {
destination 0.0.0.0:ftp
ip-protocol tcp
profiles { ftp { } tcp { } }
translate-address disabled
}
```

En général, **F5 recommande l'utilisation de serveurs virtuels Full Proxy ou Forwarding** au niveau 1 lorsque le DDoS est une préoccupation majeure.

2.2.2 Atténuation des SYN floods au niveau 1

Les TCP SYN floods sont toujours atténués par F5. Dans la version 11.5, F5 migre même les SYN floods contre les serveurs virtuels Direct server Return (DSR). Pour vérifier que votre BIG-IP gère la protection SYN flood, vous pouvez afficher les statistiques SYN flood pour chaque serveur virtuel individuel avec la simple commande **show**.

```
% tmsh show ltm virtual vip1
…

Cookies SYN

 Statut de logiciel complet

 Hardware SYN Cookie Instances 0

 Software SYN Cookie Instances 2

 Current SYN Cache 0

 Dépassement du cache SYN

 0 Total logiciel 432.2K

 Total logiciel accepté 0

 Total logiciel rejeté 0

 Total matériel 0

 Total du matériel accepté 0
```

De nombreuses plateformes F5 peuvent atténuer les SYN floods au niveau matériel, ce qui permet aux unités centrales de pilotage du traffic principal d'effectuer d'autres tâches.

Plate-forme	Matériel informatique	SYNs par deuxième	Version
Lame B4300	80M		11.3
Lame B2100	40M		11.3
10200V	80M		11.3
10000S	40M		11.4
7200V	40M		11.4
7000S	20M		11.4
5200V	40M		11.4
5000S	20M		11.4
*Les plates-formes plus anciennes, notamment les 8800, 8400, 6800 et 6400, incluent également la prise en charge du cookie SYN matériel ; toutefois, ces modèles ne sont pas pris en charge par la version 11.3, qui constitue la base de ce document.			

Tableau 1 : Liste des plates-formes de support matériel de SYN Flood

Pour activer l'offload matériel pour l'atténuation du SYN flood pour un serveur virtuel spécific, créez un profile tcp avec une posture de sécurité plus stricte. Cet exemple définit deux variables liées au DDoS. Il active les **cookies SYN** matériels. Il définit également la variable d'**acceptation différée** qui réduit l'impact que les attaques TCP "à fenêtre zéro" peuvent avoir sur leserveur

```
% tmsh create ltm profile tcp tcp_ddos { hardware-syn-cookie deferre
d-accept
activé zero-window-timeout 10000 }
```

virtuel.

Associez ensuite le nouveau profile tcp au serveur virtuel en remplaçant le profile "tcp" existant.

```
% tmsh list ltm virtual vip1 profiles

% tmsh modify ltm virtual vip1 profiles replace-all-with { tcp_ddos
my_ddos1
http }
```

2.2.3 Refuser UDP et UDP Floods au niveau 1

Les floods UDP sont un vecteur DDoS courant, car ils sont faciles à générer et peuvent être difficiles à défendre. En général, n'autorisez pas le traffic UDP vers un serveur virtuel, sauf si l'application derrière l'accepte activement.

Même pour les applications qui acceptent UDP, un flood UDP peut submerger le système, et vous pouvez trouver qu'il est nécessaire de refuser temporairement le traffic UDP au serveur virtuel de l'application.

```
% tmsh create security firewall rule-list drop_udp { rules add { dro
p_udp_rule
{ action drop ip-protocol udp place-after first } } }

% tmsh modify ltm virtual vip1 fw-rules { drop_udp_vip1 { rule-list
drop_udp }
} }
```

Lorsque l'attaque a cessé, vous pouvez supprimer la règle du serveur virtuel.

La version 11.5 peut surveiller et atténuer les floods UDP avec des exceptions granulaires. Cela permet à une ligne de base de traffic UDP de passer par un serveur virtuel de niveau 1. Si le traffic UDP dépasse les seuils, il est abandonné, sauf s'il correspond à l'une des huit exceptions de port définies par l'utilisateur (par exemple, RTSP ou DNS).

2.2.4 Refuser les Floods ICMP

ICMP est un autre vecteur DDoS courant. Les fragments ICMP sont faciles à générer et à usurper, et peuvent bloquer les ressources de nombreux types de périphériques réseau.

AFM peut faire la différence entre une quantité normale d'ICMP et un flood ICMP en se basant sur l'analyse des modèles de traffic. Lorsque le firewall réseau d'AFM est activé sur un serveur virtuel, il surveille l'augmentation de plusieurs types de traffic. Une quantité normale sera autorisée, le reste du flood étant interdit.

Details

#	Attack ID	Attack Type	Virtual Server	Allowed Requests	Dropped Requests	Total Requests
1	129352313	ICMP flood	/Common/wildcard_vs	21,410	293,107	314,517

2.2.5 Utiliser le Profile de dispositif DDoS d'AFM

Les attaquants peuvent notamment consommer les ressources du firewall en lançant des floods de paquets invalides spécialement conçus. Le firewall devra examiner (et enregistrer) chaque paquet. F5 a constaté que les combinaisons suspectes de flags (telles que PSH+ACK avec des charges utiles vides) peuvent être populaires un mois, puis être abandonnées au profit d'une autre combinaison plus tard.

Ce paysage mouvant rend difficile toute prédiction quant aux attaques L3/L4 susceptibles de se produire. L'administrateur de sécurité (pour les firewalls d'autres fournisseurs) doit être conscient de ces attaques et être prêt à insérer des règles pour les bloquer, en veillant à ne pas utiliser plus de CPU que nécessaire.

L'approche de F5 face à ce problème a été de déplacer une grande partie de la validation des protocoles L3/L4 dans la logique matérielle personnalisée des plateformes TMOS qui la prennent en charge. Par défaut, le module AFM surveille des dizaines de vecteurs d'attaque DDoS de couche 3 et de couche 4, tels que des floods de paquets en arbre de Noël ou des paquets d'attaque LAND. La quasi-totalité de ces paquets sont rejetés, quel que soit le réglage de BIG-IP. AFM peut envoyer un message de journal spécial lorsqu'un flood de ces paquets est détecté.

Le tableau 1 indique les plateformes TMOS qui prennent en charge la validation matérielle des protocoles L3/L4. Ce sont les mêmes plates-formes qui ont le support matériel SYN flood.

Toutes les plateformes (y compris l'édition virtuelle) permettent la gestion des paramètres qui suivent ces floods de paquets suspects L3/L4. L'écran de gestion est accessible depuis l'onglet Sécurité de l'interface utilisateur. Sélectionnez ensuite **Protection DoS** et **Configuration du dispositif**.

Attack Type	Detection Threshold PPS	Detection Threshold Percent	Default Internal Rate Limit
L2 Length >> IP Length	10000	500	100000
IPV6 Fragment	10000	500	100000
Payload Length < L2 Length	10000	500	100000
TCP Header Length Too Short (Length < 5)	10000	500	100000
IPV6 Source Address == Destination Address	100	500	1000
FIN Only Set	10000	500	100000
Header Length > L2 Length	10000	500	100000
Bad IPV6 Version	10000	500	100000
Bad IPV6 Hop Count	10000	500	100000
Bad TCP Checksum	10000	500	100000
IPV6 Length > L2 Length	10000	500	100000
ICMP Flood	100	500	500
Bad UDP Checksum	10000	500	100000
IP Length > L2 Length	10000	500	100000
IPV6 Extended Header Frames	10000	500	100000

Figure 3 : Paramètres de configuration du réseau DDoS

Ces paramètres sont également disponibles via la ligne de commande avec la commande **security dos device-config**. Notez également que ces paramètres sont par micro-noyau de gestion du traffic (tmm), et non par plate-forme. Dans le tableau, les colonnes correspondent à ces valeurs.

- **Seuil de détection PPS.** Il s'agit du nombre de paquets par seconde (de ce type d'attaque) que le système BIG-IP utilise pour déterminer si une attaque est en cours. Lorsque le nombre de paquets par seconde dépasse le seuil fixé,

le système BIG-IP enregistre et signale l'attaque, puis continue à vérifier les éléments suivants chaque seconde, et marque le seuil comme une attaque tant que le seuil est dépassé.

- **Seuil de détection en pourcentage.** Il s'agit de la valeur d'augmentation en pourcentage qui spécifies qu'une attaque est en train de se produire. Le système BIG-IP compare le taux actuel à un taux moyen de la dernière heure. Par exemple, si le taux moyen de la dernière heure est de 1000 paquets par seconde et que vous définissez le seuil d'augmentation en pourcentage à 100, une attaque est détectée à 100 % au-dessus de la moyenne, soit 2000 paquets par seconde. Lorsque le seuil est dépassé, une attaque est enregistrée et signalée. Le système BIG-IP instaure alors automatiquement une limite de débit égale à la moyenne de la dernière heure, et tous les paquets dépassant cette limite sont abandonnés. Le système BIG-IP continue de vérifier toutes les secondes jusqu'à ce que le taux de paquets entrants passe en dessous du seuil d'augmentation en pourcentage. La limitation du débit se poursuit jusqu'à ce que le taux retombe sous la limite spécifiée.
- **Limite de débit interne par défaut.** Il s'agit de la valeur, en paquets par seconde, qui ne peut être dépassée par les paquets de ce type. Tous les paquets de ce type dépassant le seuil sont abandonnés. La limitation du débit se poursuit jusqu'à ce que le débit redescende en dessous de la limite spécifiée.

2.2.6 Atténuer les inondations de connexions TCP

Les floods de connexion TCP sont une anomalie de couche 4 et peuvent affecter n'importe quel dispositif à état sur le réseau, notamment les firewalls. Souvent, ces floods sont vides de contenu réel. Le LTM ou l'AFM au first niveau peut les atténuer en absorbant les connexions dans des tables de connexion à haute capacité.

Plate-forme	Connexion TCP Table Taille au	Connexion SSL Table Taille au
VIPRION 4480 (4 X B4300)	144 millions	32 millions
VIPRION 4480 (1 X B4300)	36 millions	8 millions
VIPRION 4400 (4 X B4200)	48 millions	5 millions
VIPRION 4400 (1 x B4200)	12 millions	1 million
VIPRION 2400 (4 x B2100)	48 millions	10 millions
VIPRION 2400 (1 x B2100)	12 millions	2,5 millions
Série 11000	24-30 millions	2,64-3,9 millions
Série 10200	36 millions	7 millions
Série 8900	12 millions	2,64 millions

Plate-forme	Connexion TCP Table Taille au	Connexion SSL Table Taille au
Série 7000	24 millions	4 millions
Série 6900	6 millions	660 Mille
Série 5000	24 millions	4 millions
Série 4200V	10 millions	2,4 millions
Série 3900	6 millions	660 Mille
Edition virtuelle	3 millions	660 Mille

2.2.7 Configure du fauchage adaptatif

Même avec des tables de connexion à haute capacité, il existe encore des paramètres qui peuvent être ajustés pour approfondir le profile de protection contre les attaques de flood.

Dans le cas où la table de connexion du BIG-IP est pleine, les connexions seront "récupérées" en fonction des paramètres de récupération adaptative de l'eau basse et haute.
Ces valeurs peuvent être ajustées à la baisse par rapport aux valeurs par défaut de 85 et 95, afin de commencer à atténuer plus rapidement un DDoS "piquant", et ainsi réduire la fenêtre pendant laquelle l'attaque initiale chargera les serveurs.

```
% tmsh modify ltm global-settings connection adaptive-reaper-lowater 75
```

2.2.8 Modifier les délais d'inactivité pour lutter contre les inondations de connexions vides

Si les floods de connexion de la couche 4 ne présentent généralement pas un risque élevé pour les appareils F5, ils ont definiment un impact sur d'autres appareils à état, tels que d'autres firewalls. Ces dispositifs s'effondrent presque toujours bien avant que les tables d'état de F5 ne se fillent (voir le tableau 2 de la section 2.2.6). Si la connexion flood se compose principalement de connexions vides, vous pouvez demander à BIG-IP d'être plus agressif pour fermer ces connexions vides.

Il y a trois profiles primaires associés à la couche 4 sur BIG-IP :

- fastL4 - le profile TCP haute performance assisté par le matériel
- tcp-le profile TCP standard utilisé par la majorité des serveurs virtuels.
- udp-le profile standard UDP

Remarque : vous pouvez en voir d'autres, comme ceux associés à l'optimisation du réseau étendu, qui sont basés sur les profiles tcp ou udp.

Utilisez les attributs suivants de ces profiles pour contrôler la durée d'inactivité d'une connexion avant qu'elle ne soit fermée par BIG-IP. Lors d'une attaque lourde, utilisez des valeurs de plus en plus petites.

Pour le profile fastL4, remplacez les valeurs **reset-on-timeout** et **idle-timeout**. Le délai d'attente par défaut est de 300 secondes, qui doit être réduit de manière significative lors d'une attaque.

```
 % tmsh create ltm profile fastl4 fastl4_ddos { reset-on-timeout dis
abled idle- timeout 15 }
```

Pour chaque serveur virtuel fastL4 attaqué, remplacez le profile fastL4 par votre nouveau profile.

Pour le profile tcp, remplacez les deux mêmes valeurs pour les mêmes raisons. Pendant que vous y êtes, vous pouvez aussi ajuster les valeurs **hardware-syn-cookie** et **zero-window- timeout**. Voir la section 2.2.2.

Pour le profile udp, réduisez uniquement la valeur **idle-timeout (**la valeur par défaut est de 60 secondes).

2.2.9 Contrôle de la mise en forme du débit

Une autre technique défensive qui peut être déployée rapidement est la mise en forme du débit. La mise en forme du débit peut limiter le taux de traffic entrant au BIG-IP et peut être le moyen le plus simple de repousser une attaque volumétrique. Bien que puissante, la mise en forme du débit n'est pas la technique idéale pour se défendre contre les DDoS. Parce qu'elle ne fait pas la différence entre les bonnes et les mauvaises requêtes, la mise en forme du débit peut également rejeter votre bon traffic, ce qui n'est probablement pas ce que vous souhaitez.

Vous configurez les profiles de mise en forme du débit manuellement, puis les affectez à un serveur virtuel.

Dans cet exemple, la classe de mise en forme du débit nommée "protect_apache" garantit qu'au moins 1mbs de traffic atteindra la cible, mais que pas plus de 10mbs seront autorisés.

```
net rate-shaping class protect_apache { rate 1mbps ceiling 10mbps }
```

Appliquez ensuite cette classe de mise en forme du débit à chacun de vos serveurs virtuels ciblés.

2.2.10 Définir le taux maximal de rejet ICMP

La variable système **TM.MaxRejectRate** peut réduire les effets d'une attaque par déni de service en vous permettant de limiter le nombre de RST TCP ou de paquets inaccessibles ICMP que le système BIG-IP envoie en réponse aux connexions entrantes qui ne peuvent pas être mises en correspondance avec des connexions de serveur virtuel. La valeur par défaut de la variable système **TM.MaxRejectRate** est de 250 TCP RST ou 250 paquets ICMP inaccessibles par seconde.

Abaisser la valeur à 100 peut contribuer à une réduction de la congestion sortante sans affecter autrement les performances du réseau.

```
% tmsh modify sys db tm.maxrejectrate value 100
```

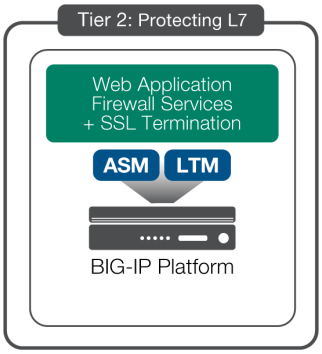
2.3 Niveau 2 - Défense de la demande

Le deuxième niveau est celui où vous déployez des mécanismes de défense sensibles aux applications et gourmands en ressources CPU, comme les murs de connexion, la politique de firewall des applications Web et les iRules LTM. Le niveau 2 est également celui où la terminaison SSL a généralement lieu. Bien que certaines organisations résilient SSL au niveau 1, cela est moins courant à ce niveau en raison de la sensibilité des clés SSL et des politiques interdisant de les conserver dans le périmètre de sécurité.

2.3.1 Comprendre les inondations de GET

Les GETs et POSTs récursifs font partie des attaques les plus pernicieuses d'aujourd'hui. Ils peuvent être très difficiles à distinguer du traffic légitime.

Les floods GET peuvent submerger les bases de données et les serveurs. Les GET Floods peuvent également provoquer un " reverse full pipe " : F5 a enregistré un attaquant qui envoyait 100Mbs de requêtes GET à une victime et en sortait 20Gbs de données.



Si vous disposez d'une solution anti-DDoS basée sur les signatures (de F5 ou d'un autre fournisseur), exploitez-la pour protéger votre application. Avec LTM et ASM, F5 propose de nombreux moyens différents pour atténuer les attaques difficiles de la couche application.

Les stratégies d'atténuation des effets de GET floods comprennent :

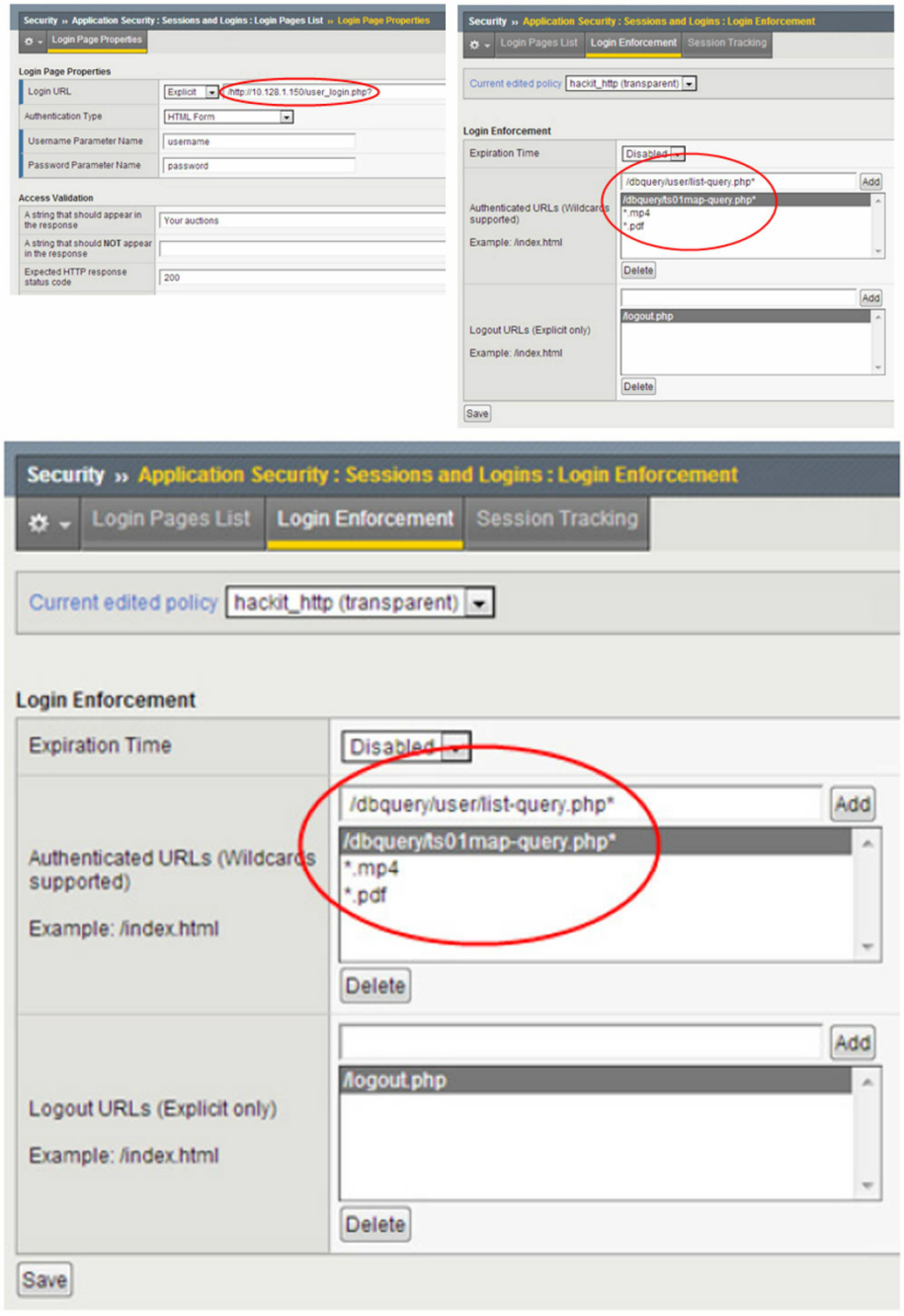
- La défense Login-Wall
- Profiles de protection DDoS
- Application réelle du navigateur
- CAPTCHA
- iRègles d'étranglement des demandes
- iRègle personnalisée

2.3.2 Réduire la surface de menace en configurant un Login-Wall

La technique la plus puissante pour déjouer les attaques au niveau de l'application consiste à n'autoriser que les utilisateurs authentifiés à accéder aux parties de votre application qui concernent les bases de données. La création d'un mur de connexion peut être un travail délicat qu'il vaut mieux réaliser en temps de paix et non lors d'une attaque DDoS trépidante. Notez que toutes les applications ne peuvent pas s'appuyer sur des utilisateurs enregistrés et doivent traiter du traffic anonyme, mais pour celles qui le peuvent, les murs de connexion constituent la défense.

2.3.2.1 Désigner un mur de connexion avec ASM

ASM offre des facilités pour ce faire dans le cadre de la politique ASM grâce à l'utilisation de pages de connexion et à l'application de la connexion. Cette fonction permet de faire en sorte que les utilisateurs ne puissent pas interagir avec un ensemble d'URL tant qu'ils ne se sont pas authentifiés avec succès sur l'une des pages de connexion.



Définissez d'abord les pages de connexion à partir de l'écran Sécurité → Sécurité des applications →Sessions et connexions.

Utilisez ensuite l'onglet **"Login Enforcement"** pour spécifier les pages qui doivent être protégées. Idéalement, il s'agira d'objets volumineux tels que les fichiers .MP4 et .PDF, ainsi que de toute requête de base de données qui pourrait être utilisée contre vous dans le cadre d'une attaque asymétrique.

Pour une explication complète de la fonction d'application de la connexion, consultez la section " Création de pages de connexion " dans le guide de configuration ASM.

Remarque : si vous n'êtes pas sûr des ressources à protéger, vous pouvez reconnaître vos propres applications (voir la section 3.2.2).

2.3.2.2 Script d'un mur de connexion

Vous pouvez réaliser un mur de connexion avec une simple iRule LTM en définissant un cookie spécifique à la page de connexion, puis en vérifiant ce cookie sur chaque autre page. Créez cette iRule, attachez-la et testez-la. Puis détachez-la et conservez-la dans votre bibliothèque pour l'activer si nécessaire.

Voici un lien vers une iRule de mur de connexion sur DevCentral.

2.3.2.3 Protéger les applications avec des profiles de protection DoS

Le pare-feu d'applications Web F5, ASM, comprend des "profiles DoS" spécifiques aux applications. Ces profiles puissants détectent les conditions DoS en surveillant la latence du serveur **ou les taux de requête http.** ASM peut ensuite déclencher un événement iRule facultatif lorsque l'attaque est atténuée.

Les options d'atténuation sont les suivantes :

Utilisez les commandes suivantes pour créer un profile DoS et l'attacher à l'application :

```
% tmsh create security dos profile my_dos_prof { application add { L
rule1 {
latency-based { url-rate-limiting enabled mode blocking } } } }

% tmsh modify ltm virtual my_vip1 profiles add { my_dos_prof }
```

Vous pouvez accéder à ce profile DoS à partir de l'onglet Sécurité. Sélectionnez ensuite Protection DoS. Dans cet écran, cochez Sécurité des applications, puis configurez les paramètres de protection contre le L7DOS.

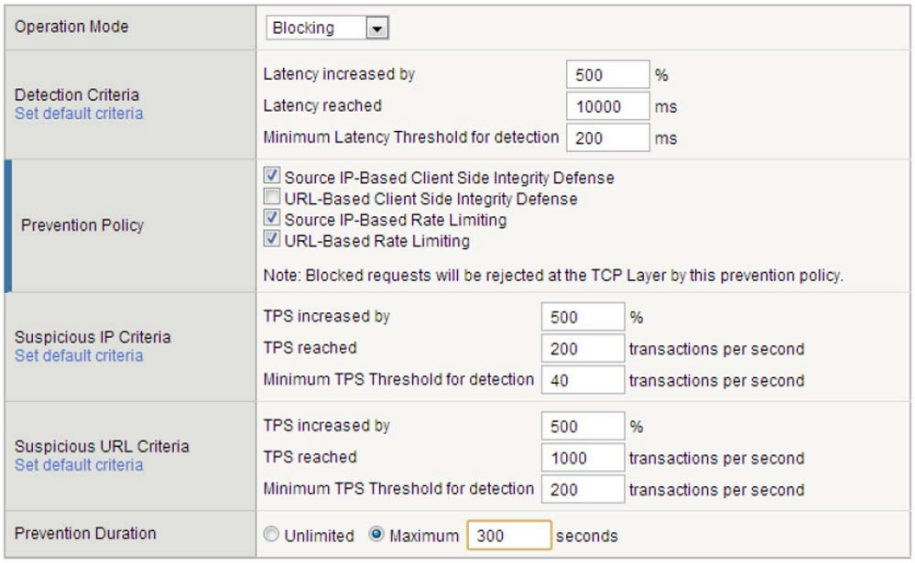


Figure 4. Configuration de la protection complète L7DOS du module ASM

2.3.2.4 Appliquer les navigateurs réels

Outre l'authentification et la détection basée sur les tps (section 2.3.2.3), il existe d'autres moyens pour les dispositifs F5 de distinguer les navigateurs Web réels des bots probables.

Le moyen le plus simple, avec ASM, est de créer un profile de protection DoS et d'activer l'option " Source IP-Based Client Side Integrity Defense ". Cela injectera une redirection JavaScript dans le flux client et vérifiera chaque connexion la first fois que cette adresse IP source est vue.

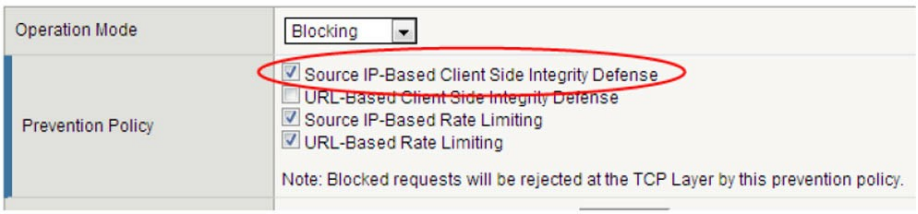


Figure 5. Insérer une redirection Javascript pour vérifier un vrai navigateur

Depuis la ligne de commande :

```
 % modify security dos profile my_ddos1 application modify { Lrule1
{ tps-based { ip-client-side-defense enabled } } }
```

2.3.2.5 Inondations par requête GET via le script

La communauté F5 DevCentral a développé plusieurs iRules puissantes qui étranglent automatiquement les requêtes GET. Les clients les refining continuellement pour rester au fait des techniques d'attaque actuelles.

Voici l'une des iRules qui est suffisamment simple pour être représentée dans ce document. La version live se trouve sur cette page DevCentral : HTTP-Request-Throttle

```
when RULE_INIT {

 Timer de vie de l'objet subtable. Définit combien de temps cet objet e xiste dans le tableau.
sous-tableau

 set static::maxRate 10

 # Ceci définit la durée de la fenêtre glissante pour compter les demandes.
.

 # Cet exemple permet 10 requêtes en 3 secondes set static::windowSecs 3

 set static::timeout 30

}

when HTTP_REQUEST {

 if { [HTTP::method] eq "GET" } {

 set getCount [table key -count -subtable [IP::client_addr]] if { $getCount < $static::maxRate

 } {

 incr getCount 1

 table set -subtable [IP::client_addr] $getCount "ignore"
$static::timeout $static::windowSecs

 } else {

 HTTP::respond 501 content "Demande bloquéeDépassement de la limite de demandes par seconde."
```

```
  retour
  ner

  }


}
```

Une autre iRule, qui découle en fait de la précédente, est une version avancée qui comprend également un moyen de gérer l'adresse des IP interdites depuis l'iRule elle-même :

- Laissez tomber les connexions suspectes.
- Renvoyer une redirection JavaScript au client afin d'imposer l'utilisation d'un navigateur.
- Limitation du débit par adresse client ou URI.
- URI-RequestLimiteriRule-Déclenche les requêtes HTTP excessives vers des URI spécific ou à partir d'une IP

2.3.2.6 Utilisez les CAPTCHA pour éliminer les bots

Une autre façon d'atténuer les GET floods est de vérifier l'"humanité" en utilisant un mécanisme CAPTCHA.Le mécanisme CAPTCHA montre des images de mots brouillés à l'utilisateur, qui prouve son humanité en tapant les mots dans un formulaire Web. Les CAPTCHA restent l'un des meilleurs moyens de distinguer les humains des ordinateurs, même si les pirates informatiques et les chercheurs tentent de les "casser" depuis plus de dix ans. Les progrès réalisés dans le domaine des algorithmes de reconnaissance des formes semblent rapprocher les attaquants de l'automatisation du système CAPTCHA. Cependant, selon l'expérience de F5, le travail de calcul nécessaire pour "casser" un CAPTCHA diminue considérablement l'avantage asymétrique d'un attaquant DDoS moderne, ce qui fait que ces attaques restent théoriques pour le moment. Cela signifie que les CAPTCHA restent un moyen efficace de repousser les botnets.

Google propose le service reCAPTCHA, qui remplit cette fonction tout en décodant les textes anciens. Il existe une iRule Google ReCAPTCHA sur DevCentral qui peut être utilisée pour fournir la verification qu'un humain se trouve à l'autre bout de la connexion. Téléchargez l'iRule (environ 150 lignes) et modifiez-la pour fournir certaines des informations de base (comme votre clé Google reCAPTCHA et votre serveur DNS). Mettez-la à disposition sur votre BIG-IP. Attachez-la à un serveur virtuel et testez-la, puis tenez-la prête pour le déploiement.

2.3.3 Script d'une atténuation personnalisée

Si toutes les autres techniques doivent être écartées, vous pouvez findre qu'il est nécessaire d'écrire une iRule personnalisée pour défendre votre application contre une attaque de la couche applicative. Ces iRules personnalisées entrent généralement dans l'une des deux catégories suivantes : le filtering et le blocage sans discernement.

Bien que cette technique soit peut-être la plus "manuelle" de toutes celles présentées dans ce document, elle est également la plus puissante et la plus utilisée par les clients agiles de F5. L'extrême programmabilité des iRules de F5 donne à un administrateur la possibilité de bloquer pratiquement n'importe quel type d'attaque, à condition qu'il maîtrise suffisamment bien le script. Les iRules liées à la sécurité protègent aujourd'hui de nombreuses organisations et constituent l'un des véritables différentiateurs de F5 pour les attaques DDoS de la couche application.

Si l'attaque vous laisse un accès Internet sortant, recherchez sur devcentral.f5.com certains des mots-clés qui pourraient correspondre à votre attaque. Vous findrez peut-être qu'une iRule a déjà été écrite pour vous !

Pour écrire votre propre iRule, first disséquez le traffic d'attaque et finissez une caractéristique du traffic d'attaque entrant que vous pouvez utiliser pour distinguer le mauvais traffic du bon. Ensuite, écrivez une iRule qui détecte ce traffic et le laisse tomber. Si vous n'êtes pas un auteur d'iRule, il existe des iRules disséminées dans ce document (et partout dans DevCentral) que vous pouvez utiliser comme exemples. Attachez votre nouvelle iRule au serveur virtuel de l'application.

Un exemple d'iRule de sécurité simple est cette première iRule de **Dirt Jumper**, qui met l'accent sur le fait que le logiciel malveillant n'inclut pas de // dans son field de référence.

Si vous n'êtes pas en mesure de distinguer facilement le bon traffic du mauvais, vous pouvez écrire une iRule qui rejette le traffic en fonction de l'objet demandé. Par exemple, si les attaquants demandent un file PDF ou MP4 particulièrement volumineux, vous pouvez utiliser une iRule pour abandonner toutes les

Vous pouvez également utiliser des groupes de données externes qui sont hébergés en dehors du BIG-IP.

Utilisez ensuite un simple scrubber iRule pour éliminer les requêtes qui demandent des URI correspondant à la classe de données.

```
ltm data-group internal block_uris {

 records {

 /faqs/faq.mp4 { }

 /locator/locations.pdf { }

 /cgi-bin { }

 }

 type de chaîne

}
```

Ce n'est definitivement pas la meilleure solution, car elle refusera le bon traffic comme le mauvais. Cela peut maintenir vos serveurs en vie, mais si vous avez le temps et la capacité d'écrire une règle comme celle ci-dessus, vous pouvez généralement findir quelque chose pour distinguer le bon traffic du mauvais.

2.3.4 Atténuer les DDoS SSL de niveau 2

Bien qu'il soit possible et parfois préférable de terminer le SSL à l'un ou l'autre niveau, F5 recommande un appareil physique (non virtuel) pour terminer le SSL au niveau 2. De nombreuses attaques DDoS SSL seront atténuées par la présence même du matériel d'accélération SSL utilisé dans les dispositifs physiques F5. Il s'agit notamment de

- Attaques du protocole SSL
- Attaques par rejeu SSL
- Connexion SSL floods
  Que le matériel soit utilisé ou non, F5 atténuera également les floods de la connexion SSL grâce au fauchage adaptatif (voir section 2.2.7) et à une table de connexion à haute capacité (section 2.2.6).

  L'attaque par renégociation SSL peut être atténuée de deux manières. Dans la plupart des cas, vous pouvez simplement désactiver temporairement la fonction de renégociation SSL au niveau du profile de clients SSL du serveur virtuel. Cependant, les connexions à très longue durée de vie (comme les guichets automatiques ou les connexions de base de données) nécessiteront toujours la possibilité de renégocier.

2.3.5 Comprendre le multiplexage des connexions et l'épuisement des ports

En général, n'exécutez pas les fonctions telles que le multiplexage des connexions et le SNAT au niveau 1. Ces fonctions et les éléments supplémentaires associés, comme l'insertion de l'en-tête X- Forwarded-For, doivent être traités au niveau 2.

2.3.5.1 Multiplexage des connexions

Une attaque DDoS de niveau 7 peut épuiser les ressources du back-end telles que les tables de connexion. L'une des façons de combattre cet effet est de multiplexer les connexions à travers l'équilibreur de charge. Sur LTM, cette fonction est appelée OneConnect et peut réduire le nombre de connexions TCP utilisées d'un ordre de grandeur tout en maintenant (voire en améliorant) le nombre total de demandes par seconde.

La fonction OneConnect doit être testée avec chaque application avant d'être utilisée comme défense DDoS. Certaines applications peuvent nécessiter des connexions distinctes par utilisateur.

2.3.5.2 Épuisement des ports

Un SNAT prend en charge environ 64 000 connexions simultanées par IP de destination. Un volume élevé de demandes peut dépasser la limite de 64 000 connexions et entraîner l'épuisement du port TCP. Vous pouvez utiliser un pool SNAT pour surmonter cette limitation. Configure et définit l'adresse IP appropriée au sein du pool SNAT pour atténuer l'épuisement.

Par exemple, si votre serveur virtuel **vip1** utilise la traduction d'adresse source automatique simple, vous pouvez le changer pour utiliser un pool d'adresses IP avec les commandes suivantes. Cet exemple utilise seulement trois adresses pour augmenter les ports disponibles de 64 000

```
% tmsh create ltm snatpool ddos_snatpool members add { 10.1.20. 161 10.1.20.162
10.1.20.163 }

% tmsh modify ltm virtual vip1 source-address-translation { poo l ddos_snatpool }
```

à 192 000.

Pour chaque adresse ajoutée au pool SNAT, vous pouvez souhaiter attribuer une valeur de délai d'attente discrète (la valeur par défaut est indefinite). Avec un délai d'inactivité, BIG-IP peut fermer les connexions

```
 % tmsh modify ltm snat-translation 10.128.20.161 { ip-idle-tim eout 60 }
```

inactives et contribuer à protéger les firewalls à état en amont.

Répétez cette commande pour chacune des adresses de votre snatpool (10.1.20.162 et 10.1.20.163 dans l'exemple ci-dessus).

3 Autres pratiques recommandées en matière de DDoS

3.1 Atténuer les DDoS DNS

Le DNS est le deuxième service le plus ciblé après HTTP. Lorsque le DNS est perturbé, tous les services externes du centre de données (et non une seule application) sont affectés. Ce point unique de défaillance totale, ainsi que l'infrastructure DNS historiquement sous-provisionnée, font du DNS une cible très tentante pour les attaquants. Même lorsque les attaquants ne ciblent pas spécifiquement le DNS, ils le font souvent par inadvertance : si les clients attaquants interrogent tous l'IP de l'hôte cible avant de lancer leurs floods, le résultat est une attaque indirecte contre le DNS.

En raison du protocole DNS relativement simple, basé sur le protocole UDP, une attaque DNS présente deux caractéristiques principales :

- Les attaques DNS sont faciles à générer.
- Les attaques DNS sont difficiles à défendre.

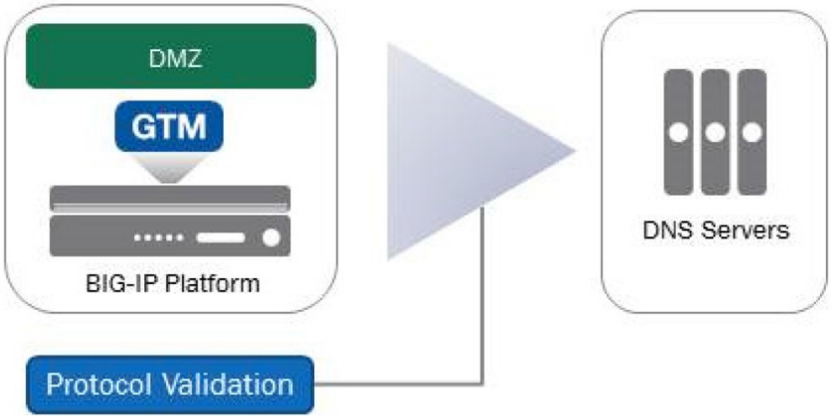


Figure 6 : Atténuation des DDoS DNS

Il existe quatre stratégies sur site pour atténuer les attaques DDoS par le DNS :

- Utiliser la validation du protocole.
- Détecter et prévenir les erreurs de DNS.
- Surprovisionnement des services DNS contre les requêtes NXDOMAIN.
- Liste noire en dernier recours.

3.1.1 Considérer le placement des services DNS

Vous pouvez remarquer que dans la figure 1, le service DNS existe en tant que son propre ensemble de dispositifs derrière le périmètre de sécurité. Souvent, le DNS est servi à partir de cette zone démilitarisée (DMZ) située entre les niveaux de sécurité. Cela permet de maintenir le DNS indépendant des applications qu'il dessert - par exemple, si cette partie du centre de données disparaît, le DNS peut rediriger les demandes vers un centre de données secondaire (ou le cloud). **F5 recommande cette stratégie consistant à maintenir le DNS séparé** des niveaux de sécurité et d'application pour une flexibilité et une disponibilité maximales.

Certaines grandes entreprises disposant de plusieurs centres de données iront plus loin et serviront les DNS en dehors du périmètre de sécurité principal en utilisant une combinaison du GTM DNS Express de F5 et du module firewall AFM. Le principal bénéfit de cette approche est que les services DNS restent disponibles même dans le cas où les firewalls de niveau 1 deviennent offline en raison de DDoS.

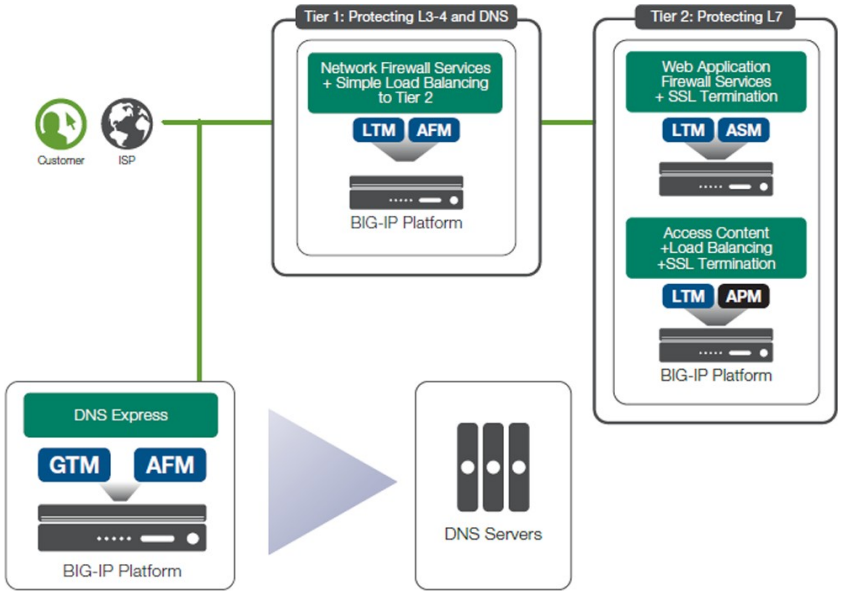


Figure 7 : Architecture DNS externe alternative

3.1.2 Utiliser la validation de protocole pour protéger les services DNS

Que vous serviez le DNS à l'intérieur ou à l'extérieur de la DMZ, vous pouvez utiliser GTM ou AFM pour valider les requêtes DNS avant qu'elles n'atteignent le serveur DNS.

Si GTM effectue l'équilibrage global de la charge du serveur, il bloque probablement déjà de nombreuses attaques DNS DDoS. Vous pouvez visualiser les performances des requêtes/réponses DNS à partir du tableau de bord principal de l'interface graphique GTM. Comme GTM est un proxy complet pour les DNS, il validera automatiquement chaque requête et rejettera celles qui sont invalides.

Cependant, vous pouvez find reque vos serveurs sont toujours submergés par des requêtes d'apparence valide. Si vous disposez du module F5 firewall AFM, vous pouvez utiliser un **Profile de sécurité de protocole** pour filtrer davantage uniquement les types spécificaux de requêtes DNS.

Dans l'**onglet Sécurité**, sélectionnez **Sécurité du protocole**, puis **Profiles de sécurité**. Sélectionnez **DNS** et appuyez sur le bouton **Créer**. Sur cet écran, vous pouvez construire un profile de sécurité de protocole pour filter ou bloquer différents types de requêtes.

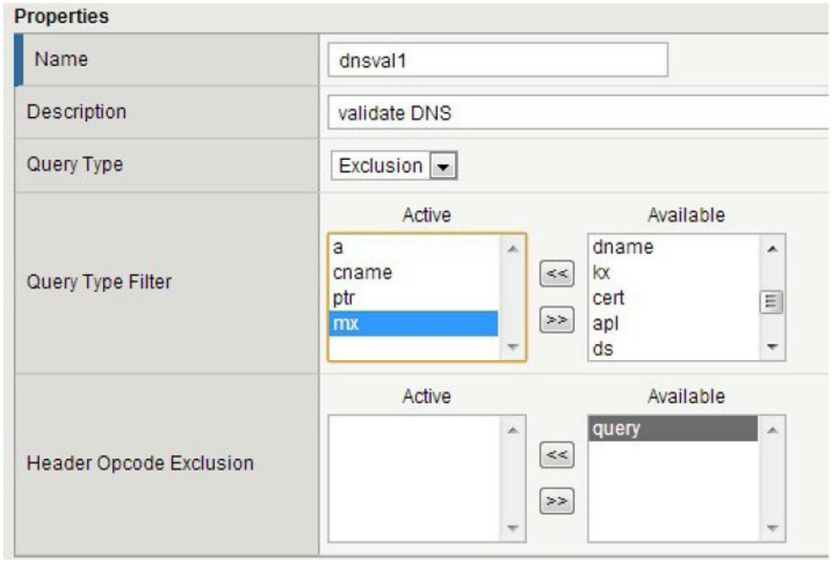
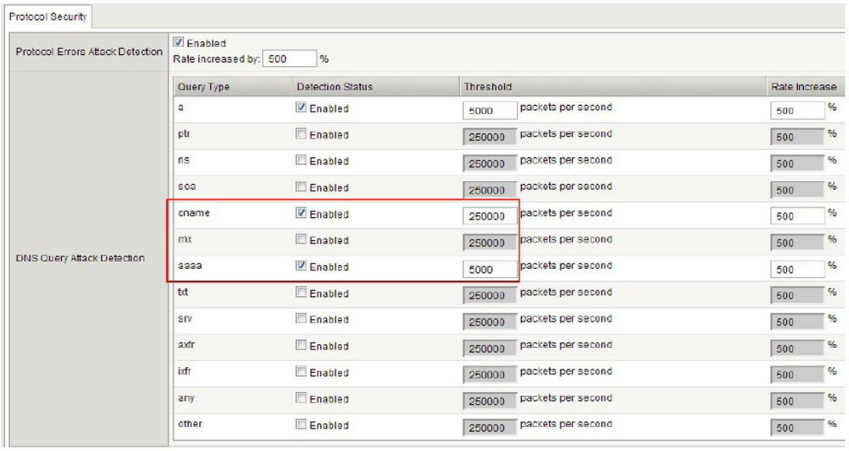


Figure 8 : Validation du protocole DNS

3.1.3 Détecter les inondations du DNS

Le module F5 firewall AFM dispose d'une puissante fonction DNS DDoS - il peut détecter les floods DNS par type d'enregistrement. Dans l'onglet **Sécurité**, sélectionnez **Protection DoS**, puis **Profiles DoS** et finalement **créer**. À partir de l'écran de création, cliquez sur la case à cocher pour DNS et définissez et acceptez les paramètres de seuil.



La case à cocher Erreurs de protocole signifie que le système détecte les requêtes DNS malveillantes ou malformées et affiche, en pourcentage, l'augmentation légale du trafic de requêtes DNS avant que le système ne suive les requêtes DNS malformées et malveillantes.

Remarque : à l'heure actuelle, cette fonction firewall détecte les floods mais n'abandonne pas les paquets pour les atténuer.

3.1.4 Surprovisionnement des services DNS contre les inondations de requêtes

Les services DNS ont été historiquement sous-provisionnés. Cela s'explique en partie par le fait que pour de nombreuses organisations, la propriété du DNS n'a pas été une évolution positive pour une équipe particulière. Quelle que soit la véritable raison, un pourcentage significant de déploiements DNS sont sous-provisionnés au point de ne pas pouvoir résister à des attaques DDoS, même de petite ou moyenne envergure.

Les caches DNS sont devenus populaires car ils permettent d'augmenter la performance perçue d'un cache DNS et ils ont fourni une certaine résilience contre les attaques de requêtes DNS standard. Les attaquants sont passés à ce que l'on appelle les attaques " no such domain " (ou NXDOMAIN), qui épuisent rapidement les bénéfices de performance fournis par le cache.

La méthode recommandée par F5 pour remédier à ce problème est de faire précéder le service DNS du module proxy DNS spécial à haute performance appelé DNS Express. DNS Express agit comme un résolveur absolu devant les serveurs DNS existants. Il charge les informations de la zone depuis les serveurs, puis résout chaque demande ou renvoie NXDOMAIN. Ce n'est pas un cache et il ne peut pas être vidé par une requête NXDOMAIN.

Dans GTM ou les services DNS, DNS Express peut servir 250 000 requêtes par seconde et par CPU et est donc résistant à toutes les attaques DNS, sauf les plus virulentes. Les serveurs DNS restent en place pour gérer les données de la zone.

3.1.5 La liste noire en dernier recours

Le traffic DNS est traditionnellement UDP, qui est facile à générer et facile à usurper. Les défenses conventionnelles des couches 3 et 4, telles que la mise en liste noire par IP source, sont généralement inefficaces contre un flood DNS. En fait, le blocage des requêtes DNS par IP source peut être carrément dangereux. Par exemple, si vous bloquez sans le savoir les requêtes d'un important FAI, vous risquez de priver de service de nombreux utilisateurs légitimes sans vous en rendre compte.

Voir " Systèmes BIG-IP : DOS Protection and Protocol Firewall Implementations" (chapitre 3-Detecting and Preventing DNS DDoS attacks).

3.1.6 Attention à la participation aux DDoS A ack

3.1.6.1 Types de requêtes inutilisées

Un attaquant peut tromper un service DNS en bombardant une cible tierce en envoyant des requêtes pour des services non utilisés. Utilisez les écrans AFM (voir la figure 9 ci-dessus) pour désactiver les types de requêtes que vous n'utilisez pas. Ainsi, lorsque des requêtes sont envoyées pour ces types, elles sont abandonnées. Aucune réponse ne sera fournie, ce qui permet d'éviter de participer à une attaque DDoS.

Cela est particulièrement vrai pour les transferts MX (services de messagerie) et de zone. Si votre organisation effectue des transferts à des moments connus et specific, gardez les types IXFR, AXFR et ZXFR désactivés à tout autre moment.

3.1.6.2 DNSSEC

Le DNSSEC est une évolution importante du service mondial des noms de domaine. À terme, elle réduira les pratiques trompeuses telles que le phishing. La situation est plus compliquée pour les DNS DDoS. Les réponses DNSSEC sont parfois 10 à 20 fois plus volumineuses que les réponses DNS UDP traditionnelles. Cela signifie que les serveurs DNSSEC sont en fait incités à attaquer d'autres ordinateurs en les bombardant par inadvertance de réponses invalides.

Avec GTM, F5 dispose de la solution DNSSEC la plus performante du marché. La capacité de GTM pourrait constituer une arme puissante si elle était utilisée comme vecteur d'attaque. C'est pourquoi GTM vous permet de limiter le nombre de réponses afin d'éviter qu'il ne participe à une attaque.

```
% tmsh modify sys db dnssec.maxnsec3persec value 10
```

La variable **dnssec.maxnsec3persec** contrôle la limite supérieure des messages NSEC3 autoritaires NXDOMAIN que GTM enverra par seconde. La valeur 0 est illimitée et constitue la valeur par défaut. Une valeur plus restrictive, par exemple entre 10 et 100 par seconde, peut empêcher GTM lui-même d'être utilisé lors d'une attaque.

```
% tmsh modify sys db dnssec. signaturecachensec3 valeur true
```


La définition de la variable **dnssec.signaturecachensec3** à false empêche les messages NXDOMAIN d'utiliser le cache de GTM, empêchant ainsi un attaquant de filer le cache de GTM avec des réponses "no such domain".

3.2 Procédures de préparation aux meilleures pratiques DDoS supplémentaires

Le temps consacré à la préparation d'une attaque DDoS augmentera l'efficacité de votre défense. Voici quelques autres moyens de préparer votre organisation à une attaque DDoS.

3.2.1 Configure et vérification de la journalisation

Pendant une attaque, il y a de fortes chances que vous envoyiez des diagnostics et que vous consigniez les anomalies et les pics de traffic. Des performances élevées sont indispensables pour faire face à une attaque DDoS de grande ampleur. L'instrumentation est également importante, ce qui signifie que vous voudrez utiliser la fonction de journalisation à haut débit de BIG-IP pour envoyer ces informations à un dispositif de journalisation tiers tel que Splunk ou un SIEM tel qu'ArcSight.

Remarque : Vous **DEVEZ** utiliser les fonctions de journalisation à haut débit de BIG-IP au niveau 1 pour atténuer une attaque DDoS. N'utilisez pas la journalisation locale ; une attaque DDoS intense peut submerger la journalisation locale sur disque.

3.2.1.1 Configuration de l'enregistrement à haut débit

- Créez un pool pour le mapper à vos serveurs de logs externes (dans ce cas, il s'agit de syslog). Réécrivez si nécessaire pour ArcSight, TrustWave ou toute autre solution SIEM prise en charge par votre environnement. Créez ensuite les objets de configuration du journal pour formater et transmettre les chaînes de caractères correctement.
- Créez un profile de journal à l'aide de l'interface graphique.

```
% tmsh create ltm pool hsl_pool members add { 10.128.10.25 0:514 }

% tmsh create sys log-config destination remote-high-speed
-log log_dest_HSL { pool-name hsl_pool }

% tmsh create sys log-config destination remote-syslog log
_dest_format { format
rfc5424 remote-high-speed-log log_dest_HSL }

% tmsh create sys log-config publisher log_pub_ddos { dest inations { log_
dest_HSL log_dest_format } }
```

Accédez à la **page Sécurité > Journaux d'événements > Profiles de journalisation.** Créez un profile de journalisation en procédant comme suit :

Nom du Profile	ddos_log_profile
Pare-feu réseau	Activé
Pare-feu réseau : Editeur	log_pub_ddos
Enregistrement des correspondances de règles	Accepter, abandonner et rejeter
Enregistrer les erreurs IP	Activé
Enregistrer les erreurs TCP	Activé
Enregistrer les événements TCP	Activé
Format de stockage	field-list Sélectionnez tous les éléments disponibles et déplacez-les vers la liste des éléments sélectionnés.

- Associez cet objet de profile de journal aux serveurs virtuels protégeant votre application.

```
% tmsh modify /ltm virtual vip1 { security-log-profiles a dd { ddos_ log_profile } }
```

3.2.2 Reconnaissez vos propres applications

Les attaquants DDoS modernes vont reconnaître une application plusieurs jours ou semaines avant de lancer leur attaque DDoS. Ils vont explorer votre site web et récupérer le **temps de chargement** et la **taille des données** pour chaque URI valide. En triant l'ensemble des données obtenues, ils isoleront rapidement les requêtes les plus exigeantes en termes de CPU ou de base de données et les objets les plus volumineux (tels que les PDF et les MP4).
Au cours de l'attaque DDoS, ils demanderont ces objets de manière répétée, submergeant ainsi votre infrastructure.

Bien que la section 3.8 vous aidera à atténuer cette attaque lorsqu'elle se produira, vous pouvez vous aider à l'avance en reconnaissant vos propres applications. Cela vous donnera une visibilité avancée sur les URI et les sous-systèmes qui seront probablement des cibles, ce qui vous permettra de prendre des décisions de triage plus éclairées par la suite.

Idéalement, vous disposez d'un outil comme LoadRunner ou d'un autre outil de surveillance des performances qui peut vous fournir les mesures dont vous avez besoin. Si vous n'avez pas cette capacité, le moyen le plus simple de récupérer le tableau de base des URL, du temps de chargement et de la taille des données est d'utiliser l'utilitaire wget, disponible sur la plupart des distributions Linux. Exécutez-le avec la syntaxe suivante :

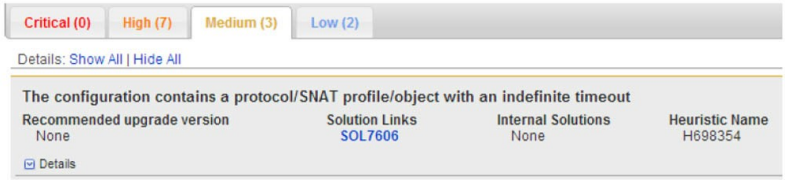
```
% wget -r --spider http://10.128.10.150 2>&1 | grep saved

2013-08-25 15:44:29 (2,48 Mo/s) - `10.128.1.150/index.html
sauvegardé [22304]

2013-08-25 15:44:29 (5,53 Mo/s) - '10.128.1.150/index.php
 sauvegardé [22304]

2013-08-25 15:44:29 (7,06 Mo/s) - `10.128.1.150/sell.php'
sauvegardé [41695]
```

Le dernier chiffre (entre crochets) est la taille des données de la requête. Vous devrez obtenir le temps de chargement en soustrayant les temps (deuxième field) les uns des autres.

3.2.3 Valider la santé des dispositifs BIG-IP existants avec iHealth

F5 fournit un service de diagnostic et d'heuristique basé sur le cloud appelé iHealth. iHealth examinera la configuration d'un appareil F5 et fera des recommandations pour que BIG-IP reste rapide,sécurisé et disponible. Si la majorité des paramètres s'applique plutôt aux deux firmes, certains de ces paramètres peuvent s'appliquer à la disponibilité et, par extension, à la résilience DDoS-.

Dans cet exemple, iHealth montre qu'un pool SNAT a été configuré sans valeurs de délai d'attente. Cela peut rappeler à un administrateur soucieux des ressources qu'il doit s'assurer que le pool SNAT utilisé est conforme aux normes de sécurité.
pour leurs serveurs virtuels durcis devraient inclure des délais d'inactivité pour maintenir le nombre de connexions à un niveau bas et empêcher un firewall amont de basculer.



Consultez le site web iHealth pour plus d'informations sur iHealth.

3.2.4 Préparer un manuel de stratégie DDoS

Un manuel de procédures ou Runbook DDoS est un manuel de procédures destiné à aider vos employés informatiques à lutter contre une attaque DDoS. Un bon manuel aidera les nouveaux administrateurs (et les administrateurs existants) à lutter contre une attaque DDoS. Le Playbook doit être tenu à jour avec des listes blanches et des informations de contact actualisées.

Quelques organisations effectuent périodiquement des exercices (ou même des tests) de déni de service distribué contre elles-mêmes afin de rester à jour et de tester le manuel. Essayez de faire en sorte que votre personnel s'entraîne à appliquer les procédures du manuel lorsque les personnes clés ne sont pas présentes - les attaques ne se produisent pas toujours au moment le plus opportun.

Si vous n'avez pas de playbook, vous pouvez en obtenir un auprès de F5.

3.2.5 Examiner les tactiques défensives dans l'architecture à deux niveaux

Certaines des tactiques défensives décrites dans les sections précédentes méritent d'être revues, notamment pour les administrateurs qui utilisent un firewall réseau non-F5.

Rappelez-vous :

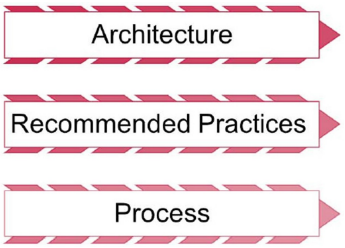
- Les pools SNAT atténuent l'épuisement des ports au niveau 1.
- Formez le traffic au niveau 1.
- Récupérer de manière agressive les connexions TCP.
- Ne mettez les DNS sur liste noire qu'en dernier recours.
- Mettez en place des murs de connexion et des CAPTCHAs au niveau 2.
- Désactivez les fonctions optionnelles gourmandes en ressources CPU au niveau 2.
- Utilisez toujours la journalisation à distance à haut débit.

En mettant en œuvre les suggestions proposées dans ce guide des meilleures pratiques, vous aurez fait beaucoup pour préparer vos applications à une attaque DDoS.

4 Conclusion

Il est important de comprendre le spectre des menaces modernes que représentent les attaques par déni de service. Il est encore plus important de comprendre comment utiliser les équipements défensifs dont vous disposez déjà.

En fonction de vos ressources et de vos besoins, vous avez peut-être déjà remanié votre réseau pour le rendre résistant aux attaques DDoS. Si c'est ce que vous envisagez, prêtez une attention particulière à l'architecture multi-niveaux recommandée décrite à la section 2.1. Même si la sécurité de votre réseau n'est pas entièrement construite à partir de la technologie F5, il est toujours judicieux de s'attaquer indépendamment aux couches 4 et 7 dans le cadre de la lutte contre les DDoS.



En suivant les pratiques recommandées, vous préparerez votre réseau, vos applications et votre personnel à résister aux attaques.

L'étape finale des pratiques recommandées par F5 pour l'atténuation des attaques DDoS consiste à préparer un playbook DDoS. Un tel playbook est un guide procédural en temps réel pour l'atténuation d'une attaque qui comprend des feuilles de travail et des journaux.

Annexe

Taxonomie et contre-mesures de l'application A ack

La section suivante recommande des mesures d'atténuation pour des vecteurs d'attaque specific de la couche 7. Nombre d'entre eux sont des attaques de type " lent et faible " qui peuvent être particulièrement pernicieuses.

Contenu

- Slowloris
- Garder la mort
- Canon à ions en orbite basse (LOIC)
- Slow-POSTs
- Attaques à fenêtre zéro
- Attaque de lecture lente
- RUDY
- Apache Killer
- Renégociation SSL
- Dirt Jumper iRule

Slowloris

Slowloris est un vecteur HTTP courant dans lequel un attaquant envoie (très lentement) de petits en-têtes HTTP pour maintenir la session HTTP en vie (par exemple, "X-a : b" toutes les 299 secondes). Si le serveur virtuel effectue actuellement un équilibrage de charge au niveau de la couche 4, envisagez de le faire passer à la

```
% tmsh list ltm virtual vip1 ltm virtual vip1
{ destination 10.128.10.141:http profiles {
fastL4 { }
}
}

% tmsh modify ltm virtual vip1 profiles replace-all-with { tcp http }
```

couche 7. Cela ajoutera une certaine protection native lorsque le profile HTTP sera ajouté.

Ainsi, BIG-IP absorbera les connexions Slowloris. Si vous craignez qu'un trop grand nombre d'entre elles s'accumulent et causent des problèmes à d'autres appareils (comme un firewall), utilisez l'iRule Slowloris suivante pour abandonner toute connexion qui n'a pas abouti au bout de 10 secondes (n'hésitez pas à ajuster ce nombre).

```
# Slowloris iRule

when CLIENT_ACCEPTED {

 set hsl [HSL::open -proto UDP -pool hsl_pool]

 set rtimer 0

 après 10000 {

 if { not $rtimer } {

 drop

 HSL::send $hsl "Dropped [IP::client_addr] - connection to
o
lent"

 }

 }

}

when HTTP_REQUEST {

 set rtimer 1

}
```

Garder la mort

Cette attaque est basée sur la consommation du processeur et de la mémoire vive. En utilisant Keep-Alive et la méthode HTTP HEAD, elle peut créer un flood de requêtes sans déclencher une défense firewall qui se base sur le nombre de connexions ouvertes au serveur.

Le module ASM peut refuser les requêtes HEAD (qui ne sont généralement pas utilisées par les navigateurs). Vous pouvez rejeter les demandes HEAD en configurant les " méthodes autorisées " dans la politique de sécurité de l'application en question.

Voir la solution 12312 pour plus d'informations.

Canon à ions en orbite basse (LOIC)

Le Low Orbit Ion Cannon est un outil de botnet volontaire étroitement associé au groupe hacktiviste Anonymous. Bien que l'outil utilise des SYN floods et des UDP floods, il est surtout connu pour ses floods HTTP de couche 7. En supposant que les floods SYN et UDP ont été atténués (voir les sections 2.2.2 et 2.2.3), la dernière étape consiste à atténuer les floods LOIC GET.

Souvent, le moyen le plus rapide de le faire est de le filtrer sur le "message de protestation" de l'attaque inclus dans chaque requête HTTP LOIC. Utilisez Wireshark ou tcpdump ou un autre outil pour isoler le message, puis ajoutez ce message à un groupe de données. Utilisez %20 pour représenter les espaces. Le message peut changer au fil du temps et vous devrez peut-être le surveiller pendant toute la

```
 ltm data-group anonmsgs { records { Somos%20legi { } U%20
dun%20goofed { } } type string }
```

durée de l'attaque.

Notez que vous pouvez utiliser des classes de données externes qui sont hébergées en dehors du BIG-IP - voir " help **search data-group" dans le** shell de la commande tmsh.

Utilisez ensuite un simple scrubber iRule pour supprimer les requêtes contenant des données utiles de cette classe de données.

```
ltm rule loic_defense_rule { when CLIENT_ACCEPTED {

 set hsl [HSL::open -proto UDP -pool hsl_pool]

 }

 when HTTP_REQUEST {

 if { [class match [HTTP::uri] contains anonmsgs] } { drop

 HSL::send $hsl "Dropped [IP::client_addr] - suspected Low Orbit Ion Cannon"
 (Chasseur d'ions en orbite basse)

 }

 }

}
```

Slow-POSTs

Le cœur de l'attaque Slow-POST repose sur l'envoi d'une requête POST avec un "content-length" donné, qui est généralement un grand nombre, puis sur l'envoi très lent du corps du message au serveur, tout en maintenant un temps d'inactivité long. Le serveur laisse la connexion ouverte pendant qu'il continue à recevoir des données. Si un grand nombre de ces demandes sont exécutées sur un serveur, il est possible que la table de connexion soit épuisée, ce qui rendrait le serveur incapable de répondre à d'autres demandes.

Si vous disposez du module ASM, vous pouvez atténuer la lenteur des messages à l'aide de deux des variables qui se trouvent dans l'écran des variables système ASM-Naviguez **vers Sécurité : Options : Sécurité des applications : Configuration avancée : Variables système et** modifiez les variables suivantes.

slow_transaction_timeout (valeur par défaut : 10 secondes). Diminuez cette valeur si nécessaire.

max_slow_transactions (valeur par défaut : 25 transactions). Réduisez cette valeur à 5 ou moins si nécessaire.

Si vous ne disposez pas d'ASM, consultez cette iRule LTM pour atténuer le Slow-POST. Elle peut être utilisée avec l'iRule Slow-read de la section suivante (il suffit de les joindre en tant que deux iRules distinctes) car l'iRule Slow-read est basée sur le serveur et l'iRule Slow-POST sur le client.

Zero Window A acks

L'attaque Zero Window est une attaque de couche 4 difficultée à détecter. Elle fonctionne en établissant une connexion TCP avec la cible, en demandant certaines données, puis en fixant la taille de la fenêtre TCP à zéro. Cela bloque la connexion au niveau du serveur, du cache ou de l'intergiciel.

Si l'attaquant définit une longueur de fenêtre TCP nulle contre un BIG-IP, vous pouvez utiliser la valeur du profile zero-window- timeout tcp mentionnée dans la section.
2.2.2 à atténuer.

A ack de lecture lente

L'attaque par lecture lente consiste à envoyer des requêtes HTTP légitimes, puis à lire très lentement les réponses HTTP à partir du tampon, dans le but de maintenir le plus grand nombre possible de connexions actives sur la victime.

Dans la version 11.3.0, la prévention de la lenteur du module ASM fonctionne sur les requêtes entrantes telles qu'un Slow POST. Pour les Slow-read, utilisez l'atténuation LTM iRule suivante :

```
when SERVER_CONNECTED {
 TCP::collect
}

when SERVER_DATA {

 set rtimer 0

Temps en millisecondes avant que la réponse HTTP lue soit
considérée comme lente :

 après 5000 {

 if { not $rtimer} {

 set hsl [HSL::open -proto UDP -pool hsl_pool]

# Lecture lente détectée pour cette réponse du serveur.
Incrémentez le compte en ajoutant un
l'entrée du tableau :

# Ajouter l'IP source du client::port à la sous table avec
un ti meout

 table set -subtable "MyApp" "[IP::client_addr]
:[TCP::clie nt_port]"
"ignoré" 180

#  Si  nous  dépassons  la  limite  de  concurrence,

 rejeter  si  {  [table  keys  -subtable  "MyApp"  -

 count] > 5} { côté client {rejeter}

 table delete -subtable "MyApp" "[IP::client_addr] :
[TCP::c lient_
port]"

 HSL::send $hsl "Droped [IP::client_addr] - reading too s
low"

 }

 }
```

```
 }

 TCP::notify réponse

 TCP::release

 TCP::collect

}

when USER_RESPONSE {

 set rtimer 1

}

when CLIENT_CLOSED {

 table delete -subtable "MyApp" "[IP::client_addr]
:[TCP::c lient_port]"
```

RUDY

R-U-Dead-Yet (RUDY en abrégé) utilise Slow-POST et une attaque DoS HTTP générique via des soumissions de field longs formulaires.

Apache Killer

L'Apache Killer est également connu sous le nom d'attaque par plage. Lorsqu'un navigateur client (tel qu'un navigateur de téléphone mobile) a besoin d'une partie seulement d'un document, il peut demander une "plage" de données avec un en-

```
 Plage : octets=0-100
```

tête HTTP de plage. Si le client ne veut que les firts 100 premiers octets, il peut dire :

L'attaque Apache Killer consiste à demander des plages multiples qui se chevauchent, ce qui perturbe les serveurs web comme

```
 Range:bytes=0-,5-1,5-2,5-3,...
```

Apache :

Il existe trois façons d'atténuer Apache Killer. Vous pouvez modifier le profile HTTP pour supprimer simplement l'en-tête Range. Par exemple, si votre profile http était nommé " http_ddos2 ", vous

exécuteriez cette commande :

```
 % tmsh modify ltm profile http http_ddos2 { header-erase
gamme }
```

Une façon plus chirurgicale d'atténuer Apache Killer est avec l'iRule suivante, qui ne supprime les demandes de plages que lorsque plus de five plages sont demandées.

```
when CLIENT_ACCEPTED {

 set hsl [HSL::open -proto UDP -pool hsl_pool]
 pcre : "/Range :[\t ]*bytes=(([0-9\- ])+,){5,}/Hi" ;
}

when HTTP_REQUEST {

 # supprimer les demandes d'intervalles pour CVE-2011-3192
s'il y a plus de cinq intervalles.
demandé

 if {[HTTP::header "Range"] matches_regex {bytes=(([0-9\-
 ])+,){5,}} } {

 HTTP::header remove Range

 HSL::send $hsl "Le client [IP::client_addr] a envoyé plus
 de 5 plages. Effacement de
en-tête de gamme".

 }

}
```

La troisième méthode d'atténuation utilisant les solutions BIG-IP consiste à utiliser la signature d'attaque ASM suivante pour détecter et agir sur une attaque utilisant cette technique.

Renégociation SSL

Si vous constatez que de nombreuses renégociations se produisent à partir de clients SSL specific, il se peut que vous subissiez une attaque de renégociation SSL. La façon la plus simple de l'atténuer est de désactiver la renégociation SSL à partir du profile de clientssl associé au serveur virtuel. Toutefois, si vous devez prendre en charge la renégociation pour les clients légitimes (tels que les anciens navigateurs à cryptographie " step-up " ou à cryptographie par le serveur) tout en atténuant l'attaque, vous pouvez utiliser cette

```
when RULE_INIT {

 set static::maxquery 5

 set static::mseconds 60000

}

when CLIENT_ACCEPTED {

 set ssl_hs_reqs 0

 set hsl [HSL::open -proto UDP -pool hsl_pool]

}

when CLIENTSSL_HANDSHAKE {

 incr ssl_hs_reqs

 after $static::mseconds { if {$ssl_hs_reqs > 0} {incr ssl
_hs_reqs -1} }

 if { $ssl_hs_reqs > $static::maxquery } { après 5000

 tomber

 HSL::send $hsl "Dropped [IP::client_addr] - too many SSL renegotiations" (Dépassement
de l'adresse du client)

 }
```

iRule, ou d'autres semblables. Cette règle ferme toute connexion qui tente plus de five renégociations en une minute :

Dirt Jumper iRule

Certaines versions de l'outil Dirt Jumper n'incluent pas de // dans leur referrer field. Voici une iRule simple pour détecter et supprimer les connexions de Dirt Jumper.

```
when CLIENT_ACCEPTED {

 set hsl [HSL::open -proto UDP -pool hsl_pool]

}

when HTTP_REQUEST {

 if { [HTTP::header exists "Referer"] } {

 if { not ([HTTP::header "Referer"] contains "\x2F\x2F") }
 {

 HSL::send $hsl "DDoS Dirt-Jumper HTTP Header Structure mi
ssing x2f x2f
Referer l'identifiant de protocole de

 [IP::client_addr]" drop

 }

 }

}
```

Télécharger le volume 2

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

Amériques
info@f5.com

Asie-Pacifique
apacinfo@f5.com

Europe/Moyen-Orient/Afrique
emeainfo@f5.com

Japon
f5j-info@f5.com