Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point DDoS Protector™

Stoppez les attaques de déni de service en quelques secondes grâce à une protection multi-couches personnalisée capable de bloquer de nombreuses attaques.

Appliances Check Point DDoS Protector

Dans le paysage des menaces actuelles, le nombre d'attaques de déni de service distribuées augmente, ainsi que leur vitesse et leur complexité. Les attaques de déni de service et de déni de service distribuées sont relativement faciles à mener, et peuvent causer de graves dommages aux entreprises qui comptent sur des services web pour fonctionner correctement. Plus de 50 boîtes à outils d'attaques de déni de service distribuées sont disponibles sur Internet, et un nombre croissant d'attaques sont lancées depuis plus de 230 pays différents. Les attaques de déni de service distribuées sont souvent motivées par le profit : en 2011, les cybercriminels ont ainsi détourné plus de 12,5 milliards de dollars. Nous constatons en 2012 une poussée inquiétante des attaques de déni de service contre les institutions financières, et les motivations hacktivistes et politiques sont également en train de devenir le forum le plus populaire pour lancer des attaques de déni de service. Le groupe Anonymous a dirigé avec succès de nombreuses campagnes contre des individus, des entreprises, des gouvernements et des états, en représailles d'actions ou de déclarations avec lesquelles le groupe n'était pas d'accord.

De nombreuses solutions contre les attaques de déni de service existent auprès des FAI, offrant une protection générique contre les attaques visant la couche réseau. Cependant, les attaques de déni de service distribuées modernes sont devenues plus sophistiquées. Elles sont capables de lancer de multiples attaques contre des réseaux et des applications. Des solutions de protection efficaces permettent aux entreprises de personnaliser leur protection pour répondre aux besoins de sécurité changeants, de réagir rapidement lors d'une attaque, et offrent différentes options de déploiement.

VUE D'ENSEMBLE

Les nouvelles appliances Check Point DDoS Protector permettent aux entreprises de poursuivre leur activité grâce à plusieurs couches de protection personnalisables, et des performances de 12 Gbps qui défendent automatiquement contre les attaques par inondations du réseau et les attaques de la couche applicative, pour une réactivité sans pareil contre les attaques sophistiquées de déni de service. Elles proposent des options de déploiement souples pour protéger facilement les entreprises de toute taille. Elles intègrent également l'administration de la sécurité pour l'analyse du trafic en temps réel, et des renseignements sur les menaces pour une protection avancée contre les attaques de déni de service. Check Point fournit une assistance 24h/24 et 7j/7, ainsi que des ressources dédiées pour assurer une protection à la minute près.

FONCTIONNALITÉS CLÉS

- Protection contre les attaques de déni de service connues et inconnues
- Protection contre les attaques visant le réseau et les applications
- Moteurs de filtrage flexibles capables de détecter et bloquer les activités malveillantes
- Protection contre les attaques HTTP
- Protection contre les attaques visant la bande passante
- Création rapide de signatures personnalisées garantissant la continuité de l'activité de l'entreprise

AVANTAGES CLÉS

- Protection contre les attaques de déni de service distribuées évolutives pour minimiser l'impact sur l'activité de l'entreprise
- Techniques avancées permettant la continuité des services web lors d'attaques
- Appliance clé en main fonctionnant dès sa mise en œuvre
- Intégration avec les solutions d'administration de Check Point pour plus de visibilité et de contrôle
- Solution performante contre les attaques de déni de service distribuées grâce à une capacité de 14 Gbps et un débit de 12 Gpbs
- Protection multi-couches capable de bloquer différents types d'attaques
- Protection personnalisée répondant aux besoins en sécurité des entreprises de toute taille
- Options de déploiement flexibles comprenant l'installation sur site ou via votre FAI

softwareblades™

PROTECTIONS MULTI-COUCHES

Protections contre les attaques par inondation du réseau et du trafic

Protection contre les attaques de déni de service distribuées visant les réseaux :

Protection comportementales — Protection contre les attaques ciblant TCP, UDP, ICMP, IGMP et les attaques fragmentées, grâce à une détection des comportements capable de s'adapter.

Bouclier — Protection contre les outils connus d'attaques à l'aide de filtres prédéfinis et personnalisés.

Protection Syn — Blocage des attaques d'usurpation SYN avec seuils de taux SYN par serveur protégé.

Liste noire — Blocage des attaques génériques avec classifications origine/destination L3 et L4 et règles d'expiration.

Limite de connexion — Blocage des protocoles génériques non pris en charge (non DNS, HTTP) et des attaques de niveau applicatif par inondation via des seuils de taux.

Protections contre les attaques applicatives

Protection contre les attaques de déni de service distribuées plus complexes abusant des ressources applicatives :

Protection SYN avec défi web — Protection contre les attaques ciblant les connexions HTTP avec seuil de taux SYN par serveur protégé.

Protections DNS comportementales — Blocage des attaques sur les requêtes DNS grâce à une détection des comportements DNS capable de s'adapter, fournissant une limitation de l'empreinte DNS et des possibilités de défi/réponse DNS.

Protections HTTP comportementales (« Atténuateur HTTP ») — Blocage des attaques sur les connexions HTTP et des attaques sur la bande passante HTTP montante grâce à une détection des comportements DNS sur serveur capable de s'adapter, empreinte HTTP avec défi/réponse web, redirection 302 et actions sur défi JS.

Protections contre les attaques ciblant les applications

Blocage des attaques nécessitant des critères de filtrage spéciaux. Des définitions flexibles de filtrage recherchent des modèles spécifiques de contenus dans chaque paquet. Possibilité d'analyser et de bloquer les attaques continues par définition de protections à la volée.

ADMINISTRATION

Les appliances DDoS Protector intègrent Check Point Security Management avec :

SmartEvent

Solution d'analyse et de gestion unifiées des événements fournissant des informations en temps réel pour remédier aux menaces et bloquer instantanément les attaques par des protections à la volée. Passage de l'aperçu métier à l'aperçu analyses en seulement trois clics.

SmartLog

Analyseur avancé de journaux fournissant des renseignements de sécurité proactifs, avec des résultats de recherche ultra-rapides à partir de n'importe quel champ de journal pour une visibilité instantanée sur des milliards d'enregistrements, et de multiples périodes et domaines.

SmartView Tracker

Solution d'audit complète permettant de diagnostiquer les problèmes de système et de sécurité, de recueillir des informations à des fins juridiques ou d'audit, et de générer des rapports pour analyser le trafic réseau. En cas d'attaque ou d'activité réseau suspecte, utilisez SmartView Tracker pour temporairement ou définitivement stopper les connexions provenant d'adresses IP spécifiques.

Alertes

SNMP V1, 2C et 3, Log File, Syslog, Email.

Configuration

SNMP V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, SOAP, API, Console (sélectionnable par l'utilisateur).

Synchronisation horaire

Protocole NTP.

Export des informations de signature en temps réel

L'interface Northbound XML exporte les paramètres comportementaux.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SPÉCIFICATIONS

Modèle DDoS Protector	506	1006	2006	3006	4412	8412	12412
Niveau	Entreprise				Datacenter		
Performance[1]							
Capacité[2]	500 Mbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps	8 Gbps	14 Gbps
Débit[3]	500 Mbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps	8 Gbps	12 Gbps
Sessions simultanées (max)	2 000 000	2 000 000	2 000 000	2 000 000	4 000 000	4 000 000	4 000 000
Taux de prévention d'attaques (paquets par seconde)	1 000 000	1 000 000	1 000 000	1 000 000	10 000 000	10 000 000	10 000 000
Latence	<60 microsecondes						
Signatures en temps réel	Détection et protection contre les attaques en moins de 18 secondes						
Ports d'inspection							
Ethernet 10/100/1000 cuivre	4	4	4	4	8	8	8
GbE (SFP)	2	2	2	2	4	4	4
10 GbE (XFP)	-	-	-	-	4	4	4
Ports d'administration							
Ethernet 10/100/1000 cuivre	2	2	2	2	2	2	2
RS-232	1	1	1	1	1	1	1
Mode de fonctionnement							
Fonctionnement réseau	Transmission L2 transparente						
Modes de déploiement	En ligne, surveillance des ports span, surveillance des ports de copie, out-of-path local, atténuation out-of-path						
Prise en charge des protocoles de Tunneling	VLAN Tagging, L2TP, MPLS, GRE, GTP						
IPv6	Prise en charge des réseaux IPv6 et blocage des attaques IPv6						
Action sur la politique de sécurité	Blocage et signalement, Signalement uniquement						
Actions de blocage	Perte de paquet, remise à zéro (source, destination, les deux), suspension (source, port source, destination, port destination, ou n'importe quelle combinaison), défi/réponse pour les attaques HTTP et DNS						
Haute disponibilité							
Fail-open/Fail-close	Fail-open/fail-close interne pour les ports cuivre; fail-open interne pour les ports SFP, fail-open en option pour les ports SFP[4]				Fail-open/fail-close interne pour les ports cuivre; fail-open interne pour les ports SFP et XFP, fail-open en option pour les ports SFP et XFP[5]		
SKU	CPAP-DP506	CPAP-DP1006	CPAP-DP2006	CPAP-DP3006	CPAP-DP4412	CPAP-DP8412	CPAP-DP12412

[1] Les performances effectives peuvent changer selon la configuration du réseau, le type de trafic, etc.
[2] La capacité représente la transmission de trafic maximale en l'absence de profils de sécurité configurés
[3] Le débit est mesuré avec des protections comportementales et des protections sur signatures, avec le profil de protection eCommerce
[4] Un commutateur fail-open externe fibre avec ports SFP est disponible moyennant un coût supplémentaire
[5] Des commutateurs fail-open externes fibre avec ports SFP ou XFP sont disponibles moyennant un coût supplémentaire

softwareblades™

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Accessoires DDoS Protector	SKU
Module optique 10 Gbps (XFP) monomode LR (fibre)	CPAC-DP-10LR-XFP
Module optique 10 Gbps (XFP) multimode SR (fibre)	CPAC-DP-10SR-XFP
Module optique 1 Gbps monomode ZX (fibre)	CPAC-DP-1ZX-SFP
Module optique 1 Gbps 1000BaseT (cuivre)	CPAC-DP-1C-SFP
Module optique 1 Gbps monomode LX (fibre)	CPAC-DP-1LX-SFP
Module optique 1 Gbps multimode SX (fibre)	CPAC-DP-1SX-SFP
Unité de dérivation externe 10 GbE supportant un (1) segment LR - protection contre les pannes de courant et défauts de liaison - pour DDoS Protector X412	CPAC-DP-1LR-10BP
Châssis de dérivation externe 10 GbE supportant un (1) segment d'interface LR extensible jusqu'à quatre (4) - protection contre les pannes de courant et défauts de liaison - pour DDoS Protector X412	CPAC-DP-4LR-10BP
Module de dérivation externe 10 GbE, segment d'interface LR - protection contre les pannes de courant et défauts de liaison - pour DDoS Protector X412	CPAC-DP-1LR-10BPM
Châssis de dérivation externe 10 GbE supportant un (1) segment d'interface SR extensible jusqu'à quatre (4) - protection contre les pannes de courant et défauts de liaison - pour DDoS Protector X412	CPAC-DP-4SR-10BP
Module de dérivation externe 10 GbE, segment d'interface SR - protection contre les pannes de courant et défauts de liaison - pour DDoS Protector X412	CPAC-DP-1SR-10BPM
Unité de dérivation externe 1 GbE supportant un (1) segment SX - protection contre les pannes de courant et défauts de liaison - pour DDoS Protector X412	CPAC-DP-1SX-1BP
Unité de dérivation externe 1 GbE supportant un (1) segment LX à SX - pour DDoS Protector X412	CPAC-DP-1LX-1BP
Deux châssis d'installation en rack pour commutateurs de dérivation	CPAC-DP-2RM
Double alimentation DC pour DDoS Protector X412	CPAC-DP-2PS-DC
Alimentation DC pour DDoS Protector X412	CPAC-DP-PS-DC

CONTACTS
CHECK POINT

Siège mondial
5 Ha'Solelim Street, Tel Aviv 67897, Israël | Tél. : +972 3 753 4555 | Fax : +972 3 624 1100 | Email : info@checkpoint.com
Siège français
1 place Victor Hugo, Les Renardières, 92400 Courbevoie, France | Tél. : +33 (0)1 55 49 12 00 | Fax : +33 (0)1 55 49 12 01
Email : info_fr@checkpoint.com | www.checkpoint.com

Jeudi 7 juin 2012