5599 - 0670 I https://pccommayorista.com
contacto@pccommayorista.com

AhnLab TrusGuard DPX

TrusGuard DPX(DDoS Prevention eXpress)

Optimum choice for large-scale,
hybrid and advanced DDoS attacks

HIGH CAPACITY ACCURATE SELF-LEARNING PROMPT

Disruptions to internet services can cause major financial losses for companies and chaos for customers. Distributed Denial of Service (DDoS) attacks disrupt services bye flooding a network or server with enough packets or requests to crash it or seriously diminish its capability. Originally, DDoS attacks targeted networks, but like other tools at a hacker's disposal, they are evolving in both quality and quantity.

Attackers can now easily acquire DDoS tools on the black market, and increased curiosity about the amount of damage that can be done by these attacks are making them more popular than ever. Flooding a network with traffic is still the basic element of any DDoS attac,k, but additional methods are being used to increase the effectiveness of these attacks.

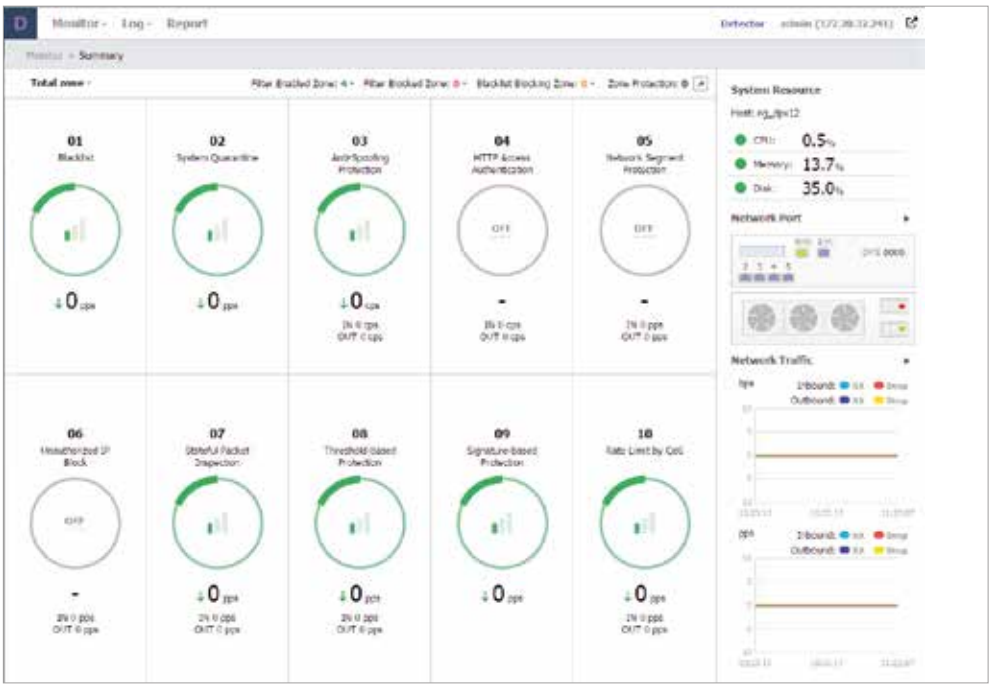
For example, shutting down web or database servers with smaller packets is becoming commonplace, as are hybrid attacks, where small packets that attack web or database servers are hidden inside large packets that attack the network. The evolution of these attacks calls for a progressive solution that not only detects DDoS packets, but also offers a detailed analysis.

AhnLab TrusGuard DPX is the product of years of ongoing research into DDoS attack patterns and expertise in analyzing and detecting malware. It ensures business continuity and resource availability with an inclusive security layer that detects hybrid DDoS attacks and effectively deals with rapidly escalating volumes of traffic.

Disruptions to internet services can cause both financial losses for companies and chaos for customers

AhnLab TrusGuard DPX: The Optimum DDoS Attack Protection System

TrusGuard DPX is designed to defeat today's highly complex and sophisticated DDoS attacks with an intelligent defense strategy. To overcome the limitations of typical DDoS mitigation solutions and network devices such as IPS and firewalls, TrusGuard DPX employs multi-layered mitigation filters to identify and block all types of attacks, while allowing legitimate transactions to pass through without false-positives.



The More, The Better

Recently, various types of traffic hace been used in DDoS attacks, but TrusGuard DPX provides all-inclusive features to block today's complex attacks, regardless of the technologies or methods they employ.

- *Real-time traffic monitoring and automatic self-learning*
- *Protection from network to application (HTTP)*
- *Source IP based protection and spoofed IP protection*
  -TCP Flooding : SYN, SYN-ACK, ACK, Fin, PSH, RST, URG, XMAS
  -Other : UDP, ICMP, IP, Fragments, DNS Query
- *TCP session based protection: TCP Multi-Connection, TCP Established Attack, Low Bandwidth TCP Session Flooding*
- *HTTP based protection: HTTP Get Flooding, HTTP Null Page Flooding, HTTP CC Attack, HTTP Redirect Bypass Flooding, SQL Query Based HTTP Attack*
- *Protection against new and advanced attacks, like RUDY or Slowloris*

Accurate and Discreet

Typical DDoS attack mitigation solutions are struggling to keep up with the emergence of hybrid attacks. These solutions give off false positives routinely, which cause unnecessary interruptions and misdirect important organizational resources. TrusGuard DPX, on the other hand, minimizes service disruptions caused by false-positives, due to accurate detection of malicious TCP and HTTP requests. In addition, TrusGuard DPX protects systems against targeted, small-scale HTTP attacks that slip in below the threshold of typical solutions.

Quantity Means As Much As Quality

The outstanding scalability provided by the clustering capability can simultaneously manage up to 120 Gbps of bandwidth. A list of trusted IP addresses is synchronized with all the other devices within the cluster, to ensure that legitimate traffic can pass, even during a DDoS attack. Clustered devices function seamlessly as a single unit, to respond effectively to volumetric DDoS attacks, while providing scalability to protect all sizes of networks.

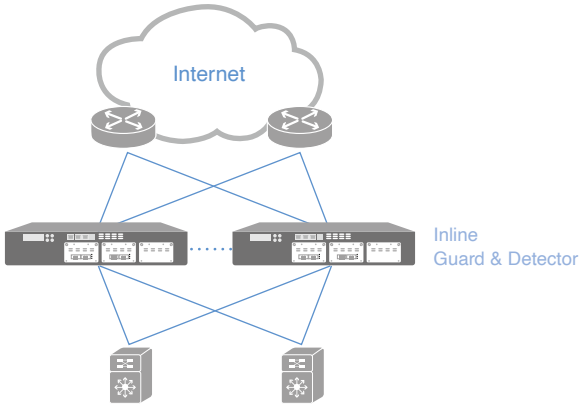
TrusGuard DPX can simultaneously configure up to 328 different zones with unique protection policies for each zone. The protecion polices define filters and traffic thresholds for the zone and allow in-depth protection where needed.

Never Trouble with Deployment

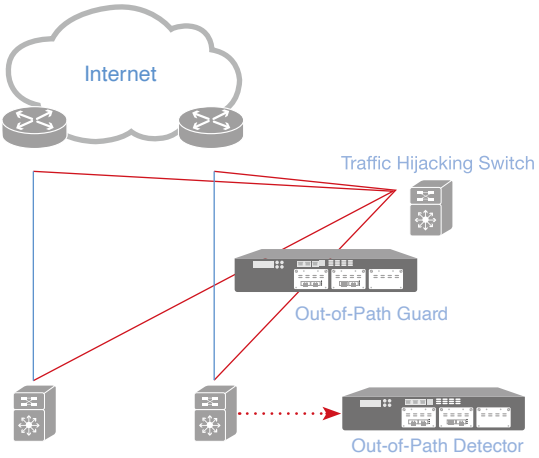
TrusGuard DPX can be deployed inline on a network or as part of an out-of-path topology. Generally, inline deployment is the simplest and least expensive option. By allowing traffic bypasses, TrusGuard DPX provides a safe level of fault tolerance and continues to route traffic, even in the event of a system failure.

An out-of-path topology is most suitable for large-scale networks. When located outside of the network path, TrusGuard DPX ensures fault tolerance and operational stability without affection the traffic flow.

Inline



Out of Path



The Expectations

Organizations need an effective, comprehensive approach to ensure the continuity of services and resources. With its clustering technology and multiple protection layers, TrusGuard DPX effectively mitigates both volumetric and small, targeted attacks. TrusGuard DPX provides the optimal defense for internet resources and services.

- *Maintains Business Continuity: By preventing business disruptions, TrusGuard DPX reduces the risk of lost sales, inconvenienced customers, or damaged reputations.*
- *Reduces Human Resource Costs: With its multi-layered mitigation filters and autonomous learning capability, TrusGuard DPX can reduce the need for hands-on monitoring and changes to configuration settings that are required by typical DDoS mitigation solution.*
- *Monitors 24/7: TrusGuard DPC shows the status of traffic and filters on the network, including system resource usage and network port connections. It can be accessed from mobile devices, which provides unparalleled visibility of network security.*
- *Minimizes aftershocks: As soon as new attack patterns or methods are detected, TrusGuard DPX responds promptly, which minimizes the time and effort required to deal with aftershocks of the incident.*

Performance and Specifications

Model		DPX 6000A	DPX 10000A
Throughput (Max)		10G	40G
CPU		6 Core	28 Core
RAM		64GB	64GB
CFast		8GB	8GB
Interface	1GC	10 (Max 34 ports, Including Mgmt)	2 (Max 34 ports, Including Mgmt)
	1GF	2 (Max 16 ports)	0 (Max 16 ports)
	10GF	0 (Max 16 ports)	4 (Max 16 ports)
Bypass		Support	Support
Power		550W Redundant	550W Redundant

About AhnLab

AhnLab creates agile, integrated internet security solutions for corporate organizations. Founded in 1995, AhnLab, a global leader in security, delivers comprehensive protection for networks, transactions, and essential services. AhnLab delivers best-of-breed threat prevention that scales easily for high-speed networks, by combining cloud analysis with endpoint and server resources. AhnLab's multidimensional approach combines with exceptional service to create truly global protection against attacks that evade traditional security defenses. That's why more than 25,000 organizations rely on AhnLab's award-winning products and services to make the internet safe and reliable for their business operations.

AhnLab

More security,
More freedom

PC com Mayorista

¡Contáctanos, juntos queremos hacer negocio contigo!

Av. Prol. División del Norte # 4318
Col. Nueva Oriental Coapa, Tlalpan C.P. 14300

(55) 5599-0670
https://pccommayorista.com
contacto@pccommayorista.com

AhnLab