EXHIBIT A

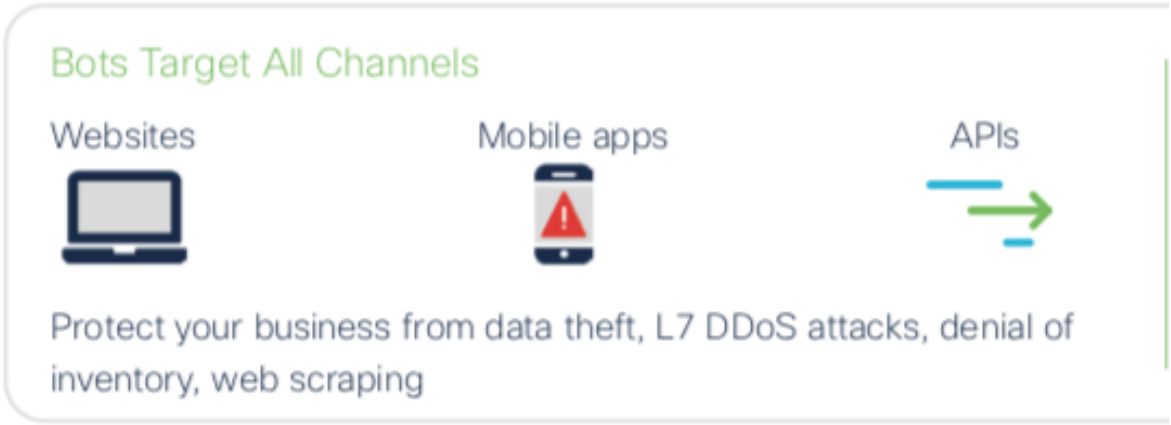
Exhibit A -- CHART FOR U.S. PATENT NO. 7,302,708 ("'708 Patent")

Accused Instrumentalities: Cisco's products, including at least each of the following security appliances and software infringe at least Claims 1-2 and 9-11: Cisco Secure Web Application Firewall (WAF), Secure Application Delivery Controller Alteon, and Virtual ADC (vADC), Cisco Firepower 4100 series and 9300 appliances, Cisco SecureX, Cisco Firepower version 8.13 and newer. The infringement chart below is based on the Cisco's Secure Web Application Firewall ("Cisco WAF") running on Cisco appliances such as Cisco Secure Application Delivery Controller, which is exemplary of the infringement of the '708 Patent.

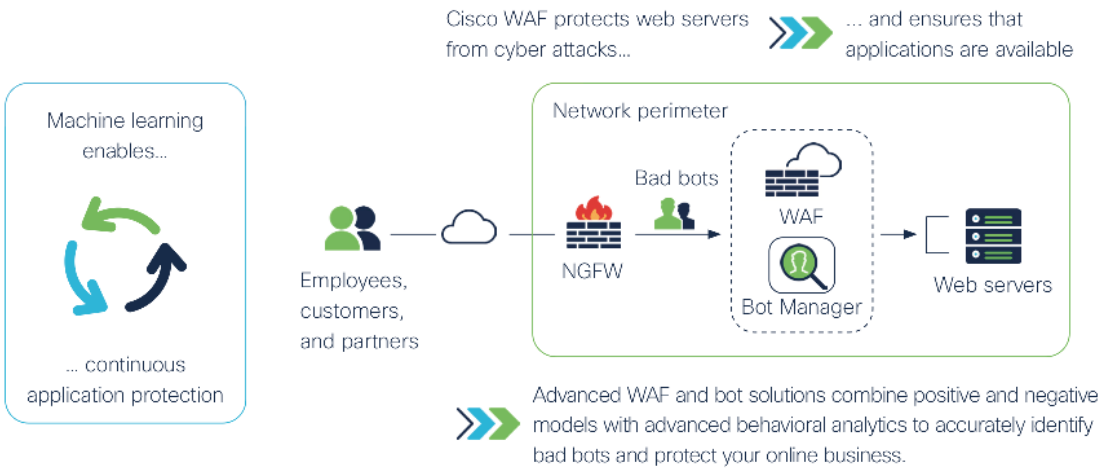
Claims	Cisco WAF
[1pre] A method for secure access to a computer system, comprising the steps of:	To the extent the preamble is deemed limiting, Cisco WAF performs a method for secure access to a computer system. Cisco® Secure Web Application Firewall (WAF) and bot protection defends your online presence and ensures that website, mobile applications, and APIs are secure, protected, and "always on." Bots Target All Channels Websites Mobile apps APIs Protect your business from data theft, L7 DDoS attacks, denial of inventory, web scraping 80% of organizations can't distinguish good bots from malicious bots Advanced WAF and bot management solutions ensure reliable, secure delivery of web and mobile applications while minimizing costs by enabling security policies to easily be deployed across multicloud environments. Advanced bot management uses machine learning and adaptive security to accurately distinguish good bots from malicious bots, ensuring that your network and applications are available to legitimate users. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

	Cisco and Radware have an OEM partnership Through its partnership with Radware, Cisco sells Cisco Secure DDoS, Cisco Advanced WAF and Bot Management solutions, Cisco SSL inspection solutions, and Cisco Secure ADC *See, e.g.,* Cisco Secure DDoS available at https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-ddos-services.pdf Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html Zero-day DDoS protection Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry. *See e.g.,* https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

	Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations. The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection types include the following: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP floods—which includes UDP Fragmentation Flood • ICMP flood • IGMP flood The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.
[1a] receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;	Cisco WAF receives in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function. Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity. *See, e.g.,* https://www.radware.com/partners/cisco-waf-bot/



See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 1.



See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 2.

	The first step to securing your assets against a DDoS attack is to know which assets are most at risk. Begin by listing all external-facing assets that could be attacked. This list should include both physical and virtual assets: • Physical locations and offices • Data centers • Servers • Applications • IP addresses and subnets • Domains, subdomains, and specific FQDNs. *See e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/ddos-5steps-protect-organization-so.html

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 146.

	A Signature Protection profile contains one or more rules for the network segment that you want to protect. Each rule defines a query on the Signatures database. Radware DefensePro DDoS Mitigation activates protections from the Signatures database that matches the set of rules. The user-defined profile is updated each time you download an updated Signatures database. To configure Signature Protection profiles, Signature Protection must be enabled and global DoS Shield parameters must be configured. For more information, see Configuring Global Signature Protection, page 104 and Configuring Global DoS Shield Protection, page 105. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Signature Protection profiles. Each rule in the profile can include one or more entries from the various attribute types. Rules define a query on the Signatures database based on the following logic: • Values from the same type are combined with logical OR. • Values from different types are combined with logical AND. The rules are combined in the profile with a logical OR. The relationship inside a signature between all filters is a logical AND. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 150.

	Connection Limit profiles defend against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection Limit profiles. Connection Limit profiles contain attack definitions for groups of TCP or UDP application ports. Radware DefensePro DDoS Mitigation counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client plus server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the specified threshold, any session/connection over the threshold is dropped, unless the action mode defined for this attack is Report Only. Recommended settings for policies that include Connection Limit profiles: • Configure policies containing Connection Limit profiles using Networks only with source = Any, the public network, and destination = Protected Network. You can define segments using VLAN tags and physical ports. • It is not recommended to define networks when the Source and Destination are set to Any. • Policies containing Connection Limit profiles can be configured with Direction set to either One Way or Two Way. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 171.

Parameter	Description
Protection Name	A descriptive name for easy identification when configuring and reporting.
Protection ID	(Read-only) The ID number assigned to the Connection Limit protection.
Application Port Group Name	The Layer 4 port or class object that defines the application you want to protect. To specify any port, the field may contain the value **any** or be empty. **Note:** You can click the adjacent button to open the dialog box in which you can add a class.
Protocol	The Layer 4 protocol of the application you want to protect. Values: TCP, UDP Default: TCP
Number of New Connections	The maximum number of new TCP connections, or new UDP sessions, per second, allowed for each source, destination or source-and- destination pair. All additional sessions are dropped. When the threshold is reached, attacks are identified, and Radware DefensePro DDoS Mitigation generates a security event. Values: 0–100,000,000 Default: 50
Tracking Type	The counting rule for tracking sessions. Values: • Source Count—Sessions are counted per source IP address. • Destination Count—Sessions are counted per destination IP address. • Source and Destination Count—Sessions are counted per source IP and destination IP address combination. Default: Source Count

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 173.

Parameter	Description
Action	The action when an attack is detected. Values: • Drop—The packet is discarded. • Report-only—The packet is forwarded to the destination IP address. Default: Drop

	See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 174. • **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN Floods, TCP Floods, UDP floods, ICMP and IGMP floods. • **SYN-flood Protection**—Protects against any type of SYN flood attack using SYN cookies. A SYN flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, you configure SYN Protection as a Network Protection to allow easier protection of multiple network elements. • **DNS Protection**—Protects against zero-day DNS query floods. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure. It is therefore crucial to protect the DNS infrastructure from these threats. DNS query floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNS servers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 36.

	resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a recursive flood or random-subdomains flood, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate ("good") subdomains and attack ("bad") subdomains appear as legitimate queries to the DNS server. In DefensePro 8.x versions 8.13 and later, the DNS Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/or targeted domain, and allow only the "good" queries to the protected DNS servers. • **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection includes DoS Shield protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect. • **Packet-Anomaly Protection**. • **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs. • **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 37.

Managing Network Classes

In Radware DefensePro DDoS Mitigation for Cisco Firepower, you can use Network classes in Network Protection policies to match source or destination traffic. A Network class is identified by a name and defined by a network address and IPv4 mask or IPv6 prefix.

To configure a Network class

1. In the Configuration perspective, select **Classes > Networks**.
2. To add or modify a Network class, do one of the following:
   - To add a class, click the (Add) button.
   - To edit a class, double-click the entry in the table.
3. Configure the Network class parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 137.

Parameter	Description
Network Name	The name of the Network class. The network name is case-sensitive. The network name cannot be an IP address. Maximum characters: 64
Entry Type	Specifies whether the network is defined by a subnet and mask, or by an IP range. Value: IP Mask
Network Type	Values: IPv4, IPv6
Network Address	The network address.
Prefix	The mask of the subnet, which you can enter in either of the following ways: • A subnet mask in dotted decimal notation—for example, 255.0.0.0or 255.255.0.0. • An IP prefix, that is, the number of mask bits—for example, 8or 16.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 138.

	You can define network segments using Context Group classes. Use them to classify traffic in security policies. Each Radware DefensePro DDoS Mitigation instance supports a maximum 64 Context Group classes. Each Context Group class can contain a maximum 32 discrete tags and 32 ranges. That is, in effect, each DefensePro device supports up to 64^2 definitions. **To configure a Context Group class** 1. In the Configuration perspective, select **Classes > Context Groups**. 2. Do one of the following: — To add an entry, click the (Add) button. — To edit an entry, double-click the entry in the table. 3. Configure the parameters, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 138.

Table 69: Context Groups Class Parameters

Parameter	Description
Context Group Name	The name of the group. Maximum characters: 19
Group Mode	Values: • Discrete—An individual Context Group, as defined in the interface parameters of the device. • Range—A group of sequential Context Group numbers, as defined in the interface parameters of the device. Default: Discrete
Tag (This parameter is available only for the **Discrete** mode.)	The Context Group number. Values: 0–4095
Range From (This parameter is available only for the **Range** mode.)	The first Context Group in the range. Values: 0–4095 **Note:** You cannot modify the value after creating the Context Group.
Range To (This parameter is available only for the **Range** mode.)	The last Context Group in the range. Values: 0–4095

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 139.

Application classes are groups of Layer-4 ports for UDP and TCP traffic. Each class is identified by its unique name, and you can define multiple Layer-4 ports in a single class. You cannot modify the predefined (**System Defined**) application classes for standard applications; however, you can add entries for the class. You can add and modify user-defined (**User Defined**) classes to the Application Port Group table.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 139.

Table 70: Application Class Parameters

Parameter	Description
Ports Group Name	The name of the Application Port Group. To associate a number of ranges with the same port group, use the same name for all the ranges that you want to include in the group. Each range appears as a separate row with the same name in the Application Port Group table.
Type of Entry	(Read-only) Values: System Defined, User Defined
From L4 Port	The first port in the range.
To L4 Port	The last port in the range. To define a group with a single port, set the same value for the **From L4 Port** and **To L4 Port** parameters.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 140.

	Managing MAC Address Classes MAC groups identify traffic whose source or destination is a transparent network device. **To configure a MAC address class** 1. In the Configuration perspective, select **Classes > Addresses**. 2. To add or modify a MAC address class, do one of the following: — To add a class, click the (Add) button. — To edit a class, double-click the entry in the table. 3. Enter a name for the MAC group and the MAC address associated with the group, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 140.
[1b] determining if said access request completes a prohibited temporal access pattern for said entity;	Cisco WAF determines if said access request completes a prohibited temporal access pattern for said entity. Advanced WAF and bot solutions combine positive and negative models with advanced behavioral analytics to accurately identify bad bots and protect your online business. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

Advanced WAF + Bot Manager = Better Together

Security Capability	Bot Manager	Traditional WAFS	WAF + Bot
Protection from simple bots	Yes	Yes	Yes
Fingerprinting of malicious devices	Yes	Yes	Yes
Mitigation of dynamic IP and headless browser attacks	Yes	Limited	Yes
Detection of sophisticated bot attacks	Yes	No	Yes
Risk of blocking legitimate users (false positives)	Very low	High	Very Low
Collective bot intelligence (IPs, fingerprints, behavioral patterns)	Yes	No	Yes
Customized actions against suspicious bot types	Yes	No	Yes

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

- **Intent encoding:** The visitor's journey through a web property is captured through signals such as mouse or keystroke interactions, URL and referrer traversals, and time stamps. These signals are encoded using a proprietary, deep neural network architecture into an intent encoding-based, fixed-length representation. The encoding network jointly achieves two objectives: to be able to represent the anomalous characteristics of completely new categories of bots and to provide greater weight to behavioral characteristics that differ between humans and bots.

See, e.g., https://blog.radware.com/security/2019/06/idba-a-patented-bot-detection-technology/

Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html

Zero-day DDoS protection

Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry.

See e.g., https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations.

The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.

Network-flood protection types include the following:

- TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood
- UDP floods—which includes UDP Fragmentation Flood
- ICMP flood
- IGMP flood

The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.

Enable Traffic Statistics Sampling	Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the BDoS footprint. When the parameter is enabled, and the BDoS module is trying to generate a real-time signature and there is a high rate of traffic, the device evaluates only a portion of the traffic. The BDoS module tunes the sampling factor automatically, according to the traffic rate. The BDoS module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS). Default: Enabled **Note:** For best performance, Radware recommends that the parameter be Enabled.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 112.

- **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN Floods, TCP Floods, UDP floods, ICMP and IGMP floods.
- **SYN-flood Protection**—Protects against any type of SYN flood attack using SYN cookies. A SYN flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, you configure SYN Protection as a Network Protection to allow easier protection of multiple network elements.
- **DNS Protection**—Protects against zero-day DNS query floods. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure. It is therefore crucial to protect the DNS infrastructure from these threats. DNS query floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNS servers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 36.

	resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a recursive flood or random-subdomains flood, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate ("good") subdomains and attack ("bad") subdomains appear as legitimate queries to the DNS server. In DefensePro 8.x versions 8.13 and later, the DNS Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/or targeted domain, and allow only the "good" queries to the protected DNS servers. • **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection includes DoS Shield protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect. • **Packet-Anomaly Protection**. • **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs. • **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 37.
[1c] comparing a minimum access level established for said first base node to said predetermined access level;	Cisco WAF compares a minimum access level established for said first base node to said predetermined access level. Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity. *See, e.g.,* https://www.radware.com/partners/cisco-waf-bot/

	Key benefits **Consistent security policy** • Easily deploy across multicloud to reduce costs and security risks **Comprehensive OWASP coverage** • Protection beyond the OWASP Top 10 • Positive and negative models provide complete protection with minimum false positives • Advanced security controls inspect and protect APIs from attack and manipulation **Advanced bot protection** • Accurately identifies advanced human-like bots that evade fingerprinting technologies • Distinguishes good bots from malicious bots with minimum false positives **Auto discovery** • Continuously scans apps for changes and automatically optimizes security policies *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 146.

Action	The default action for all attacks under this policy. Values: • Block and Report—The malicious traffic is terminated and a security event is generated and logged. • Report Only—The malicious traffic is forwarded to its destination and a security event is generated and logged. Default: Block and Report **Note:** Signature-specific actions override the default action for the policy.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 147.

A Signature Protection profile contains one or more rules for the network segment that you want to protect. Each rule defines a query on the Signatures database. Radware DefensePro DDoS Mitigation activates protections from the Signatures database that matches the set of rules. The user-defined profile is updated each time you download an updated Signatures database.

To configure Signature Protection profiles, Signature Protection must be enabled and global DoS Shield parameters must be configured. For more information, see Configuring Global Signature Protection, page 104 and Configuring Global DoS Shield Protection, page 105.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Signature Protection profiles.

Each rule in the profile can include one or more entries from the various attribute types. Rules define a query on the Signatures database based on the following logic:

- Values from the same type are combined with logical OR.
- Values from different types are combined with logical AND.

The rules are combined in the profile with a logical OR.

The relationship inside a signature between all filters is a logical AND.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 150.

	Connection Limit profiles defend against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection Limit profiles. Connection Limit profiles contain attack definitions for groups of TCP or UDP application ports. Radware DefensePro DDoS Mitigation counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client plus server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the specified threshold, any session/connection over the threshold is dropped, unless the action mode defined for this attack is Report Only. Recommended settings for policies that include Connection Limit profiles: • Configure policies containing Connection Limit profiles using Networks only with source = Any, the public network, and destination = Protected Network. You can define segments using VLAN tags and physical ports. • It is not recommended to define networks when the Source and Destination are set to Any. • Policies containing Connection Limit profiles can be configured with Direction set to either One Way or Two Way. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 171.

Parameter	Description
Protection Name	A descriptive name for easy identification when configuring and reporting.
Protection ID	(Read-only) The ID number assigned to the Connection Limit protection.
Application Port Group Name	The Layer 4 port or class object that defines the application you want to protect. To specify any port, the field may contain the value **any** or be empty. **Note:** You can click the adjacent button to open the dialog box in which you can add a class.
Protocol	The Layer 4 protocol of the application you want to protect. Values: TCP, UDP Default: TCP
Number of New Connections	The maximum number of new TCP connections, or new UDP sessions, per second, allowed for each source, destination or source-and- destination pair. All additional sessions are dropped. When the threshold is reached, attacks are identified, and Radware DefensePro DDoS Mitigation generates a security event. Values: 0–100,000,000 Default: 50
Tracking Type	The counting rule for tracking sessions. Values: • Source Count—Sessions are counted per source IP address. • Destination Count—Sessions are counted per destination IP address. • Source and Destination Count—Sessions are counted per source IP and destination IP address combination. Default: Source Count

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 173.

Parameter	Description
Action	The action when an attack is detected. Values: • Drop—The packet is discarded. • Report-only—The packet is forwarded to the destination IP address. Default: Drop

	See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 174. **Configuring Global Signature Protection** Signature Protection is enabled by default. When DefensePro detects a signature in a TCP session, DefensePro drops all packets of the session. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 108.
[1d] granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and	Cisco WAF grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level. Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity. *See, e.g.,* https://www.radware.com/partners/cisco-waf-bot/

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 146.

Action	The default action for all attacks under this policy. Values: • Block and Report—The malicious traffic is terminated and a security event is generated and logged. • Report Only—The malicious traffic is forwarded to its destination and a security event is generated and logged. Default: Block and Report **Note:** Signature-specific actions override the default action for the policy.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 147.

Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html

Zero-day DDoS protection

Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry.

See e.g., https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations.

The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.

Network-flood protection types include the following:

- TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood
- UDP floods—which includes UDP Fragmentation Flood
- ICMP flood
- IGMP flood

The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.

Enable Traffic Statistics Sampling	Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the BDoS footprint. When the parameter is enabled, and the BDoS module is trying to generate a real-time signature and there is a high rate of traffic, the device evaluates only a portion of the traffic. The BDoS module tunes the sampling factor automatically, according to the traffic rate. The BDoS module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS). Default: Enabled **Note:** For best performance, Radware recommends that the parameter be Enabled.

	See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 112. • **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN Floods, TCP Floods, UDP floods, ICMP and IGMP floods. • **SYN-flood Protection**—Protects against any type of SYN flood attack using SYN cookies. A SYN flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, you configure SYN Protection as a Network Protection to allow easier protection of multiple network elements. • **DNS Protection**—Protects against zero-day DNS query floods. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure. It is therefore crucial to protect the DNS infrastructure from these threats. DNS query floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNS servers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 36.

	resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a recursive flood or random-subdomains flood, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate ("good") subdomains and attack ("bad") subdomains appear as legitimate queries to the DNS server. In DefensePro 8.x versions 8.13 and later, the DNS Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/or targeted domain, and allow only the "good" queries to the protected DNS servers. • **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection includes DoS Shield protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect. • **Packet-Anomaly Protection**. • **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs. • **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 37.

	You can define network segments using Context Group classes. Use them to classify traffic in security policies. Each Radware DefensePro DDoS Mitigation instance supports a maximum 64 Context Group classes. Each Context Group class can contain a maximum 32 discrete tags and 32 ranges. That is, in effect, each DefensePro device supports up to 64^2 definitions. **To configure a Context Group class** 1. In the Configuration perspective, select **Classes > Context Groups**. 2. Do one of the following: — To add an entry, click the (Add) button. — To edit an entry, double-click the entry in the table. 3. Configure the parameters, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 138. Application classes are groups of Layer-4 ports for UDP and TCP traffic. Each class is identified by its unique name, and you can define multiple Layer-4 ports in a single class. You cannot modify the predefined (**System Defined**) application classes for standard applications; however, you can add entries for the class. You can add and modify user-defined (**User Defined**) classes to the Application Port Group table. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 139.

Managing MAC Address Classes

MAC groups identify traffic whose source or destination is a transparent network device.

To configure a MAC address class

1. In the Configuration perspective, select **Classes > Addresses**.
2. To add or modify a MAC address class, do one of the following:
   - To add a class, click the (Add) button.
   - To edit a class, double-click the entry in the table.
3. Enter a name for the MAC group and the MAC address associated with the group, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 140.

Black List	You can define DefensePro Black List rules to block certain traffic. Black List rules are used as exceptions for DefensePro security policies (see Security policy). You can define Black List rules for a single IP address or using a Network class.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 323.

[1e] denying said request if said access request completes a prohibited	Cisco WAF denying said request if said access request completes a prohibited temporal access pattern for said entity.

temporal access pattern for said entity.	Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity. *See, e.g.,* https://www.radware.com/partners/cisco-waf-bot/ 3. **Adaptive learning:** The adaptive-learning module collects the predictions made by the different models and takes actions on bots based on these predictions. In many cases, the action involves presenting a challenge to the visitor like a CAPTCHA or an SMS OTP that provides a feedback mechanism (i.e., CAPTCHA solved). This feedback is incorporated to improvise the decision-making process. Decisions to be made can be broadly categorized into two types of tasks. - **Determining thresholds:** The thresholds to be chosen for anomaly scores and classification probabilities are determined through adaptive threshold control techniques. - **Identifying bot clusters:** Selective incremental blacklisting is performed on suspicious clusters. The suspicion scores associated with the clusters (obtained from the collusion detector module) are used to set prior bias. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 6. Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations. The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection types include the following: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP floods—which includes UDP Fragmentation Flood • ICMP flood • IGMP flood The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 146.

Action	The default action for all attacks under this policy. Values: • Block and Report—The malicious traffic is terminated and a security event is generated and logged. • Report Only—The malicious traffic is forwarded to its destination and a security event is generated and logged. Default: Block and Report **Note:** Signature-specific actions override the default action for the policy.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 147.

- The action that Radware DefensePro DDoS Mitigation applies when it detects an attack on the matching network segment. The action defines the protection profiles that Radware DefensePro DDoS Mitigation applies to the network segment, and whether to block the malicious traffic. Radware DefensePro DDoS Mitigation always reports malicious traffic.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 144.

Enable Traffic Statistics Sampling	Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the BDoS footprint. When the parameter is enabled, and the BDoS module is trying to generate a real-time signature and there is a high rate of traffic, the device evaluates only a portion of the traffic. The BDoS module tunes the sampling factor automatically, according to the traffic rate. The BDoS module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS). Default: Enabled **Note:** For best performance, Radware recommends that the parameter be Enabled.

	See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 112. **Managing Network Classes** In Radware DefensePro DDoS Mitigation for Cisco Firepower, you can use Network classes in Network Protection policies to match source or destination traffic. A Network class is identified by a name and defined by a network address and IPv4 mask or IPv6 prefix. **To configure a Network class** 1. In the Configuration perspective, select **Classes > Networks**. 2. To add or modify a Network class, do one of the following: — To add a class, click the (Add) button. — To edit a class, double-click the entry in the table. 3. Configure the Network class parameters, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 137.
2. The method according to claim 1, further comprising the step of denying said request if said minimum access level for said first	Cisco WAF performs the method as recited in claim1 and comprises the step of denying said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

base node exceeds said predetermined access level for said entity.	**3. Adaptive learning:** The adaptive-learning module collects the predictions made by the different models and takes actions on bots based on these predictions. In many cases, the action involves presenting a challenge to the visitor like a CAPTCHA or an SMS OTP that provides a feedback mechanism (i.e., CAPTCHA solved). This feedback is incorporated to improvise the decision-making process. Decisions to be made can be broadly categorized into two types of tasks. ▸ **Determining thresholds:** The thresholds to be chosen for anomaly scores and classification probabilities are determined through adaptive threshold control techniques. ▸ **Identifying bot clusters:** Selective incremental blacklisting is performed on suspicious clusters. The suspicion scores associated with the clusters (obtained from the collusion detector module) are used to set prior bias. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 6. Advanced WAF + Bot Manager = Better Together Security Capability | Bot Manager | Traditional WAFS | WAF + Bot Protection from simple bots | Yes | Yes | Yes Fingerprinting of malicious devices | Yes | Yes | Yes Mitigation of dynamic IP and headless browser attacks | Yes | Limited | Yes Detection of sophisticated bot attacks | Yes | No | Yes Risk of blocking legitimate users (false positives) | Very low | High | Very Low Collective bot intelligence (IPs, fingerprints, behavioral patterns) | Yes | No | Yes Customized actions against suspicious bot types | Yes | No | Yes *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

WAFs protect websites from application vulnerability exploits like SQL injection, cross-site scripting (XSS), cross-site request forgery, session hijacking, and other web attacks. WAFs typically feature basic bot mitigation capabilities that block bots based only on IPs and fingerprinting.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 3.

Negative Security Models

- Used in most WAF solutions
- Block known threats via signatures and rules
- Cannot protect from unknown threats: zero-day attacks

Positive Security Models

- Learn and define what constitutes legitimate traffic
- Block unauthorized access and actions
- Uniquely protect against zero-day and unknown vulnerabilities

© 2021 Cisco and/or its affiliates. All rights reserved.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 2.

A Signature Protection profile contains one or more rules for the network segment that you want to protect. Each rule defines a query on the Signatures database. Radware DefensePro DDoS Mitigation activates protections from the Signatures database that matches the set of rules. The user-defined profile is updated each time you download an updated Signatures database.

To configure Signature Protection profiles, Signature Protection must be enabled and global DoS Shield parameters must be configured. For more information, see Configuring Global Signature Protection, page 104 and Configuring Global DoS Shield Protection, page 105.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Signature Protection profiles.

Each rule in the profile can include one or more entries from the various attribute types. Rules define a query on the Signatures database based on the following logic:

- Values from the same type are combined with logical OR.
- Values from different types are combined with logical AND.

The rules are combined in the profile with a logical OR.

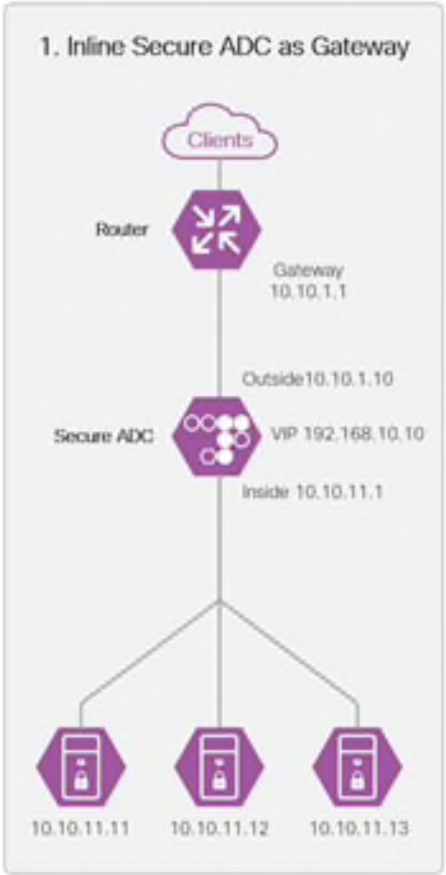
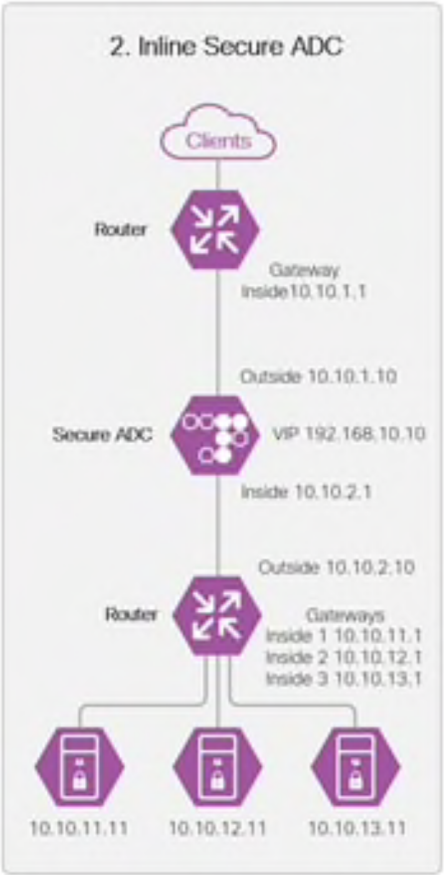
The relationship inside a signature between all filters is a logical AND.

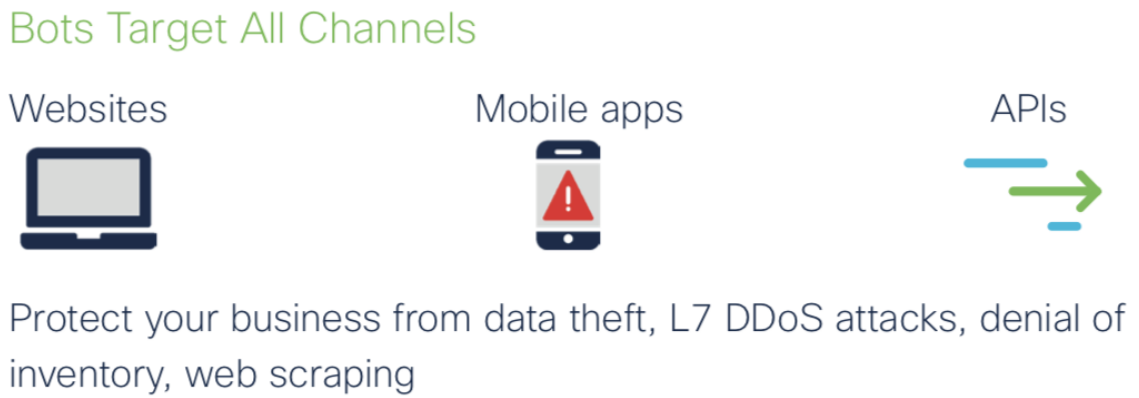
	See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 150. Connection Limit profiles defend against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection Limit profiles. Connection Limit profiles contain attack definitions for groups of TCP or UDP application ports. Radware DefensePro DDoS Mitigation counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client plus server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the specified threshold, any session/connection over the threshold is dropped, unless the action mode defined for this attack is Report Only. Recommended settings for policies that include Connection Limit profiles: • Configure policies containing Connection Limit profiles using Networks only with source = Any, the public network, and destination = Protected Network. You can define segments using VLAN tags and physical ports. • It is not recommended to define networks when the Source and Destination are set to Any. • Policies containing Connection Limit profiles can be configured with Direction set to either One Way or Two Way. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 171.

Parameter	Description
Protection Name	A descriptive name for easy identification when configuring and reporting.
Protection ID	(Read-only) The ID number assigned to the Connection Limit protection.
Application Port Group Name	The Layer 4 port or class object that defines the application you want to protect. To specify any port, the field may contain the value **any** or be empty. **Note:** You can click the adjacent button to open the dialog box in which you can add a class.
Protocol	The Layer 4 protocol of the application you want to protect. Values: TCP, UDP Default: TCP
Number of New Connections	The maximum number of new TCP connections, or new UDP sessions, per second, allowed for each source, destination or source-and- destination pair. All additional sessions are dropped. When the threshold is reached, attacks are identified, and Radware DefensePro DDoS Mitigation generates a security event. Values: 0–100,000,000 Default: 50
Tracking Type	The counting rule for tracking sessions. Values: • Source Count—Sessions are counted per source IP address. • Destination Count—Sessions are counted per destination IP address. • Source and Destination Count—Sessions are counted per source IP and destination IP address combination. Default: Source Count

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 173.

Parameter	Description
Action	The action when an attack is detected. Values: • Drop—The packet is discarded. • Report-only—The packet is forwarded to the destination IP address. Default: Drop

	See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 174.
9. A method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy, comprising the steps of:	Cisco WAF performs a method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy.  

	See, e.g., https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/sdc-aci-radware.html  https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 1.

Alteon is a combination of hardware platforms and software, which deliver a rich set of application delivery capabilities with unmatched performance. It offers a complete set of Layer 4-7 services to ensure the availability, performance, and security of mission-critical applications in on-premises and cloud data centers. These extend to traffic redirection, content modification, persistency, redundancy, advanced health monitoring, and bandwidth management that optimizes the delivery of mission-critical applications.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/secure-adc-alteon-ds.pdf at p. 4.

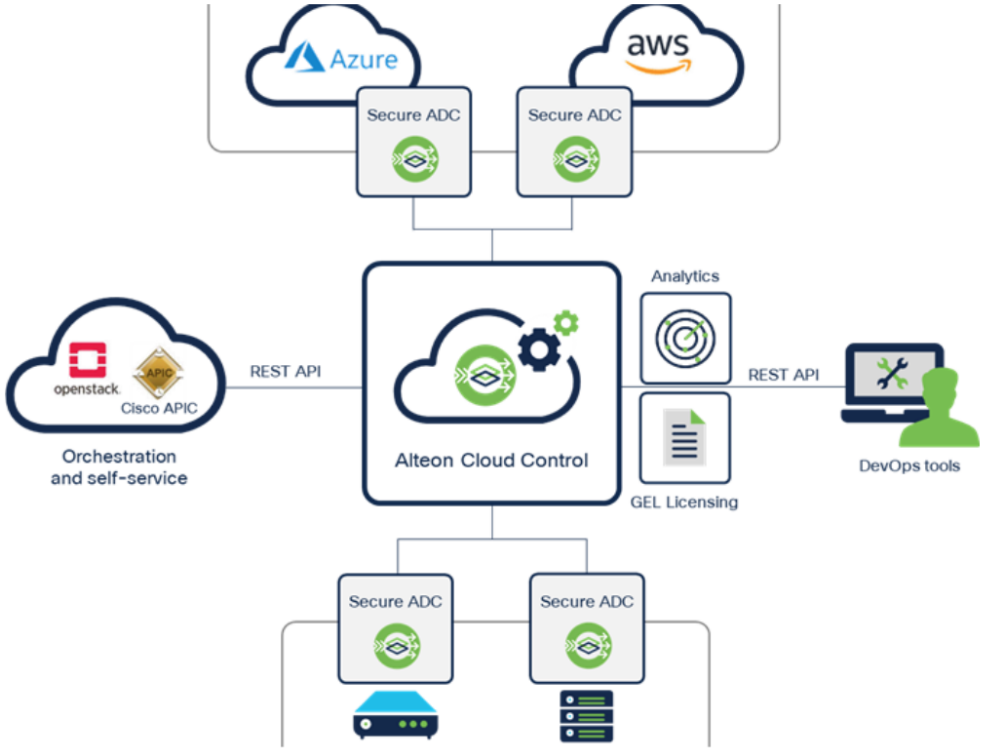
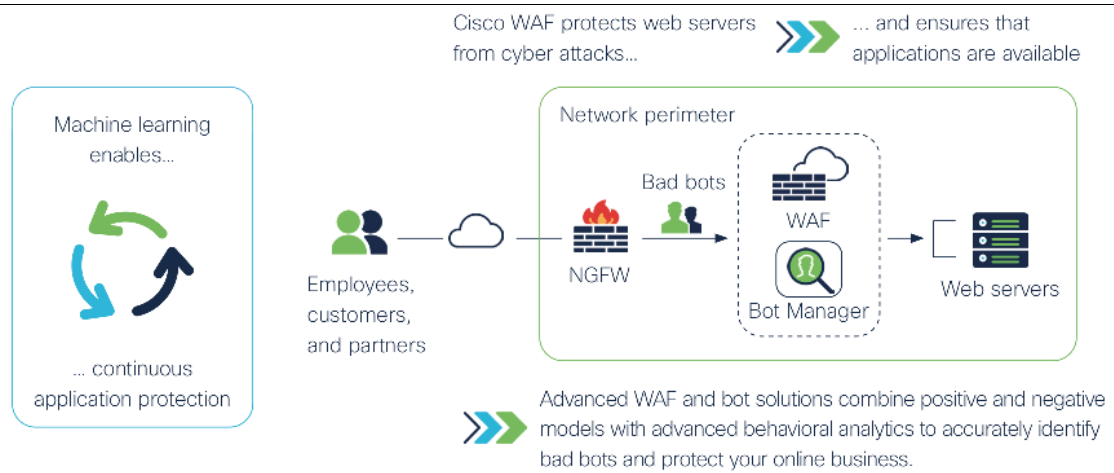


Figure 2. Secure ADC multicloud solution architecture

https://blogs.cisco.com/datacenter/cisco-secure-adc-and-secure-adc-multicloud-application-performance-in-a-cloud-first-world



See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 2.

Cisco and Radware have an OEM partnership

Through its partnership with Radware, Cisco sells Cisco Secure DDoS, Cisco Advanced WAF and Bot Management solutions, Cisco SSL inspection solutions, and Cisco Secure ADC

See, e.g., Cisco Secure DDoS available at https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-ddos-services.pdf

	Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html Zero-day DDoS protection Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry. *See e.g.,* https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

	The first step to securing your assets against a DDoS attack is to know which assets are most at risk. Begin by listing all external-facing assets that could be attacked. This list should include both physical and virtual assets: • Physical locations and offices • Data centers • Servers • Applications • IP addresses and subnets • Domains, subdomains, and specific FQDNs. *See e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/ddos-5steps-protect-organization-so.html
receiving in said computer system a request from an entity with a predetermined access level for access to a first base node;	Cisco WAF receives in said computer system a request from an entity with a predetermined access level for access to a first base node. *See supra* claim element [1a].
determining if said access request completes a prohibited temporal access pattern for said entity;	Cisco WAF determines if said access request completes a prohibited temporal access pattern for said entity. *See supra* claim element [1b].

comparing a minimum access level established for said first base node to said predetermined access level;	Cisco WAF compares a minimum access level established for said first base node to said predetermined access level. *See supra* claim element [1c].
granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and	Cisco WAF grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level. *See supra* claim element [1d].
denying said request if said access request completes a prohibited temporal access pattern for said entity.	Cisco WAF denies said request if said access request completes a prohibited temporal access pattern for said entity. *See supra* claim element [1e].
10. A secure computer system comprising:	Cisco Secure Application Delivery Controller (ADC) includes a secure computer system.

Alteon is a combination of hardware platforms and software, which deliver a rich set of application delivery capabilities with unmatched performance. It offers a complete set of Layer 4-7 services to ensure the availability, performance, and security of mission-critical applications in on-premises and cloud data centers. These extend to traffic redirection, content modification, persistency, redundancy, advanced health monitoring, and bandwidth management that optimizes the delivery of mission-critical applications.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/secure-adc-alteon-ds.pdf at p. 4.

The integration of advanced web application firewall (WAF) capabilities, such as a unique out-of-path WAF deployment mode and auto-policy generation features, enable risk-free implementation. In addition, full instance isolation and resource reservation ensures ADC resources. Even when WAF policies are updated, there is no impact on application availability and performance. This results in secured web application with guaranteed SLAs.

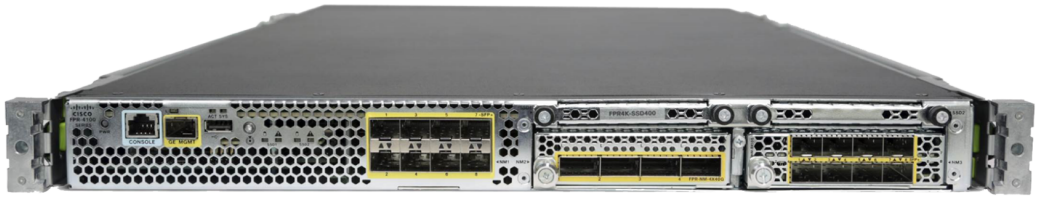
See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/secure-adc-alteon-ds.pdf at p. 6.

Cisco and Radware have an OEM partnership

Through its partnership with Radware, Cisco sells Cisco Secure DDoS, Cisco Advanced WAF and Bot Management solutions, Cisco SSL inspection solutions, and Cisco Secure ADC

See, e.g., Cisco Secure DDoS available at https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-ddos-services.pdf

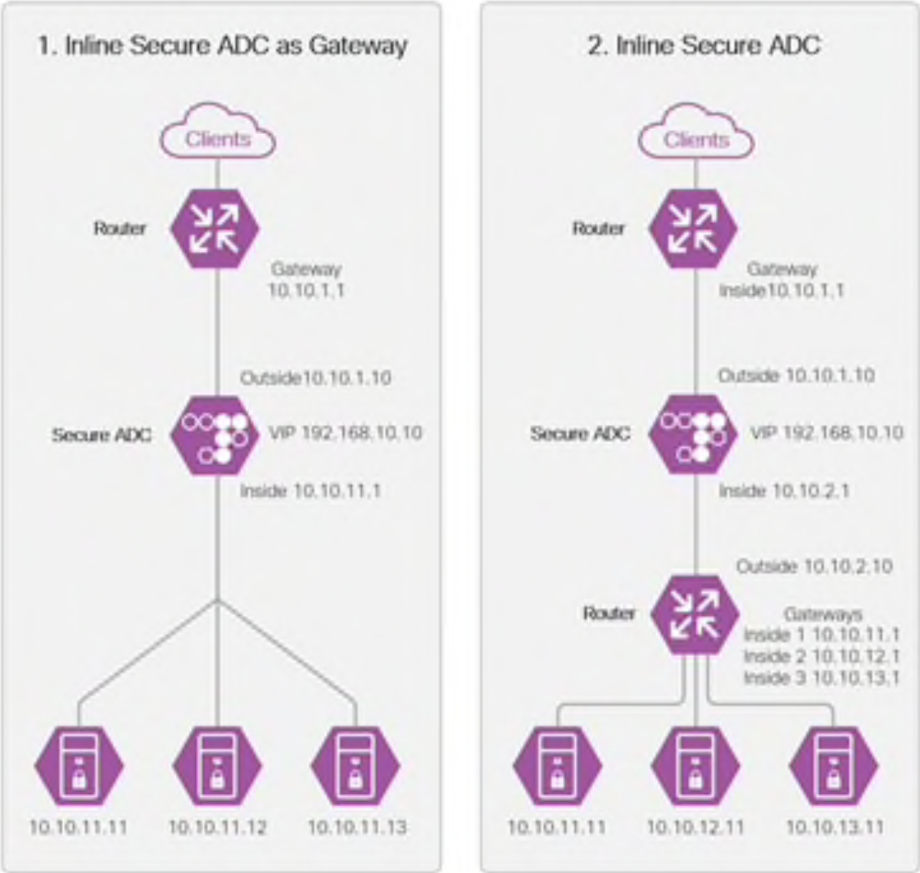
Model overview

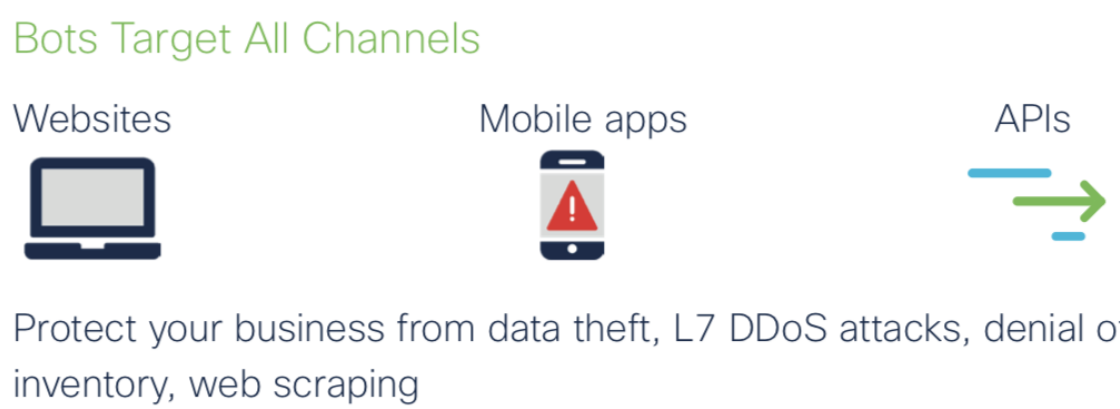


Cisco Firepower 4100 Series summary:

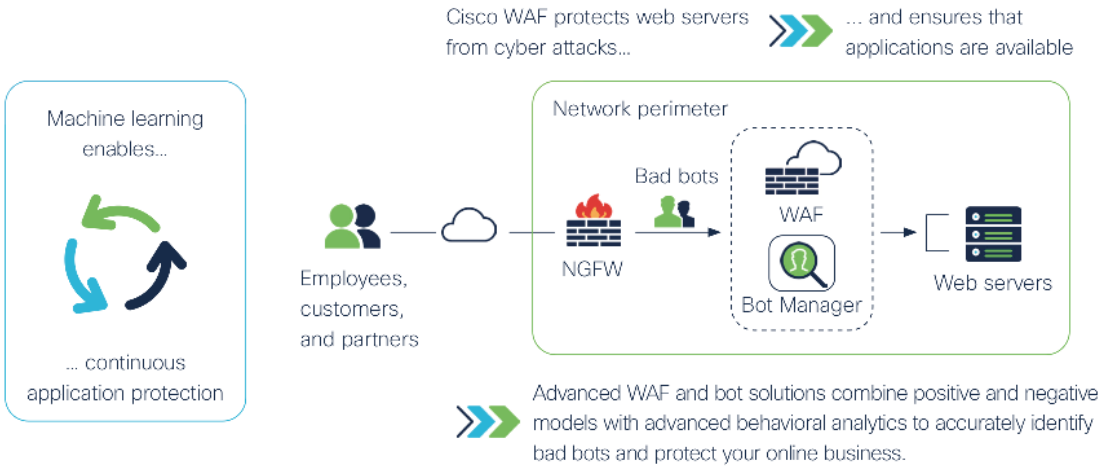
Model	Firewall	NGFW	IPS	Interfaces	Optional Interfaces
FPR-4110	35G	15.5G	16.5G	8 x SFP+ on-chassis	2 x NM's: 1/10/40G, FTW

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html

a plurality of logical base nodes representing at least one of an information type and a computer system function;	Cisco ADC includes a plurality of logical base nodes representing at least one of an information type and a computer system function.  *See, e.g.,* https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/sdc-aci-radware.html

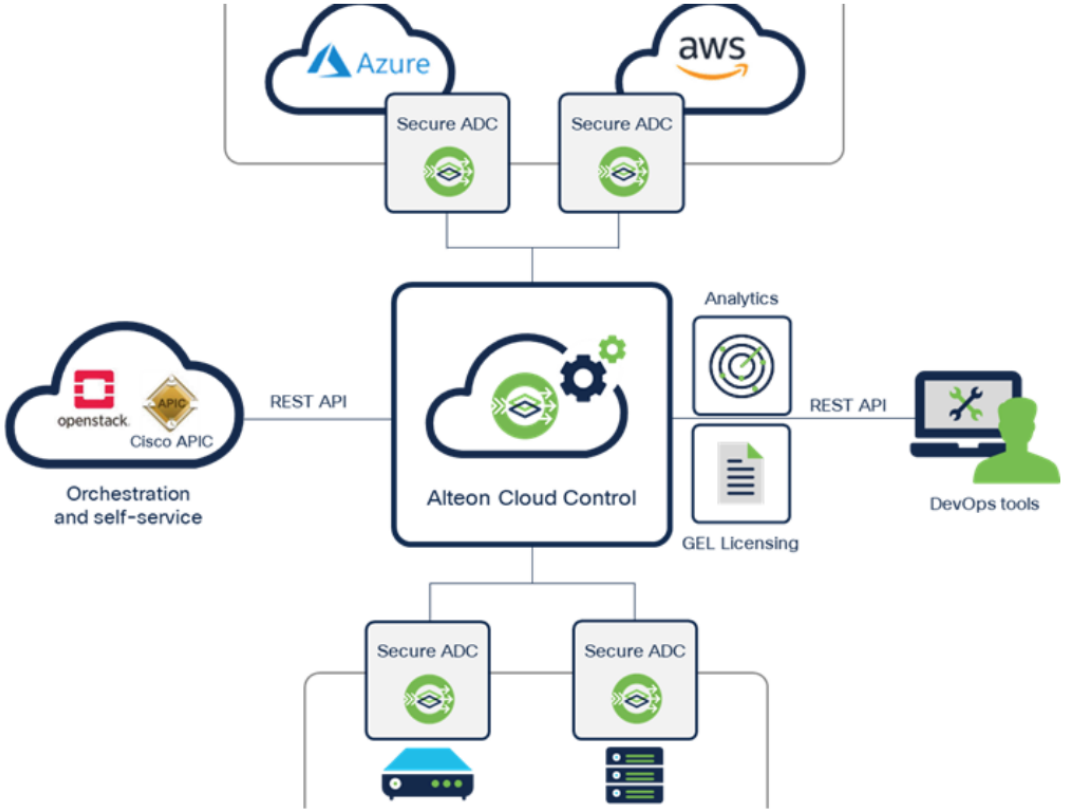


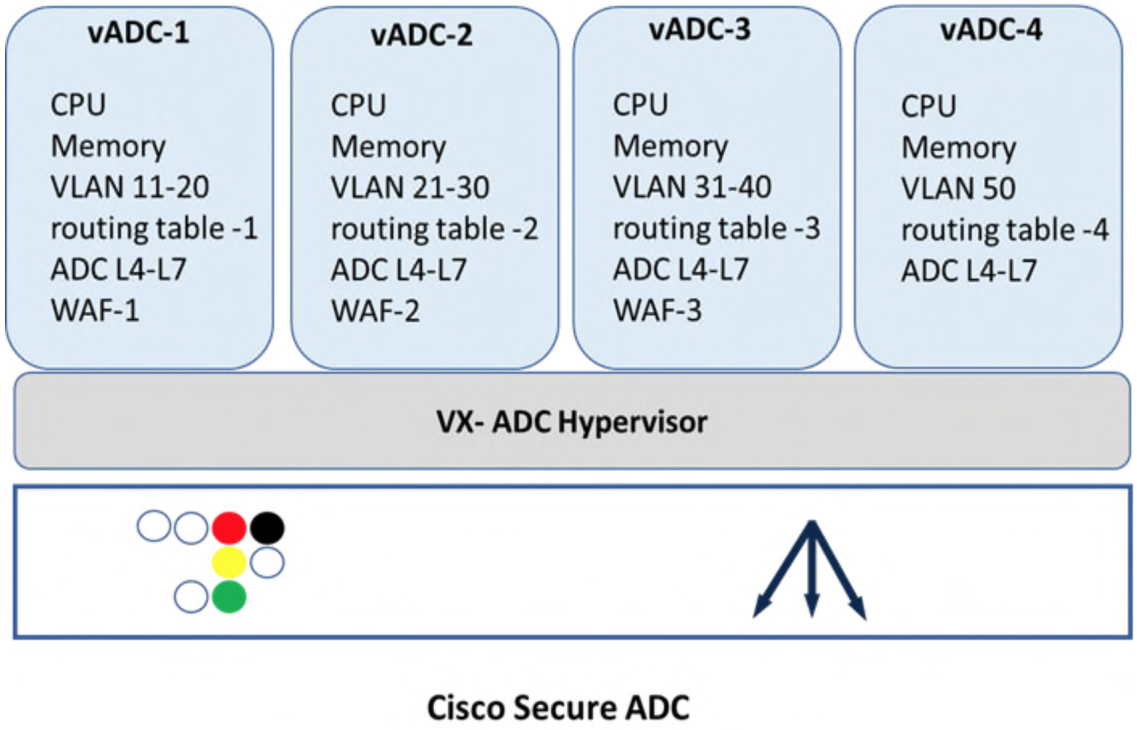
https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 1.



See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 2.

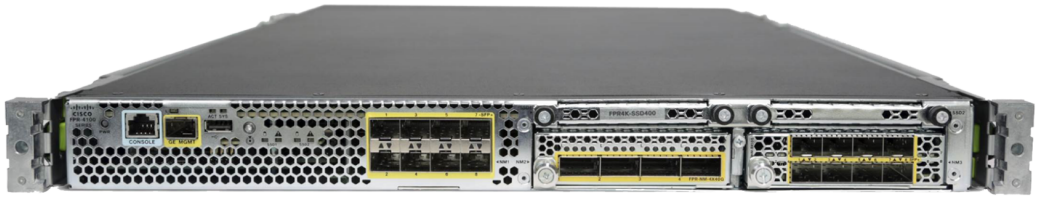
	The first step to securing your assets against a DDoS attack is to know which assets are most at risk. Begin by listing all external-facing assets that could be attacked. This list should include both physical and virtual assets: • Physical locations and offices • Data centers • Servers • Applications • IP addresses and subnets • Domains, subdomains, and specific FQDNs. *See e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/ddos-5steps-protect-organization-so.html

	 Figure 2. Secure ADC multicloud solution architecture *See, e.g.,* https://blogs.cisco.com/datacenter/cisco-secure-adc-and-secure-adc-multicloud-application-performance-in-a-cloud-first-world
a computer system interface capable of receiving a request from an entity with a predetermined	Cisco ADC includes a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node.

access level for access to a first base node;	 *See e.g.,* https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/aci-secure-adc-design-guide.html

	 Alteon is a combination of hardware platforms and software, which deliver a rich set of application delivery capabilities with unmatched performance. It offers a complete set of Layer 4-7 services to ensure the availability, performance, and security of mission-critical applications in on-premises and cloud data centers. These extend to traffic redirection, content modification, persistency, redundancy, advanced health monitoring, and bandwidth management that optimizes the delivery of mission-critical applications. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/secure-adc-alteon-ds.pdf at p. 4.

Model overview



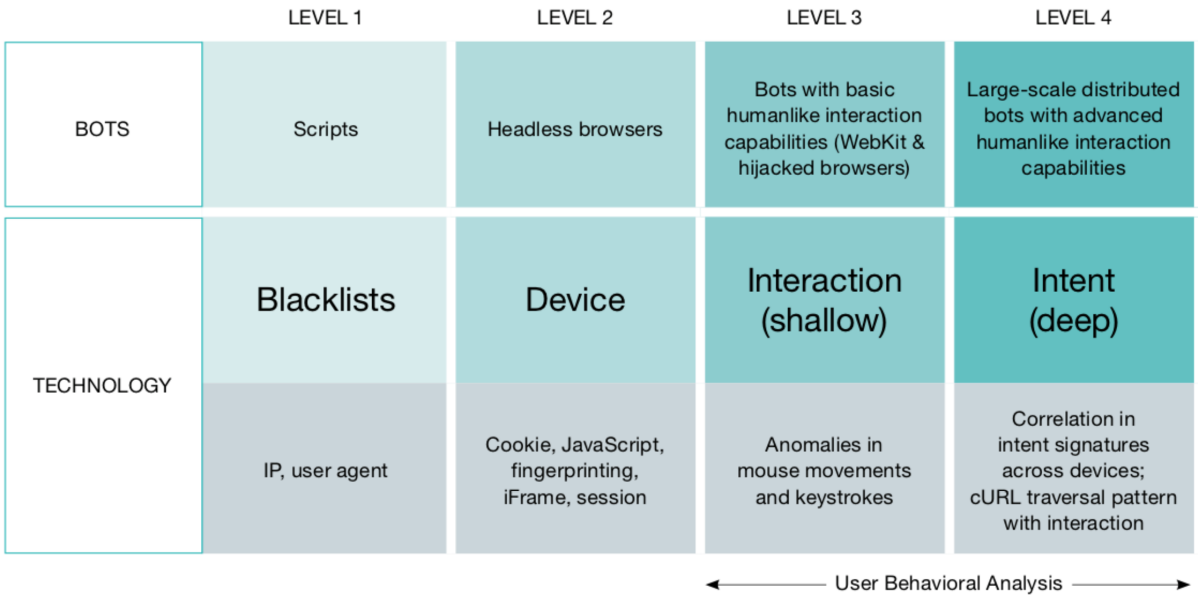
Cisco Firepower 4100 Series summary:

Model	Firewall	NGFW	IPS	Interfaces	Optional Interfaces
FPR-4110	35G	15.5G	16.5G	8 x SFP+ on-chassis	2 x NM's: 1/10/40G, FTW

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html

Maximum number of interfaces	Up to 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules; up to 24 x 1 Gigabit Ethernet ports(SFP) with network modules and fixed ports
Integrated network management ports	1 Gigabit Ethernet Supports 1-G fiber or copper SFPs

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html

a temporal access table;	Cisco ADC includes a temporal access table. IDBA is a major step forward in bot detection technology because it performs behavioral analysis at a higher level of abstraction of intent, unlike the commonly used, shallow interaction-based behavioral analysis. For example, account takeover is an example of an intent, while "mouse pointer moving in a straight line" is an example of an interaction. Capturing intent enables IDBA to provide significantly higher levels of accuracy to detect advanced bots. IDBA is designed to leverage the latest developments in deep learning. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 3.  *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 4.

	As mentioned earlier, shallow interaction-level behavioral analysis is insufficient to detect advanced Level 4 bots. This points to the need to perform behavioral analysis at a deeper level: The visitor's journey through the web property needs to be analyzed in addition to the interaction-level characteristics, such as mouse movements. This includes additional signals such as the sequence of URLs traversed, the referrers used and the time spent on each page. Using this richer behavioral information, the incoming visitor can be classified as a human or bot. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 5. **2. Intent analysis:** Here, the intent encoding of the user is analyzed using multiple machine learning modules in parallel. A combination of supervised and unsupervised learning-based modules are used to detect both known and unknown patterns. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 6. Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html

Zero-day DDoS protection

Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry.

See e.g., https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations.

The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.

Network-flood protection types include the following:

- TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood
- UDP floods—which includes UDP Fragmentation Flood
- ICMP flood
- IGMP flood

The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.

processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and	Cisco ADC includes processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level. Advanced WAF and bot solutions combine positive and negative models with advanced behavioral analytics to accurately identify bad bots and protect your online business. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf **Advanced WAF + Bot Manager = Better Together** Security Capability / Bot Manager / Traditional WAFS / WAF + Bot Protection from simple bots / Yes / Yes / Yes Fingerprinting of malicious devices / Yes / Yes / Yes Mitigation of dynamic IP and headless browser attacks / Yes / Limited / Yes Detection of sophisticated bot attacks / Yes / No / Yes Risk of blocking legitimate users (false positives) / Very low / High / Very Low Collective bot intelligence (IPs, fingerprints, behavioral patterns) / Yes / No / Yes Customized actions against suspicious bot types / Yes / No / Yes *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

	• **Intent encoding:** The visitor's journey through a web property is captured through signals such as mouse or keystroke interactions, URL and referrer traversals, and time stamps. These signals are encoded using a proprietary, deep neural network architecture into an intent encoding-based, fixed-length representation. The encoding network jointly achieves two objectives: to be able to represent the anomalous characteristics of completely new categories of bots and to provide greater weight to behavioral characteristics that differ between humans and bots. *See, e.g.,* https://blog.radware.com/security/2019/06/idba-a-patented-bot-detection-technology/ Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity. *See, e.g.,* https://www.radware.com/partners/cisco-waf-bot/

Key benefits

Consistent security policy

- Easily deploy across multicloud to reduce costs and security risks

Comprehensive OWASP coverage

- Protection beyond the OWASP Top 10
- Positive and negative models provide complete protection with minimum false positives
- Advanced security controls inspect and protect APIs from attack and manipulation

Advanced bot protection

- Accurately identifies advanced human-like bots that evade fingerprinting technologies
- Distinguishes good bots from malicious bots with minimum false positives

Auto discovery

- Continuously scans apps for changes and automatically optimizes security policies

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer.

See, e.g., https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html

Zero-day DDoS protection

Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry.

See e.g., https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations.

The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.

Network-flood protection types include the following:

- TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood
- UDP floods—which includes UDP Fragmentation Flood
- ICMP flood
- IGMP flood

The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.

Enable Traffic Statistics Sampling	Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the BDoS footprint. When the parameter is enabled, and the BDoS module is trying to generate a real-time signature and there is a high rate of traffic, the device evaluates only a portion of the traffic. The BDoS module tunes the sampling factor automatically, according to the traffic rate. The BDoS module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS). Default: Enabled **Note:** For best performance, Radware recommends that the parameter be Enabled.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 112.

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 146.

Action	The default action for all attacks under this policy. Values: • Block and Report—The malicious traffic is terminated and a security event is generated and logged. • Report Only—The malicious traffic is forwarded to its destination and a security event is generated and logged. Default: Block and Report **Note:** Signature-specific actions override the default action for the policy.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 147.

A Signature Protection profile contains one or more rules for the network segment that you want to protect. Each rule defines a query on the Signatures database. Radware DefensePro DDoS Mitigation activates protections from the Signatures database that matches the set of rules. The user-defined profile is updated each time you download an updated Signatures database.

To configure Signature Protection profiles, Signature Protection must be enabled and global DoS Shield parameters must be configured. For more information, see Configuring Global Signature Protection, page 104 and Configuring Global DoS Shield Protection, page 105.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Signature Protection profiles.

Each rule in the profile can include one or more entries from the various attribute types. Rules define a query on the Signatures database based on the following logic:

- Values from the same type are combined with logical OR.
- Values from different types are combined with logical AND.

The rules are combined in the profile with a logical OR.

The relationship inside a signature between all filters is a logical AND.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 150.

	Connection Limit profiles defend against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection Limit profiles. Connection Limit profiles contain attack definitions for groups of TCP or UDP application ports. Radware DefensePro DDoS Mitigation counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client plus server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the specified threshold, any session/connection over the threshold is dropped, unless the action mode defined for this attack is Report Only. Recommended settings for policies that include Connection Limit profiles: • Configure policies containing Connection Limit profiles using Networks only with source = Any, the public network, and destination = Protected Network. You can define segments using VLAN tags and physical ports. • It is not recommended to define networks when the Source and Destination are set to Any. • Policies containing Connection Limit profiles can be configured with Direction set to either One Way or Two Way. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 171.

Parameter	Description
Protection Name	A descriptive name for easy identification when configuring and reporting.
Protection ID	(Read-only) The ID number assigned to the Connection Limit protection.
Application Port Group Name	The Layer 4 port or class object that defines the application you want to protect. To specify any port, the field may contain the value **any** or be empty. **Note:** You can click the adjacent button to open the dialog box in which you can add a class.
Protocol	The Layer 4 protocol of the application you want to protect. Values: TCP, UDP Default: TCP
Number of New Connections	The maximum number of new TCP connections, or new UDP sessions, per second, allowed for each source, destination or source-and- destination pair. All additional sessions are dropped. When the threshold is reached, attacks are identified, and Radware DefensePro DDoS Mitigation generates a security event. Values: 0–100,000,000 Default: 50
Tracking Type	The counting rule for tracking sessions. Values: • Source Count—Sessions are counted per source IP address. • Destination Count—Sessions are counted per destination IP address. • Source and Destination Count—Sessions are counted per source IP and destination IP address combination. Default: Source Count

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 173.

Parameter	Description
Action	The action when an attack is detected. Values: • Drop—The packet is discarded. • Report-only—The packet is forwarded to the destination IP address. Default: Drop

	See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 174. • **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN Floods, TCP Floods, UDP floods, ICMP and IGMP floods. • **SYN-flood Protection**—Protects against any type of SYN flood attack using SYN cookies. A SYN flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, you configure SYN Protection as a Network Protection to allow easier protection of multiple network elements. • **DNS Protection**—Protects against zero-day DNS query floods. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure. It is therefore crucial to protect the DNS infrastructure from these threats. DNS query floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNS servers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 36.

	resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a recursive flood or random-subdomains flood, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate ("good") subdomains and attack ("bad") subdomains appear as legitimate queries to the DNS server. In DefensePro 8.x versions 8.13 and later, the DNS Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/or targeted domain, and allow only the "good" queries to the protected DNS servers. • **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection includes DoS Shield protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect. • **Packet-Anomaly Protection**. • **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs. • **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 37.

Managing Network Classes

In Radware DefensePro DDoS Mitigation for Cisco Firepower, you can use Network classes in Network Protection policies to match source or destination traffic. A Network class is identified by a name and defined by a network address and IPv4 mask or IPv6 prefix.

To configure a Network class

1. In the Configuration perspective, select **Classes > Networks**.
2. To add or modify a Network class, do one of the following:
   - To add a class, click the (Add) button.
   - To edit a class, double-click the entry in the table.
3. Configure the Network class parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 137.

Parameter	Description
Network Name	The name of the Network class. The network name is case-sensitive. The network name cannot be an IP address. Maximum characters: 64
Entry Type	Specifies whether the network is defined by a subnet and mask, or by an IP range. Value: IP Mask
Network Type	Values: IPv4, IPv6
Network Address	The network address.
Prefix	The mask of the subnet, which you can enter in either of the following ways: • A subnet mask in dotted decimal notation—for example, 255.0.0.0or 255.255.0.0. • An IP prefix, that is, the number of mask bits—for example, 8or 16.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 138.

	You can define network segments using Context Group classes. Use them to classify traffic in security policies. Each Radware DefensePro DDoS Mitigation instance supports a maximum 64 Context Group classes. Each Context Group class can contain a maximum 32 discrete tags and 32 ranges. That is, in effect, each DefensePro device supports up to 64^2 definitions. **To configure a Context Group class** 1. In the Configuration perspective, select **Classes > Context Groups**. 2. Do one of the following: — To add an entry, click the (Add) button. — To edit an entry, double-click the entry in the table. 3. Configure the parameters, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 138.

Table 69: Context Groups Class Parameters

Parameter	Description
Context Group Name	The name of the group. Maximum characters: 19
Group Mode	Values: • Discrete—An individual Context Group, as defined in the interface parameters of the device. • Range—A group of sequential Context Group numbers, as defined in the interface parameters of the device. Default: Discrete
Tag (This parameter is available only for the **Discrete** mode.)	The Context Group number. Values: 0–4095
Range From (This parameter is available only for the **Range** mode.)	The first Context Group in the range. Values: 0–4095 **Note:** You cannot modify the value after creating the Context Group.
Range To (This parameter is available only for the **Range** mode.)	The last Context Group in the range. Values: 0–4095

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 139.

Application classes are groups of Layer-4 ports for UDP and TCP traffic. Each class is identified by its unique name, and you can define multiple Layer-4 ports in a single class. You cannot modify the predefined (**System Defined**) application classes for standard applications; however, you can add entries for the class. You can add and modify user-defined (**User Defined**) classes to the Application Port Group table.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 139.

Table 70: Application Class Parameters

Parameter	Description
Ports Group Name	The name of the Application Port Group. To associate a number of ranges with the same port group, use the same name for all the ranges that you want to include in the group. Each range appears as a separate row with the same name in the Application Port Group table.
Type of Entry	(Read-only) Values: System Defined, User Defined
From L4 Port	The first port in the range.
To L4 Port	The last port in the range. To define a group with a single port, set the same value for the **From L4 Port** and **To L4 Port** parameters.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 140.

	Managing MAC Address Classes MAC groups identify traffic whose source or destination is a transparent network device. **To configure a MAC address class** 1. In the Configuration perspective, select **Classes > Addresses**. 2. To add or modify a MAC address class, do one of the following: — To add a class, click the (Add) button. — To edit a class, double-click the entry in the table. 3. Enter a name for the MAC group and the MAC address associated with the group, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 140.
wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a	In Cisco ADC, said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level. Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware - leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity. *See, e.g.,* https://www.radware.com/partners/cisco-waf-bot/

prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.	**3. Adaptive learning:** The adaptive-learning module collects the predictions made by the different models and takes actions on bots based on these predictions. In many cases, the action involves presenting a challenge to the visitor like a CAPTCHA or an SMS OTP that provides a feedback mechanism (i.e., CAPTCHA solved). This feedback is incorporated to improvise the decision-making process. Decisions to be made can be broadly categorized into two types of tasks. ▸ **Determining thresholds:** The thresholds to be chosen for anomaly scores and classification probabilities are determined through adaptive threshold control techniques. ▸ **Identifying bot clusters:** Selective incremental blacklisting is performed on suspicious clusters. The suspicion scores associated with the clusters (obtained from the collusion detector module) are used to set prior bias. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 6. Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations. The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection types include the following: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP floods—which includes UDP Fragmentation Flood • ICMP flood • IGMP flood The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 111.

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. **Note:** You can click the adjacent button to open the dialog box in which you can add and modify profiles.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 146.

Action	The default action for all attacks under this policy. Values: • Block and Report—The malicious traffic is terminated and a security event is generated and logged. • Report Only—The malicious traffic is forwarded to its destination and a security event is generated and logged. Default: Block and Report **Note:** Signature-specific actions override the default action for the policy.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 147.

- The action that Radware DefensePro DDoS Mitigation applies when it detects an attack on the matching network segment. The action defines the protection profiles that Radware DefensePro DDoS Mitigation applies to the network segment, and whether to block the malicious traffic. Radware DefensePro DDoS Mitigation always reports malicious traffic.

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 144.

Enable Traffic Statistics Sampling	Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the BDoS footprint. When the parameter is enabled, and the BDoS module is trying to generate a real-time signature and there is a high rate of traffic, the device evaluates only a portion of the traffic. The BDoS module tunes the sampling factor automatically, according to the traffic rate. The BDoS module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS). Default: Enabled **Note:** For best performance, Radware recommends that the parameter be Enabled.

	See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 112. Cisco® DDoS protection solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks. Cisco DDoS mitigation solutions protect against encrypted SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks. Multiple deployment options, including cloud-based, CPE, and hybrid deployment options, offer solutions for every customer. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html Zero-day DDoS protection Adaptive, behavioral-based algorithms block never-before-seen attacks with the lowest false positive rate in the industry. *See e.g.,* https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html#~why-cisco

- **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN Floods, TCP Floods, UDP floods, ICMP and IGMP floods.
- **SYN-flood Protection**—Protects against any type of SYN flood attack using SYN cookies. A SYN flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, you configure SYN Protection as a Network Protection to allow easier protection of multiple network elements.
- **DNS Protection**—Protects against zero-day DNS query floods. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure. It is therefore crucial to protect the DNS infrastructure from these threats. DNS query floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNS servers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 36.

resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a recursive flood or random-subdomains flood, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate ("good") subdomains and attack ("bad") subdomains appear as legitimate queries to the DNS server. In DefensePro 8.x versions 8.13 and later, the DNS Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/or targeted domain, and allow only the "good" queries to the protected DNS servers.

- **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection includes DoS Shield protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect.
- **Packet-Anomaly Protection**.
- **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs.
- **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 37.

	You can define network segments using Context Group classes. Use them to classify traffic in security policies. Each Radware DefensePro DDoS Mitigation instance supports a maximum 64 Context Group classes. Each Context Group class can contain a maximum 32 discrete tags and 32 ranges. That is, in effect, each DefensePro device supports up to 64^2 definitions. **To configure a Context Group class** 1. In the Configuration perspective, select **Classes > Context Groups**. 2. Do one of the following: — To add an entry, click the (Add) button. — To edit an entry, double-click the entry in the table. 3. Configure the parameters, and then, click **Submit**. 4. To activate your configuration changes on the device, click **Update Policies** ( ). *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 138. Application classes are groups of Layer-4 ports for UDP and TCP traffic. Each class is identified by its unique name, and you can define multiple Layer-4 ports in a single class. You cannot modify the predefined (**System Defined**) application classes for standard applications; however, you can add entries for the class. You can add and modify user-defined (**User Defined**) classes to the Application Port Group table. *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 139.

Managing MAC Address Classes

MAC groups identify traffic whose source or destination is a transparent network device.

To configure a MAC address class

1. In the Configuration perspective, select **Classes > Addresses**.
2. To add or modify a MAC address class, do one of the following:
   - To add a class, click the (Add) button.
   - To edit a class, double-click the entry in the table.
3. Enter a name for the MAC group and the MAC address associated with the group, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 140.

Black List	You can define DefensePro Black List rules to block certain traffic. Black List rules are used as exceptions for DefensePro security policies (see Security policy). You can define Black List rules for a single IP address or using a Network class.

See e.g., Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 323.

11. The secure computer system according to claim 10, wherein said processing means denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.	Cisco ADC includes system as recited in claim 10, wherein said processing means denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity. **3. Adaptive learning:** The adaptive-learning module collects the predictions made by the different models and takes actions on bots based on these predictions. In many cases, the action involves presenting a challenge to the visitor like a CAPTCHA or an SMS OTP that provides a feedback mechanism (i.e., CAPTCHA solved). This feedback is incorporated to improvise the decision-making process. Decisions to be made can be broadly categorized into two types of tasks. - **Determining thresholds:** The thresholds to be chosen for anomaly scores and classification probabilities are determined through adaptive threshold control techniques. - **Identifying bot clusters:** Selective incremental blacklisting is performed on suspicious clusters. The suspicion scores associated with the clusters (obtained from the collusion detector module) are used to set prior bias. *See, e.g.,* https://www.radwarebotmanager.com/web/wp-content/uploads/IDBA_WP.pdf at p. 6. Advanced WAF + Bot Manager = Better Together Security Capability / Bot Manager / Traditional WAFS / WAF + Bot Protection from simple bots / Yes / Yes / Yes Fingerprinting of malicious devices / Yes / Yes / Yes Mitigation of dynamic IP and headless browser attacks / Yes / Limited / Yes Detection of sophisticated bot attacks / Yes / No / Yes Risk of blocking legitimate users (false positives) / Very low / High / Very Low Collective bot intelligence (IPs, fingerprints, behavioral patterns) / Yes / No / Yes Customized actions against suspicious bot types / Yes / No / Yes *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf

	WAFs protect websites from application vulnerability exploits like SQL injection, cross-site scripting (XSS), cross-site request forgery, session hijacking, and other web attacks. WAFs typically feature basic bot mitigation capabilities that block bots based only on IPs and fingerprinting. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 3. **Negative Security Models** • Used in most WAF solutions • Block known threats via signatures and rules • Cannot protect from unknown threats: zero-day attacks **Positive Security Models** • Learn and define what constitutes legitimate traffic • Block unauthorized access and actions • Uniquely protect against zero-day and unknown vulnerabilities © 2021 Cisco and/or its affiliates. All rights reserved. *See, e.g.,* https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf at p. 2.

	A Signature Protection profile contains one or more rules for the network segment that you want to protect. Each rule defines a query on the Signatures database. Radware DefensePro DDoS Mitigation activates protections from the Signatures database that matches the set of rules. The user-defined profile is updated each time you download an updated Signatures database. To configure Signature Protection profiles, Signature Protection must be enabled and global DoS Shield parameters must be configured. For more information, see Configuring Global Signature Protection, page 104 and Configuring Global DoS Shield Protection, page 105. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Signature Protection profiles. Each rule in the profile can include one or more entries from the various attribute types. Rules define a query on the Signatures database based on the following logic: • Values from the same type are combined with logical OR. • Values from different types are combined with logical AND. The rules are combined in the profile with a logical OR. The relationship inside a signature between all filters is a logical AND. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 150.

	Connection Limit profiles defend against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks. In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection Limit profiles. Connection Limit profiles contain attack definitions for groups of TCP or UDP application ports. Radware DefensePro DDoS Mitigation counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client plus server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the specified threshold, any session/connection over the threshold is dropped, unless the action mode defined for this attack is Report Only. Recommended settings for policies that include Connection Limit profiles: • Configure policies containing Connection Limit profiles using Networks only with source = Any, the public network, and destination = Protected Network. You can define segments using VLAN tags and physical ports. • It is not recommended to define networks when the Source and Destination are set to Any. • Policies containing Connection Limit profiles can be configured with Direction set to either One Way or Two Way. See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 171.

Parameter	Description
Protection Name	A descriptive name for easy identification when configuring and reporting.
Protection ID	(Read-only) The ID number assigned to the Connection Limit protection.
Application Port Group Name	The Layer 4 port or class object that defines the application you want to protect. To specify any port, the field may contain the value **any** or be empty. **Note:** You can click the adjacent button to open the dialog box in which you can add a class.
Protocol	The Layer 4 protocol of the application you want to protect. Values: TCP, UDP Default: TCP
Number of New Connections	The maximum number of new TCP connections, or new UDP sessions, per second, allowed for each source, destination or source-and- destination pair. All additional sessions are dropped. When the threshold is reached, attacks are identified, and Radware DefensePro DDoS Mitigation generates a security event. Values: 0–100,000,000 Default: 50
Tracking Type	The counting rule for tracking sessions. Values: • Source Count—Sessions are counted per source IP address. • Destination Count—Sessions are counted per destination IP address. • Source and Destination Count—Sessions are counted per source IP and destination IP address combination. Default: Source Count

See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 173.

Parameter	Description
Action	The action when an attack is detected. Values: • Drop—The packet is discarded. • Report-only—The packet is forwarded to the destination IP address. Default: Drop

	See, e.g., *See e.g.,* Radware DefensePro DDoS Mitigation User Guide Software Version 8.13.01. https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/fxos/radware/DPforCiscoFP_8_13_01_UG.pdf at p. 174.