CISCO
SECURE

Cisco Secure Cloud Web Application Firewall (WAF) Ordering Guide

Oct 2023

Contents

1. Introduction

1.1 Purpose

This document describes the ordering guidance for the Cisco® Secure Cloud Web Application Firewall (WAF) solution.

- Cisco Secure Cloud Web Application Firewall (WAF) is a Cisco Secure OEM solution based on Radware's Cloud WAF Service that provides a fully managed, cloud-based web application firewall service.

- The service provides full protection from web application–based attacks and is based on Radware's Attack Mitigation Solution, which is comprised of Radware's AppWall[1] and, for Layer 7 distributed-denial-of-service (DDoS) protection, Radware DefensePro.[1]

- The fully managed WAF as a service solution is easy to set up and does not require the user to download or configure any software. The customer can fully protect web applications, mobile applications, and API endpoints by onboarding onto the Cloud WAF service. The onboarding involves adding application information and certificates, enabling protection features, and editing their DNS records to redirect traffic to the Cloud WAF service.

- Secure Cloud WAF provides comprehensive coverage of both common and advanced web attacks as well as DDoS attacks.

When specifying Cloud WAF services, be sure to consult with Cisco to ensure that the correct Cloud WAF options and services are recommended to the customer. This guide will help ensure that the Cloud WAF solution is configured correctly to reduce the risk of order rejection or not meeting the customer requirements.

Audience

This guide is intended for Cisco sales, partners, and distributors.

[1] AppWall and DefensePro are registered trademarks of Radware, Inc.

2. Overview of the Cloud WAF Service Offerings

Cloud WAF services provide in-depth protection for HTTP/HTTPS protocol-based applications. These applications can be web, mobile, or API-based applications. The solution suite protects against 150+ known attack vectors, including the OWASP Top 10 Web Application Security Risks, Top 10 API Security Vulnerabilities, and Top 21 Automated Threats to Web Applications.

Cisco Secure Cloud WAF comes in three offerings: Essentials is the entry-level Cloud WAF offering, Advantage offers additional features and capabilities, and Premier is the top-tier Cloud WAF service. Each package builds on the previous package with more features and functions.

Table 1. Secure Cloud WAF Service Feature Comparison

Feature	Essentials	Advantage	Premier
WAF	●	●	●
API Protection	●	●	●
Advantage Rules	●	●	●
Rate Limit	●	●	●
Access Control & IP Geo Rules	●	●	●
Reporting & Analysis	●	●	●
DDoS Protection	1 Gbps	10 Gbps	10 Gbps
Standard Support	●	●	●
Advanced Support		●	●
Advanced WAF		●	●
ERT Active Attackers Feed (EAAF)		●	●
Client-Side Protection - Detection		●	●
Client-Side Protection - Mitigation			●
API Discovery			●
Bot Manager			●
Web DDos Protection			●
Data Retention	30 Days	60 Days	90 Days
Unlimited DDoS	Add-on	Add-on	Add-on
CDN	Add-on	Add-on	Add-on
Premium Support	Add-on	Add-on	Add-on

2.1 Essentials Plan

The Cisco Secure Cloud WAF Essentials plan offers entry-level application protection level for noncritical applications. It includes Cloud WAF, API protection, zero-day attack protection, and 1 Gbps of network DDoS protection, as well as outstanding SLAs.

· 1 Gbps of DDoS Protection

· Standard Support

· Entry-Level WAF Protection

2.2 Advantage Plan

The Cisco Secure Cloud WAF Advantage plan takes application security to the next level by offering advanced protection capabilities for customers who want to ensure they are well protected from more sophisticated and unknown attacks. The plan includes, on top of the Essentials plan, Advanced WAF (see Table 1) with its positive security model engine that protects against more sophisticated unknown and zero-day attacks, 10 Gbps of network DDoS protection, and JavaScript supply chain mapping, monitoring, and attack detection for client-side protection. Advantage also includes an intelligence feed, the ERT Active Attackers Feed (EAAF), which automatically blocks known malicious active devices. Customers also benefit from the onboarding support and ongoing policy reviews included with the Advantage package.

· 10 Gbps of DDoS Protection—10x the DDoS protection of Essentials

· Advanced Support

· Advanced WAF incorporates a positive security model engine that protects against sophisticated unknown and zero-day attacks.

· EAAF is an intelligence feed that provides protection against known malicious IPs that have been detected by a deception network operated by the Radware threat intelligence team.

· Client-Side Protection (Detection)—Detects malicious events occurring on the end user's browser.

2.3 Premier Plan

The Cisco Secure Cloud WAF Premier plan provides a security blanket for your entire application environment—from client-side to server-side and everything in between. This plan includes everything that's included in the Advantage plan in addition to advanced Bot Manager with behavioral-based, multilayered detection and mitigation, automated API discovery and API security policy generation, client-side protection enforcement, and real-time automatic Web DDoS Protection.

· Client-Side Protection (Mitigation)—Blocks malicious events that occur on the end user's browser.

· API Discovery—Discovers undocumented APIs on customer's applications.

· Bot Manager—Detects and blocks malicious bot activity from the simplest to the most sophisticated bots.

· Web DDoS Protection—Detects and mitigates encrypted and high Request-per-second (RPS) DDoS attacks

2.4 Web DDoS Protection

A new, more advanced DDoS attack has been developed by malicious actors that is very sophisticated. This attack cannot be detected by the traditional network Layer 3, Layer 4, or even simple Layer 7 types of detection and mitigation solutions. The new Web DDoS attack known as a Web DDoS Tsunami attack is often mistaken as legitimate traffic by traditional DDoS and WAF solutions as the traffic behaves very similarly. This attack will easily overwhelm a system's resources by increasing the application maximum Requests Per Second (RPS) capacity, making the application unavailable to legitimate traffic. To detect this new Web DDoS Tsunami attack, traffic needs to be decrypted and the data must be parsed through new patented machine learning–based behavioral analysis that can accurately identify valid traffic from malicious traffic, thereby ensuring the availability of the application.

3. Optional Add-Ons

3.1 Content Delivery Network (CDN)

For enterprises that wish to combine website delivery with their web application security, Cisco offers a content delivery network (CDN) solution integrated directly into a unified application protection portal. The CDN solution is based on the Amazon CloudFront CDN for a massive, globally distributed footprint, enhanced performance, and DevOps-friendly usability. CDN is offered in units of 10 Mbps and must equal the Cloud WAF (CWAF) bandwidth ordered.

3.2 Unlimited DDoS Protection

For enterprises that suffer from high-volume network DDoS attacks and 1G or 10G of mitigation capacity is not enough, we offer unlimited protection with its industry's top-rated DDoS protection solution. Defend your organization against today's most advanced DDoS attacks–no matter their frequency or volume.

3.3 Premium (Enhanced) Support for Secure Cloud WAF

For organizations that require additional cybersecurity expertise, Cisco offers the Emergency Response Team (ERT) Premium managed service. This service includes:

· 10-minute response SLA via "hot-line" access

· On-demand emergency response attack mitigation

· Designated Customer Success Manager

· Post-attack forensics and recommendations

· Periodic security status reports

· Priority service case handling

· Policy tuning and application security insights

4. Steps to Building a Quote

4.1 The two steps in building a quote

Building a quote for Cisco Secure Cloud WAF Protection is comprised of the following steps:

- Scoping
- Structuring the Quote

4.2 Step #1: Scoping

The purpose of scoping is to gather the relevant customer information to provide the optimal protection coverage for their needs:

- Based on the feature table and the support table shown earlier in this document, determine which Cloud WAF package the customer needs.

  Premier provides the most features, including full bot protection and Web DDoS protection. If these are not required, then we suggest going with Advantage. Because Essentials lacks the Advance WAF and has a lower level of support, Essentials should only be used as an entry-level offering either when in a highly price-competitive situation or when the applications that need to be protected are simple and nonbusiness critical.

- What is the total amount of **legitimate traffic** for all the customer applications that will need to be protected by Cisco Secure Cloud WAF? (Based on 10-Mbps increments)

- How many **applications** will be protected by the Cisco Secure Cloud WAF solution? (Additional protected apps, x -1 as 1 application is included by default in the service)

- CWAF Essentials comes with 1 Gbps of DDoS Protection, while Advantage and Premier includes up to 10 Gbps of DDoS attack traffic protection. Does the customer require protection for higher DDoS attacks (i.e., unlimited DDoS)?

- Does the customer require an emergency response (10 minutes or less) in the event of threat or issue or will the customer benefit from a Customer Success Manager, post-attack forensics, and frequent policy recommendations (i.e., Cloud WAF Enhanced Support; see Table 2—Support Matrix)?

- Does the customer want CDN service to provide consistent application performance in other regions (i.e., optional CDN service)?
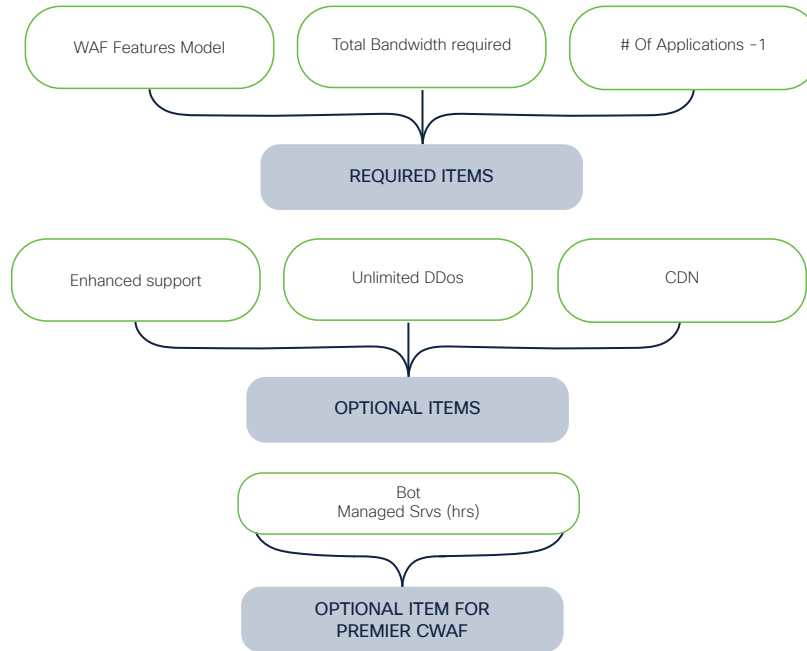
4.3 Step #2: Structuring the Quote

A price quote for Cisco Secure Cloud WAF Service is a combination of yearly fees and selected add-ons:
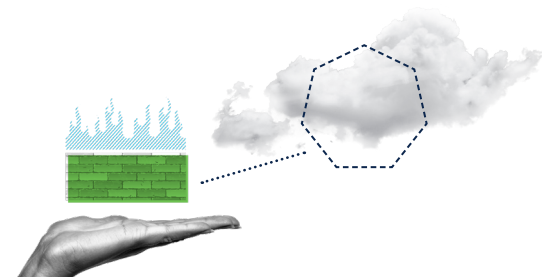
5. Ordering

As a convenience, Cisco has created a Multi-Level Build (MLB) structure in CCW to properly associate the main Cloud WAF Service with the appropriate add-ons, since not all add-ons are orderable with each of the different protection types. The MLB is provided for structure only; no additional discount is given.

To order Cisco Cloud WAF, we start with the parent SKU in the MLB, **WAF-SEC-SUB**

Figure 1. Ordering Cloud WAF from the WAF-SEC-SUB

Cloud WAF (WAF-SUB-SEC)

Using the top SKU WAF-SUB-SEC:

Required Items:

- Select the quantity of the Cloud WAF Service Essential/Advantage/Premier by adding the number of units required. **Each unit represents 10Mbps.**
  - **WAF-CWAF-E-LIC** = Essentials Bandwidth SKU
  - **WAF-CWAF-A-LIC** = Advantage Bandwidth SKU
  - **WAF-CWAF-P-LIC** = Premier Bandwidth SKU

- One application is included by default with the Bandwidth SKU. For additional applications, need to add the quantity. The application SKU needs to match the bandwidth SKU ordered as price varies per application based on service type.
  - **WAF-CWAF-APP-E-LIC** = Essentials additional application SKU
  - **WAF-CWAF-APP-A-LIC** = Advantage additional application SKU
  - **WAF-CWAF-APP-P-LIC** = Premier additional application SKU

6. Optional Add-Ons:

6.1 Content Delivery Network (CDN)

If a customer requires CDN service for their protected applications, enter the number of units for SKU for field **WAF-CDN-LIC**. The number of units for the CDN SKU must match the service units above (for example, if WAF-CWAF-E-LIC = 100 units, then the WAF-CDN-LIC must be 100 units as well).

Please note that CDN can be ordered with any service type, Essentials, Advantage, or Premier. For this example, we used Essentials, but we could have used any of the three service types.

6.2 Volumetric Network DDoS

Unlimited volumetric network DDoS protection can be ordered for any of the three services. By default, Essentials comes with 1G of network DDoS protection while Advantage and Premier both have 10G of network DDoS protection included with the service. If the customer ordering Essentials would like 10G of volumetric network DDoS, you will need to change the CWAF from Essential to Advantage or Premier.

Enter quantity of 1 for adding unlimited DDoS to the order. If any other number is entered, it will default to 1 when saved. Blank or 0, which is the default value, indicates not ordered/required for CWAF service.

Secure Cloud WAF Addon				
Secure Cloud WAF CDN **WAF-CDN-LIC**	195.31 Per User/Month	Added	100 User	🗑 Delete
Secure Cloud WAF Unlimited DDoS Protection **WAF-CWAF-UDDOS-LIC**	11,220.0000 Per Units/Month	Added	1 Units	🗑 Delete

6.3 Support and Premier/Enhanced Support

A customer has the option to order Enhanced support on any CWAF Service for a white glove service where a priority queue code will be provided for support with as well as a dedicated Customer Service Manager to provide regular updates for policy reviews and post-threat analysis. Enhanced support is highly recommended for organizations that need professional support for WAF management and for advanced policy creating and incident forensics when the skill is not available within the customer's organization.

By default, customers who order Essential are provided with Standard support. Customers who order Advantage or Premier are provided with Advanced support. Support levels can be seen in the table below.
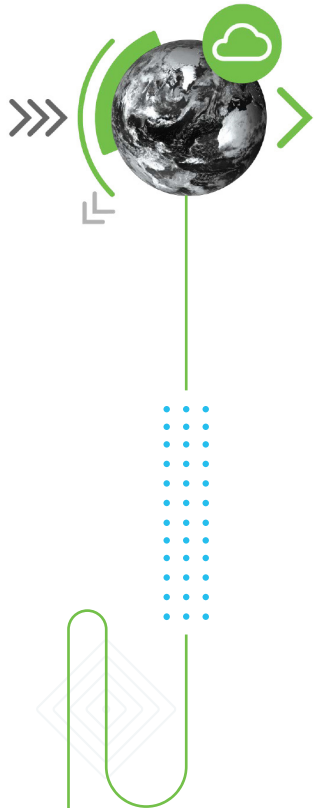
Table 2. Support Matrix

Category	Risk/Impact-based Priority	Standard Support	Advanced Support	Enhanced Support
Response SLA	P1 (Phone)	40 Min	30 Min	10 Min
	P1 (Ticket)	3 Hours	2 Hours	1 Hour
	P2	6 Hours	4 Hours	2 Hours
	P3	16 Hours	12 Hours	4 Hours
	P4	24 Hours	24 Hours	12 Hours
Ticket Updates	P1	48 Hours	48 Hours	24 Hours
	P2	96 Hours	72 Hours	48 Hours
	P3	120 Hours	96 Hours	72 Hours
	P4	144 Hours	120 Hours	96 Hours
Managed Services	Certificate Management & Notifications	No	Yes	Yes
	Onboarding & Policy Review	No	Yes	Yes
	Post-attack Analysis	No	Yes	Yes
	Quarterly Premium Security Report	No	No	Yes
	Security Configuration Review	No	6 Months	3 Months
	Extended Monitoring	No	External Monitoring on Top 5 Apps	External Monitoring on All Apps

All services are a fully managed service with 24-hour/7-days-a-week support.

Enhanced support is based on two SKUs. The first is the primary SKU to enable the service, which includes one protected application just as in the WAF Service SKU, **SVS-CWAF-SUP-E**. The second SKU is required if the customer has more than one application **SVS-CWAF-APP-SUP-E**. The quantity is total application – 1. This number should be automatically populated by CCW when selecting the Enhanced support SKU.

To order Enhanced support, select the Service tab and click on the Swap button to the right of the **SVS-CWAF-SUP-E**.

Once the Swap button has been clicked, Enhanced support will be added as seen in the image below and the appropriate number of applications that are being protected will be added.

Note: If Enhanced support is added later, please make sure to match the number of units to equal the number of applications the customer has ordered for their cloud WAF.

7. Contract Term

The term can be any duration between 12 months (1 year) to 60 months (5 years). The default CCW option is 36 months. Please note, if you change the term of the license, all licenses within the parent SKU (WAF-SEC-SUB) will be changed to match.

To change the term duration, click the Edit button on the right-hand side of the screen.

Enter the duration term in the Effective For box in number of months, anywhere from 12 to 60. For less than 12 months or greater than 60 months, please reach out to the product manager.

8. Upgrades/Adding Additional Features.

It is common in subscription-based services like Secure Cloud WAF that customers may need to upgrade their services before the renewal of the service. These upgrades may include, but are not limited to:

- Bandwidth Increase
- More Applications
- Unlimited DDoS
- CDN
- ERT Premium

Some of the upgrades may provide a lower cost per unit as the customer moves up in tiers. For example, an order with 1 unit of 10 Mbps costs more per unit than an order with 6 units of 10 Mbps. Therefore, it is suggested that, rather than just creating a new order for the upgrades, the Cisco Sales team follow the process outlined in Best Practices for Managing SaaS Subscription in CCW (https://salesconnect.cisco. com/sc/s/simple-media?vtui__mediald=a1m8c00000niUWsAAM). This allows the customer to benefit from the additional benefits of increases in their subscription services with Cisco.

9. Ordering Examples

9.1 Example 1:

50M Cloud WAF Service Essentials (CCW KO147887435LL)

Requirements:

- 50M of Cloud WAF Essentials
- 3 Applications
- 1-Year Term
- With Standard Support (Default for Essentials)

Notice that the WAF-CWAF-AOO-E-LIC has one units. This is because the Bandwidth SKU includes one application. We take the number of applications required and subtract 1: 3-1 = 2 additional applications.

9.2 Example 2:

300M Cloud WAF Advantage (CCW ZS147960664CC)

Requirements:

- 300M of Cloud WAF Advantage
- 12 Applications
- 2-Year Term
- Enhanced Support

	Hardware, Software and Services	Estimated Lead Time ⓘ	Unit List Price (USD)	Qty	Unit Net Price (USD)	Discount (%)	Extended Net Price (USD)
☐ ⊖	1.0 **WAF-SEC-SUB** more ▸ Cisco Secure Web Application Firewall Valid as of 20-Sep-2023 07:35:19 PDT	Not Applicable	0.00 ↻ MRC	1	0.00	0	0.00
	✎ **Requested Start Date** 23-Sep-2023 **Requested For** Initial Term 24 Months From 23-Sep-2023 To 22-Sep-2025				**Automatically Renews For** ⓘ 12 Months From 23-Sep-2025	**Billing Frequency** Prepaid Term	
	Edit Options | Validate | Recommended Content | Add Note | More Actions ˅						Add Subtotal
	1.1 **WAF-CWAF-A-LIC** more▸ Secure Cloud WAF Advantage (10Mb Units)	3 days	626.0400 Per Units /Month	30 Units	626.0400 Per Units /Month	0.00	450,748.80
	1.2 **WAF-CWAF-APP-A-LIC** more▸ Secure Cloud WAF Advantage Applications Add On	3 days	99.8400 Per Units /Month	11 Units	99.8400 Per Units /Month	0.00	26,357.76
	1.3 **SVS-CWAF-SUP-E** more▸ Enhanced Support for Secure Cloud Web Application Firewall	3 days	1,840.00 Per Units /Month	1 Units	1,840.00 Per Units /Month	0.00	44,160.00
	1.4 **SVS-CWAF-APP-SUP-E** more▸ Enhanced Support for Secure Cloud WAF Application Add-ons	3 days	115.00 Per Units /Month	11 Units	115.00 Per Units /Month	0.00	30,360.00

Notes for Example 2:

- WAF-CWAF-A-LIC has 30 units, which multiplied by 10 Mbps = 300 Mbps.
- WAF-CWAF-APP-A-LIC has 11 units with the 1 included with the bandwidth SKU = 12 apps.
- SVS-CWAF-SUB-E to add the Enhanced support.
- SVS-CWAF-APP-SUB-E to add the number of applications, which needs to match the number of applications in the CWAF order. In this case, both are 11 for the 12 applications (1 included in the base SKU).

9.3 Example 3:

1.2-Gbps Cloud WAF Premier (CCW RS147960754VI)

Requirements:

- 1.2G of Cloud WAF Premier
- 100 Applications
- 5-Year Term
- CDN
- Unlimited Volumetric Network DDoS

☐ ⊖ 1.0 **WAF-SEC-SUB** more ➤ Cisco Secure Web Application Firewall Valid as of 20-Sep-2023 08:34:08 PDT		Not Applicable	**0.00** ↻ MRC	1	**0.00**		0	**0.00**	

✎ Requested Start Date 23-Sep-2023	Requested For Initial Term 60 Months From 23-Sep-2023 To 22-Sep-2028	Automatically Renews For ❶ 12 Months From 23-Sep-2028	Billing Frequency Prepaid Term
Edit Options | Validate | Recommended Content | Add Note | More Actions ⌄			Add Subtotal

1.1 **WAF-CWAF-P-LIC** more➤ Secure Cloud WAF Premier (10Mb Units)	3 days	**269.2800** Per Units /Month	120 Units	**269.2800** Per Units /Month	0.00	**1,938,816.00**
1.2 **WAF-CWAF-APP-P-LIC** more➤ Secure Cloud WAF Premier Applications Add On	3 days	**132.4800** Per Units /Month	99 Units	**132.4800** Per Units /Month	0.00	**786,931.20**
1.3 **WAF-CDN-LIC** more➤ Secure Cloud WAF CDN (10Mb Units)	3 days	**195.31** Per User /Month	120 User	**195.31** Per User /Month	0.00	**1,406,232.00**
1.4 **WAF-CWAF-UDDOS-LIC** more➤ Secure Cloud WAF Unlimited DDoS	3 days	**11,220.0000** Per Units /Month	1 Units	**11,220.0000** Per Units /Month	0.00	**673,200.00**
1.5 **SVS-CWAF-SUP-B** more➤ Basic Support for Secure Cloud Web Application Firewall	3 days	**0.00** Per User /Month	1 User	**0.00** Per User /Month	0.00	**0.00**

Notes for Example 3:

- WAF-CWAF-P-LIC has 120 units, which multiplied by 10 Mbps = 1200 Mbps or 1.2 Gbps.

- WAF-CWAF-APP-P-LIC has 99 units with the 1 included with the bandwidth SKU = 100 apps.

- CDN option WAF-CDN-LIC has 120 units of 10 Mbps to equal the 1.2 Gbps of the bandwidth of the CWAF Service selected in the SKU WAF-CWAF-P-LIC.

- WAF-CWAF-UDDOS-LIC units equal 1 to enable this option for Unlimited Volumetric Network DDoS.

- SVS-CWAF-SUB-B means the default support is applied. In this case, this is Premier, which has Advanced support.

10. Additional Resources

Please search Cisco SalesConnect for additional information, including presentations, at-a-glances, and other supporting documentation on Cisco Secure WAF Protection. Additional Secure WAF information can be found on Cisco.com at www.cisco.com/go/secure-waf.

For additional support, please contact us in the "Secure DDoS Protection (Radware)" space in Webex Teams at webexteams://im?space=cfc5c720-4ed4-11ea-b877-a30147ae2247 or send an email to ddos-support@external.cisco.com.

Cisco Commerce Workspace

Cisco Commerce Workspace (CCW) is the primary tool used for ordering Cisco products and new services offered on the Cisco Price List. Three main steps are involved in creating an order: creating a quick quote, converting a quote to an order, and submitting an order. Cisco Commerce Workspace also acts as a quoting, pricing, configuration, and status tool. The Cisco Service Contract Center can be used to view the status of a covered item as well as service contract information.

11. Terms and Conditions

The Cloud DDoS Protection packages and Web Application Firewall packages and add-ons (the "Cloud Service") are governed by the terms and conditions of the Radware Master Cloud Services Agreement and applicable Cloud Service Schedule attached thereto (the "Radware Cloud Services Agreement"). You must, as early as possible in the sales cycle, notify your customer in writing that the Radware Cloud Services Agreement applies to their use of such Cloud Services and provide a link to those terms.
In accordance with the Radware Cloud Services Agreement, the Cloud Services are licensed for internal use only and customers are not authorized to provide the Cloud Services or make its functionality available to third parties on a service provider, service bureau, hosting, or time-sharing basis or for providing any other type of services to a third party unless explicitly agreed to in writing with Radware.

Cloud WAF Quick Start Guide
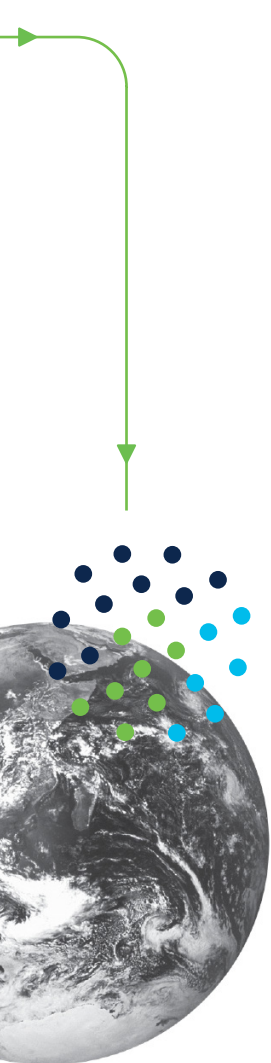
12. Cisco Capital Financing

Cisco Capital® financing can help remove or reduce the barriers preventing organizations from obtaining the technology they need. Total solution financing programs help customers and partners:

· Achieve business objectives

· Accelerate growth

· Acquire technology to match current strategies and future needs

· Remain competitive

Cisco Capital also helps your customers achieve financial goals such as optimizing investment dollars, turning CapEx into OpEx, and managing cash flow. And there's just one predictable payment. Cisco Capital operates in more than 100 countries, so regardless of location, customers and partners have access to a trusted means to secure Cisco products and services.

For more information about Cisco Capital financing, visit http://www.ciscocapital.com.
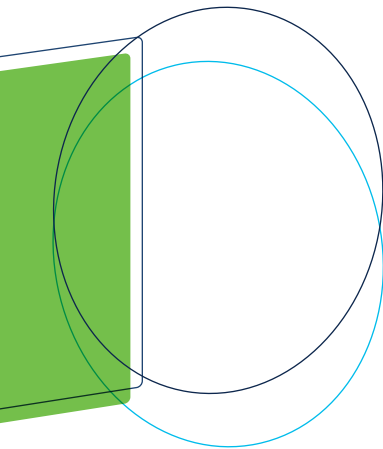
Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte.Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

For information about Cisco application security solutions, go to: www.cisco.com/go/secure-waf