Radware Cloud WAF Service

QUICK START GUIDE

August 2019

TABLE OF CONTENTS

WELCOME TO RADWARE CLOUD WAF SERVICE!

We are delighted that you have chosen to join our service, and welcome you aboard.

This guide will instruct you how to quickly set up your applications to be protected by Radware Cloud WAF service.

This guide addresses typical customer use-cases and includes the following main sections:

- Signing Up to the Cloud WAF Portal—Describes the process of receiving an invitation by e-mail, setting up your user account, and inviting additional users
- Onboarding an Application—Describes how to add certificates, add applications, and complete the application provisioning process
- Managing Application Lifecycle—Describes frequent use cases when managing the application lifecycle—for example, configuration updates, protection exceptions, and more
- Monitoring Protected Applications—Describes how you can monitor your protected applications using the real-time dashboard, receive periodic reports, configure real-time alerts, and more

SIGNING UP TO THE CLOUD WAF PORTAL

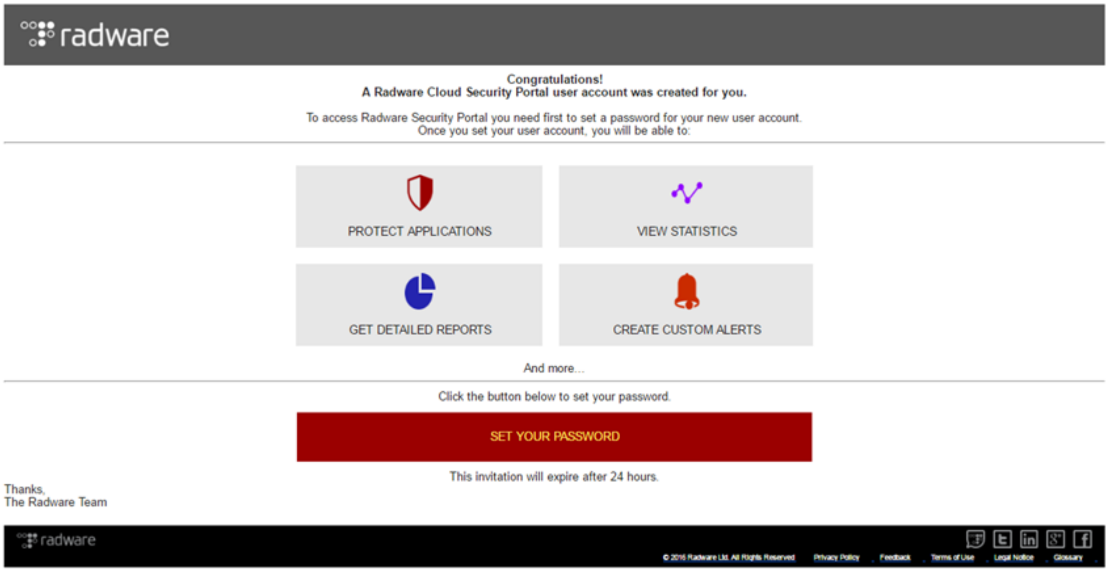
This section describes how to sign up to the Radware Cloud WAF Service portal. The procedures in this section are based on user management that is done within Cloud WAF.

Note: If your organization is using a *federated identity management* system that supports SAML, you can integrate Cloud WAF to use it. For more information, see here.

Receive Invitation E-mail

You will receive an e-mail from Radware Cloud Services (radware@radwarecloud.com) inviting you to log in to the portal.

The e-mail is triggered either by the Radware Cloud Operations team or by a colleague of yours who is already registered to the portal. If you have not received your invitation e-mail yet, please ask them to be invited.



Congratulations!
A Radware Cloud Security Portal user account was created for you.

To access Radware Security Portal you need first to set a password for your new user account.
Once you set your user account, you will be able to:

And more...

Click the button below to set your password.

This invitation will expire after 24 hours.

Thanks,
The Radware Team

After clicking **SET YOUR PASSWORD**, follow the procedure that is described in the following section, Setting Up Your User Account.

Setting Up Your User Account

Prerequisite: It is required to install Google Authenticator on your iOS- or Android-based mobile devices.

Note: if you prefer to use password-based authentication only, rather than 2FA (two factor authentication), contact Radware team (support@radware.com).

To log in the first time

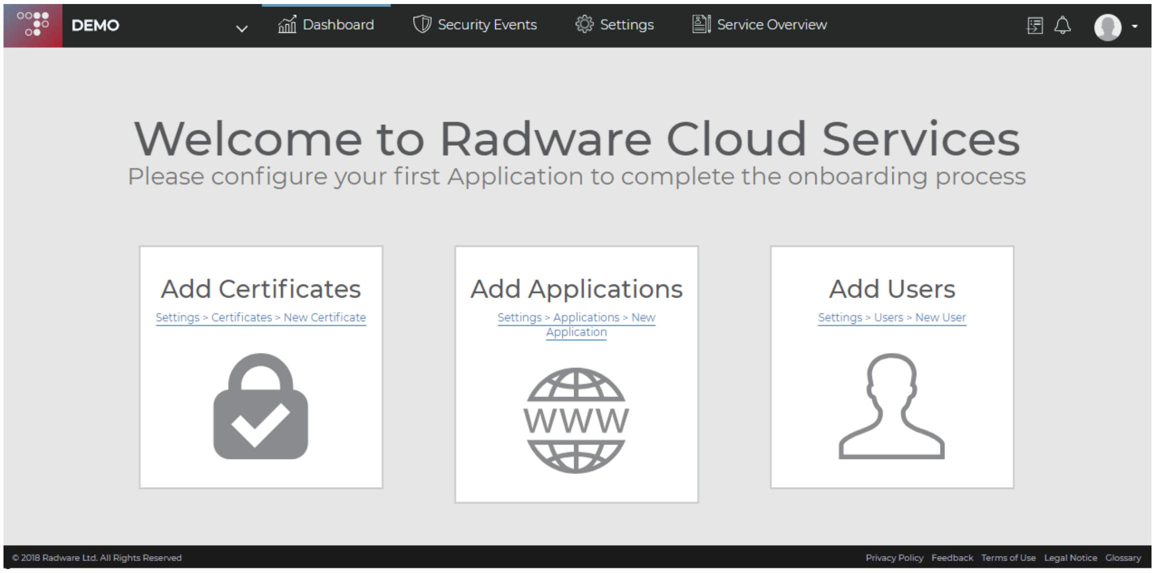
1. Set your password when you are requested to.
2. When your account is using multi-factor authentication (MFA), a QR code is displayed—then, do the following:
    a. Open Google Authenticator on your mobile device, point your device camera to the displayed QR code, and then, click **Done**. You are prompted to enter the security code for the portal login.
    b. Open the Google Authenticator application on your mobile device. The security code appears on your mobile device screen.
    c. In the login window, type the security code that appears on the Google Authenticator on your mobile device.

3. Select your security question, and type your personal answer. The security question and answer are used in case you need to reset your password.

   The first-time setup procedure is completed. You are now signed in to the portal, and can start using it.

Portal First Login

For the first user login of a new account, a welcome screen is displayed, which lets you add certificates, add applications, or invite users, as described in the following section.



Welcome to Radware Cloud Services

Please configure your first Application to complete the onboarding process

Invite Additional Users

You can add additional users from your team/organization to allow them to individually access the Cloud WAF portal.

To add a user

1. Navigate to **Settings > Users**, and click the **+** button.
2. Set the user details and the user role: **Admin** or **User**. Admin users can create new users of their account.
3. After you create a new user, the invitees receive an e-mail invitation to access the Cloud WAF portal through the procedure described in Signing Up to the Cloud WAF Portal.

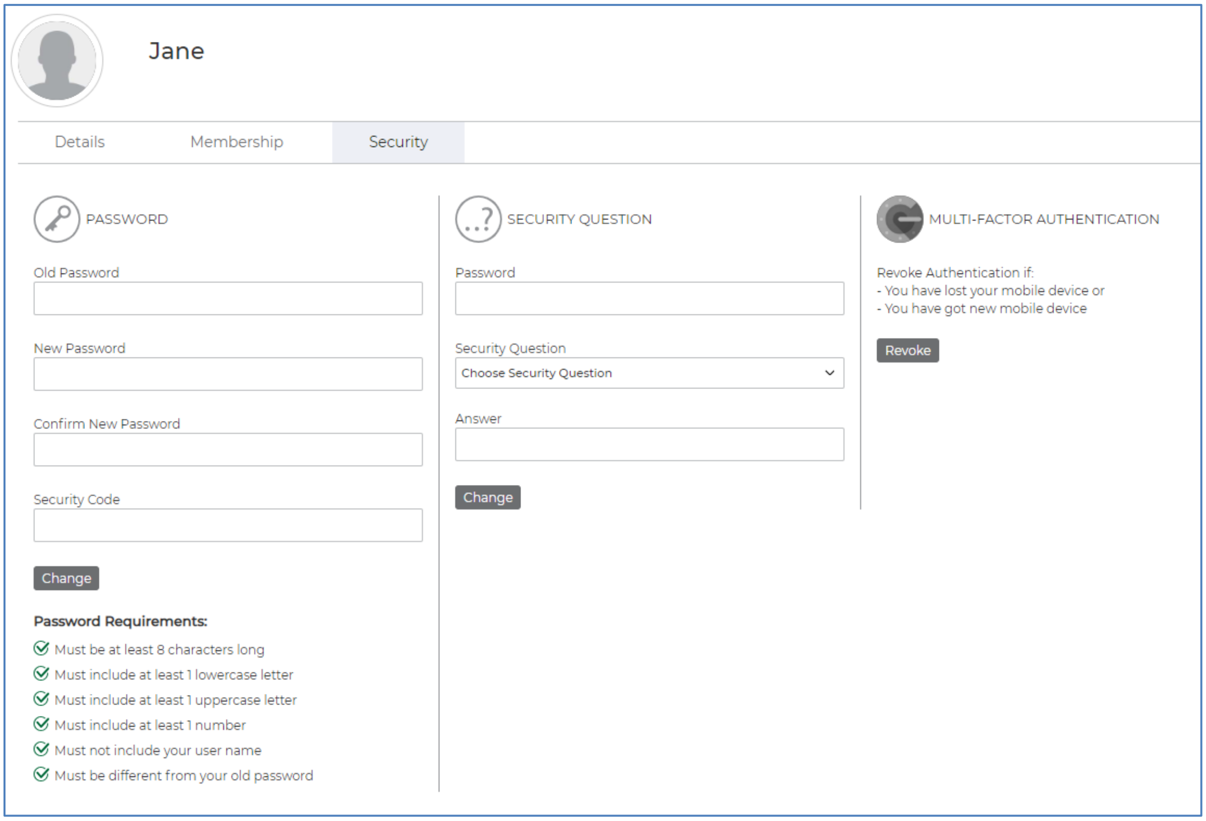
Managing Your Password

You can manage your password and authentication, which includes the following:

- Change your user password
- Update your security question
- Revoke the multi-factor authentication (MFA), in case you need to update your mobile device

To manage your own user profile

- Hover over the *user* icon at the top-right corner of the portal screen and select your user from the drop-down menu.



Revoke Authentication if:
- You have lost your mobile device or
- You have got new mobile device

Password Requirements:

✓ Must be at least 8 characters long
✓ Must include at least 1 lowercase letter
✓ Must include at least 1 uppercase letter
✓ Must include at least 1 number
✓ Must not include your user name
✓ Must be different from your old password

ONBOARDING AN APPLICATION

An Application is a logical entity in Cloud WAF that protects your domains against Web application attacks and DoS attacks. This section describes the steps required to onboard a new protected application.

Understanding Application Onboarding Process

The application-onboarding process includes the following steps:

#	Step	Description	Typical Duration
1.	Adding certificates	Relevant for HTTPS applications	Immediate.
2.	Adding an application	Provides application parameters and pointing to the certificates (if applicable). Once set, the setup for protecting your application is built within Cloud WAF.	The time to complete this activity is, on average, 30 minutes.
3.	Diverting the application traffic	To go through Cloud WAF PoPs, by updating the DNS server settings.	Once you update the DNS settings for your application, it typically takes a few hours to propagate the update over the Internet, up to 48 hours.
4.	Learning Traffic Patterns	Allows time for Cloud WAF to learn the legitimate traffic patterns.	The time to complete is activity depends on traffic volume, and may take up to 2–3 weeks.
5.	Reviewing the Learned Policies with ERT	The learned protection policies are reviewed by Radware Emergency Response Team (ERT) experts, in order to refine false positives before the service starts protecting the application.	Once coordinated, the review meeting is about one hour.
6.	Your application is now protected!	Your application is now protected against both Web Application attacks and DDoS attacks	N/A

Note: customers that are interested in **Immediate Protection**, without the **Learning and Policy Review** steps, contact support@radware.com.

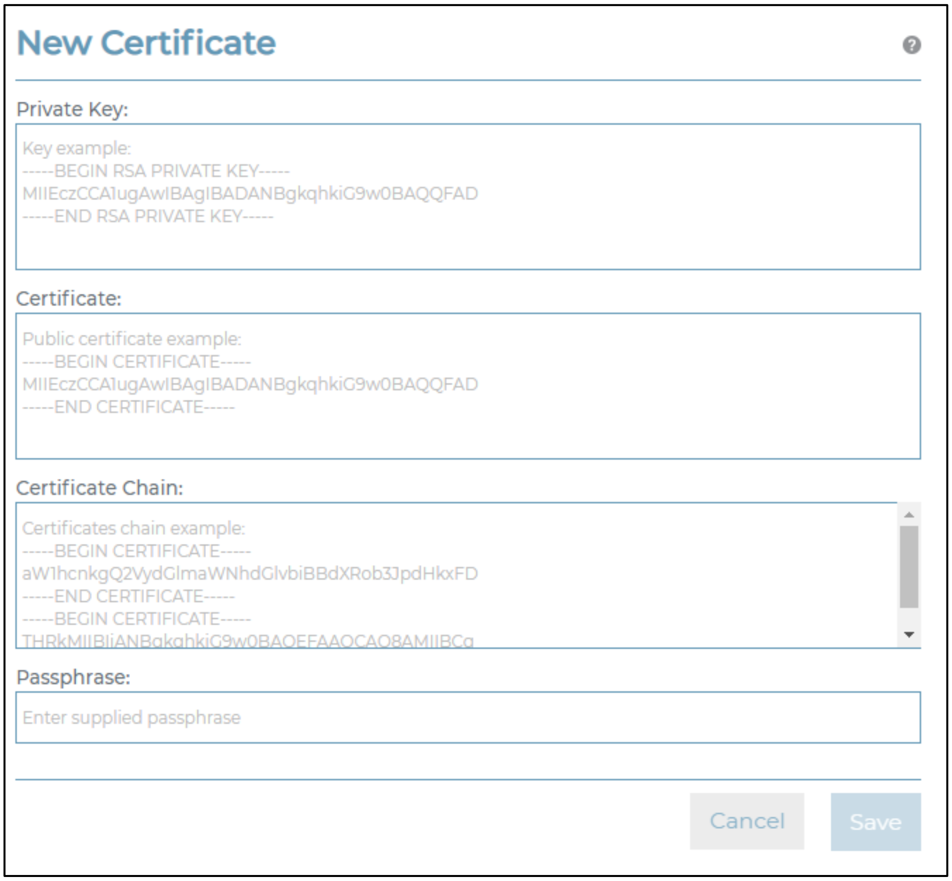
Adding Certificates

To add a new HTTPS application, you should first add the certificate(s), then create the application, and bind the certificate(s) to the application.

To add a certificate for an HTTPS application

1. Navigate to **Settings > Certificates**, and click the **+** button.
2. Paste the certificate bundle details:
   - **Private Key**—The certificate private key in PEM format.
   - **Public Key** (Certificate)—The certificate that signs the application in PEM format.
   - **Certificate chain** (optional)—A certificate chain that contains one or more intermediate certificates concatenated in PEM format.
   - **Passphrase** (optional)—The passphrase in case the key is encrypted.

   Note: The **Certificate**, **Private Key**, and the certificate chain need to be PEM-encoded. Certificates of different types such as DER, PKCS#7, and others can be converted easily to PEM format by using OpenSSL or other online tools.



New Certificate

Private Key:

```
Key example:
-----BEGIN RSA PRIVATE KEY-----
MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD
-----END RSA PRIVATE KEY-----
```

Certificate:

```
Public certificate example:
-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD
-----END CERTIFICATE-----
```

Certificate Chain:

```
Certificates chain example:
-----BEGIN CERTIFICATE-----
aW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFD
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
```

Passphrase: Enter supplied passphrase

The certificate can be used when adding an Application to be protected by Cloud WAF, or can be bound to an existing application that is already configured to use HTTPS.

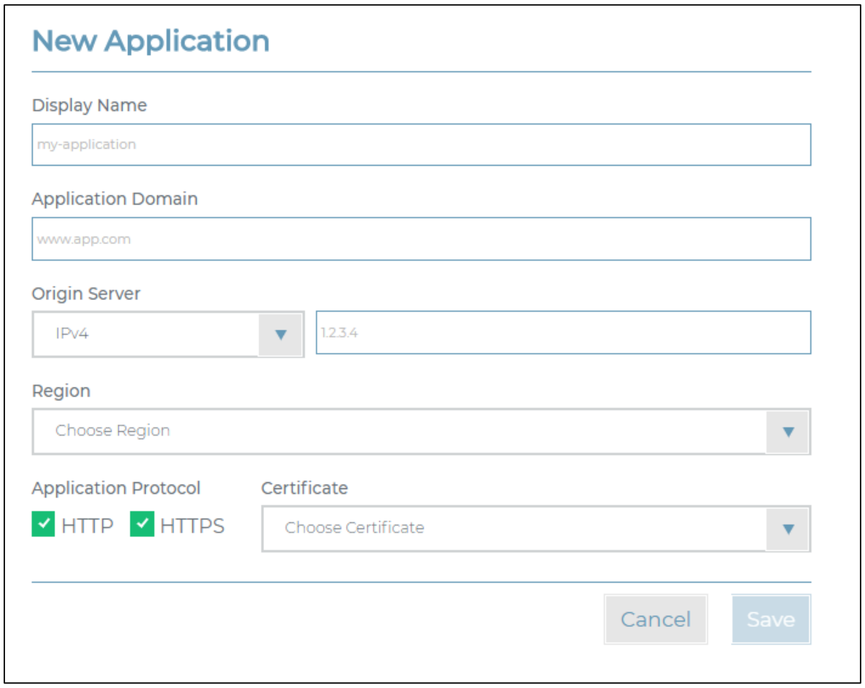
Adding an Application

To add an application

1. Navigate to **Settings > Applications**, and click the **+** button.
2. Configure the following:
   - **Display Name**—The name of the Application in the **Applications** list. Example: **Radware website**
   - **Application Domain**—The main domain that Cloud WAF is protecting. Example: **www.radware.com**
   - **Origin Server**—The IPv4 address or domain of the origin server that hosts the application. At the time of application creation, a single **Origin Server** can be specified. Examples: **23.56.43.89**, **origin.location2.radware.com.**

     Note: Once the application is deployed, you can set additional origin servers for your application.
   - **Region**—The geographic region where Radware WAF Service deploys the Application. It is recommended to select a region that is closest to the location of the origin server.
   - **Application Protocol**—The services that the Application supports: HTTP and/or HTTPS.
   - **Certificate**—The SSL certificate that terminates the HTTPS requests.

     Note: This field is mandatory for HTTPS applications. See Adding Certificates below to learn how to upload a certificate.



New Application

Display Name: my-application

Application Domain: www.app.com

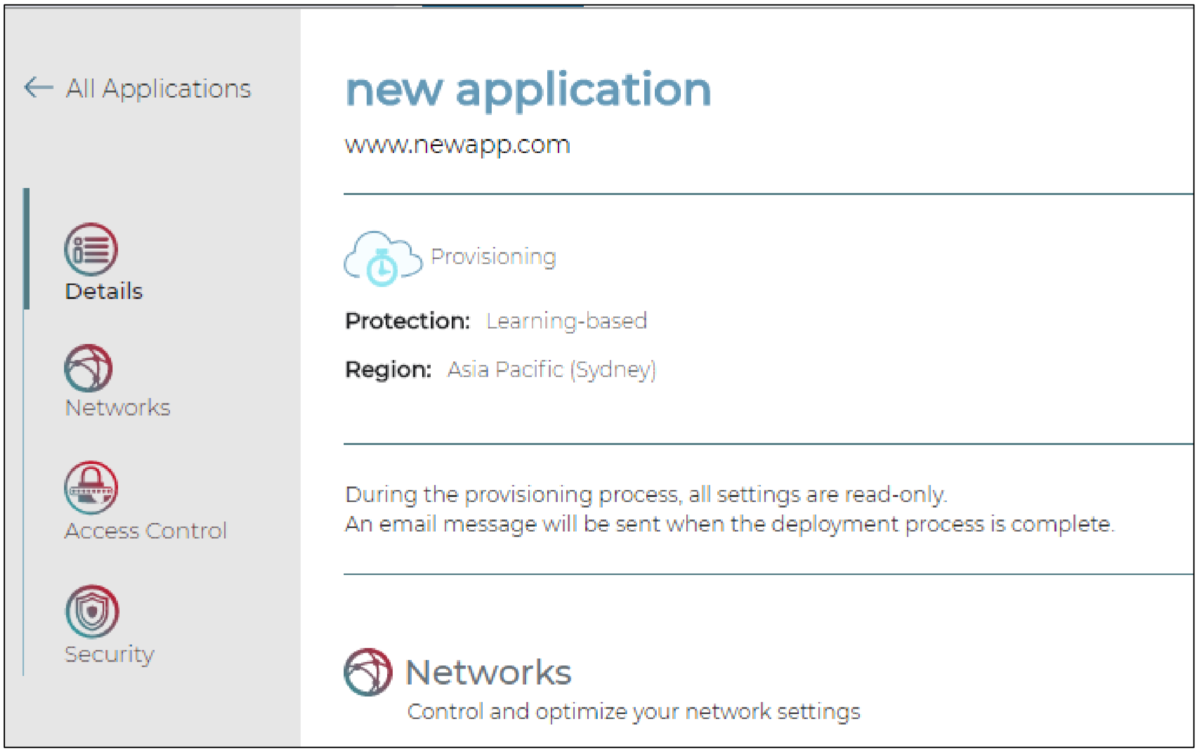
Origin Server: IPv4 ▾ 1.2.3.4

Region: Choose Region ▾

Application Protocol: ☑ HTTP ☑ HTTPS

Certificate: Choose Certificate ▾

After you configure your application, the application goes into the in the *Provisioning* state. This process typically takes a few minutes, but may take up to a few hours to complete. When the application is in the *Provisioning* state, the parameters of the application *Settings* in the portal are read-only.



Protection: Learning-based

Region: Asia Pacific (Sydney)

During the provisioning process, all settings are read-only.
An email message will be sent when the deployment process is complete.

Using One Application to Protect Multiple Domains

An application is a logical entity in the portal. Protection and reporting are provided per application. Typically, an application uses a single domain name.

Some organizations use multitude of hosts (domains) that are logically grouped. For example, applications that are frequently brought up by a CMS system or a service provider that is using a per-customer domain name, such that the number of domains equals the number of customers and may be rapidly growing. In such cases, it may be challenging to define an application per domain name, where the applications are essentially similar.

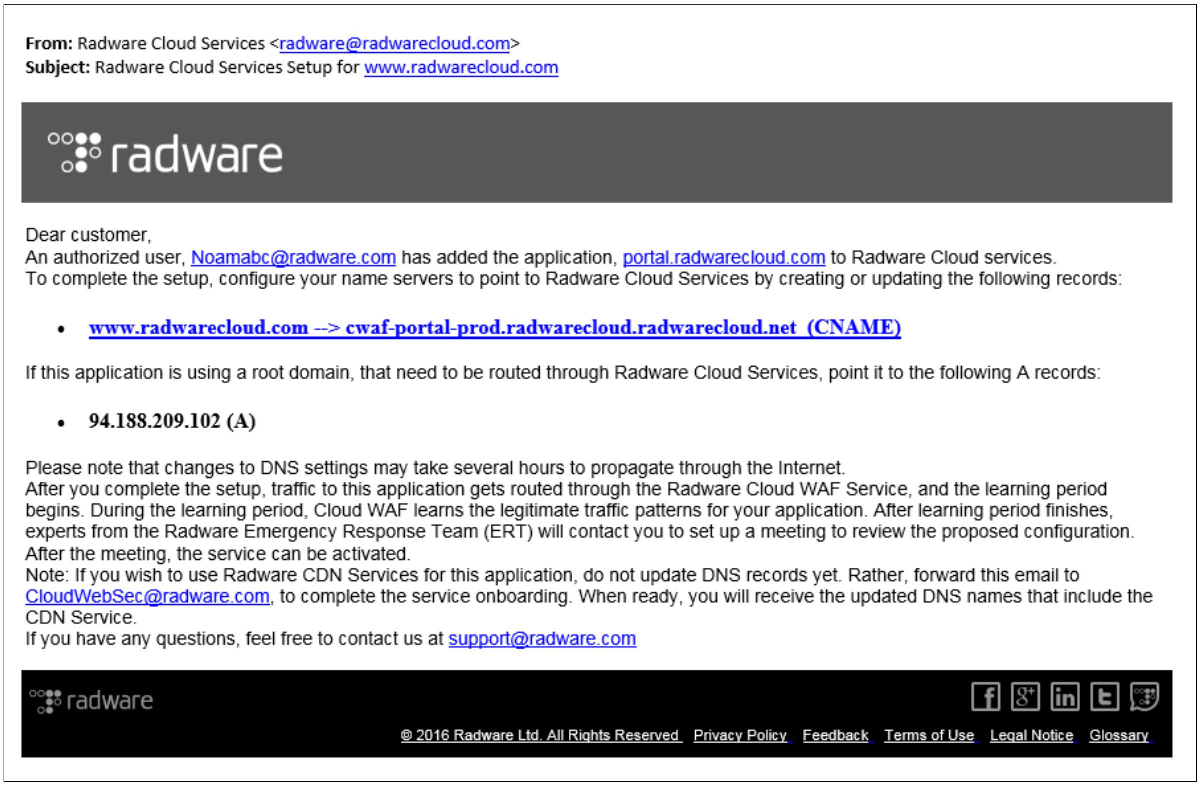
To simplify configuration and management, you can use a single application to protect multiple domains, as long as they share the following:

- The same origin server(s) (IP address or FQDN)
- The same WAF security policy
- The same SSL certificate (for HTTPS applications)
- The same character set

Diverting the Application Traffic

As soon as a new application is provisioned, the service is ready to receive incoming traffic, to learn the traffic patterns and build the security policies, so that attack traffic can be detected and blocked.

You will receive an e-mail with the setup details, including the details that are required to divert your traffic through the service.



From: Radware Cloud Services <radware@radwarecloud.com>
Subject: Radware Cloud Services Setup for www.radwarecloud.com

Dear customer,
An authorized user, Noamabc@radware.com has added the application, portal.radwarecloud.com to Radware Cloud services.
To complete the setup, configure your name servers to point to Radware Cloud Services by creating or updating the following records:

- **www.radwarecloud.com --> cwaf-portal-prod.radwarecloud.radwarecloud.net (CNAME)**

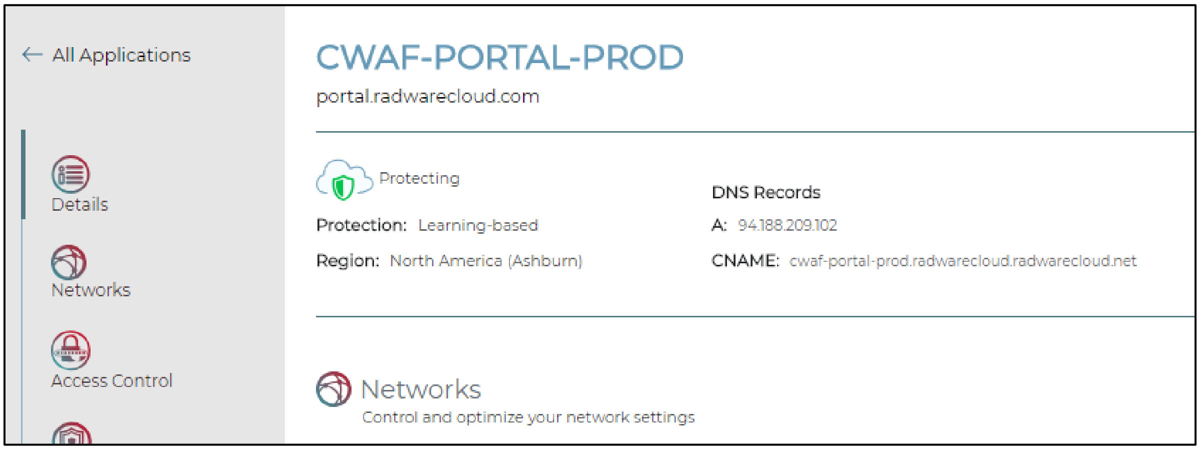
If this application is using a root domain, that need to be routed through Radware Cloud Services, point it to the following A records:

- **94.188.209.102 (A)**

Please note that changes to DNS settings may take several hours to propagate through the Internet.
After you complete the setup, traffic to this application gets routed through the Radware Cloud WAF Service, and the learning period begins. During the learning period, Cloud WAF learns the legitimate traffic patterns for your application. After learning period finishes, experts from the Radware Emergency Response Team (ERT) will contact you to set up a meeting to review the proposed configuration. After the meeting, the service can be activated.
Note: If you wish to use Radware CDN Services for this application, do not update DNS records yet. Rather, forward this email to CloudWebSec@radware.com, to complete the service onboarding. When ready, you will receive the updated DNS names that include the CDN Service.
If you have any questions, feel free to contact us at support@radware.com

© 2016 Radware Ltd. All Rights Reserved Privacy Policy Feedback Terms of Use Legal Notice Glossary

Additionally, the same information is displayed in the portal under **Settings > Applications > [select application] > Details**.



CWAF-PORTAL-PROD
portal.radwarecloud.com

Protecting

Protection: Learning-based
Region: North America (Ashburn)

DNS Records
A: 94.188.209.102
CNAME: cwaf-portal-prod.radwarecloud.radwarecloud.net

Networks
Control and optimize your network settings

You are required to point your application's authoritative DNS servers to Cloud WAF by adding the DNS records as listed in the e-mail and the portal. DNS translates the hostname, such as www.mysite.com, to the IP address of the origin server that is hosting the application. DNS changes might take a few hours to propagate over the Internet.

Once DNS diversion is done, you can see it using nslookup, for example:

```
> nslookup portal.radwarecloud.com

Non-authoritative answer:
Name:    cwaf-portal-prod.radwarecloud.radwarecloud.net
Address:  94.188.209.102
Aliases:  portal.radwarecloud.com
```

Notes:

- Before changing your DNS server settings, Radware recommends testing the service connectivity locally—using your local host static settings (hostfile) to point traffic through the Cloud WAF Service.
- To learn more about how to perform DNS diversion, you can use this article.

Learning Traffic Patterns

Once the DNS settings are updated, requests sent to your application pass through Radware Cloud WAF Service and only then get sent over to the origin server(s). Real traffic to your application enables the service to initiate the traffic-learning period in order to set up and refine the Negative and Positive Security Models.

During the learning period, Radware Cloud WAF Service creates the positive security policies based on the application transactions—on top of the out-of-the-box negative security policies. The learning period takes usually 1–2 weeks, depending on traffic volume.

During the learning period:

- DoS/DDoS protection is fully operational. Your application is immediately protected from DoS/DDoS attacks.
- WAF Protection works in passive mode. Cloud WAF monitors traffic to your application servers and responses to clients, learns legitimate traffic patterns, and generates events for detected security breaches. However, application traffic is not blocked.

Important: For Cloud WAF to be able to effectively learn the legitimate traffic patterns for your application, it is crucial that, as much as possible, traffic representing the real traffic patterns of the service go through Cloud WAF.

Best practices:

During the learning period:

- Let your Application QA team run the main business flows through the system.
- Cover special flows, such as end-of-quarter tasks, admin pages, and so on.

Reviewing the Learned Policies with ERT

As soon as enough traffic goes through the service, cloud WAF is ready to actually protect your application.

A Radware Emergency Response Team (ERT) representative will contact you to review the learned protection policy. Once reviewed and confirmed, WAF protection for the application is turned on to be active, and the state of the application changes to *Protecting*.

Best Practice: During the review with ERT, review the events generated for the IP addresses used by your testing team.

Your Application is Now Protected!

You are all set. Your application is now protected against both Web Application attacks and DoS attacks!

For additional security, to eliminate direct origin attacks, Radware recommends using a firewall on your side to allow only Cloud WAF to access the application origin server directly. The service IP addresses can be requested from ERT.

Important: Even after the review with ERT, it is possible that false positives occur.

Best practices:

- If false positives occur, refine the *Security Events* as soon as possible—to allow similar future activities and avoid any business interruption.
- Let your Application QA team run again the main business flows through the system.

About Negative and Positive Security Models

Typically, Web-application protection includes a *negative security model*, which defines what is disallowed, while implicitly allowing everything else. Relying solely on negative security models, as is the case with most other cloud WAF services, offers only partial protection against zero-day attacks, as well as OWASP Top 10 risks.

Blocking zero-day attacks, which are previously unseen attacks, requires a different approach. A *positive security model*, which defines the set of allowed requests, is required to provide proper protection where signature-based protection cannot fill the gap. The idea is to identify the legitimate traffic to the application—and to profile the application based on that traffic. However, using such security models requires defining policies and rules that can sometimes be labor intensive and require constant updates, because the application is always changing

Radware Cloud WAF Service provides both security models:

- The negative security model, which is signature based, and Radware Vulnerability Research Team (VRT) constantly generates up-to-date signatures against known vulnerabilities.
- The positive security model, which includes automated learning for new, unknown, zero-day attacks. Automated learning reduces the cost of ownership and avoids human errors associated with manual processes. Automatic policy-generation technology introduces machine-learning capabilities for automatic rule definition and maintenance.

To learn more, see Technology Behind Radware's Web Application Security Solutions.

MANAGING THE APPLICATION LIVECYCLE

This section describes frequent use cases when managing the application lifecycle.

Note: You can perform the configuration updates described in this section even when the application is in the Provisioning state.

Updating the Origin Servers Configuration

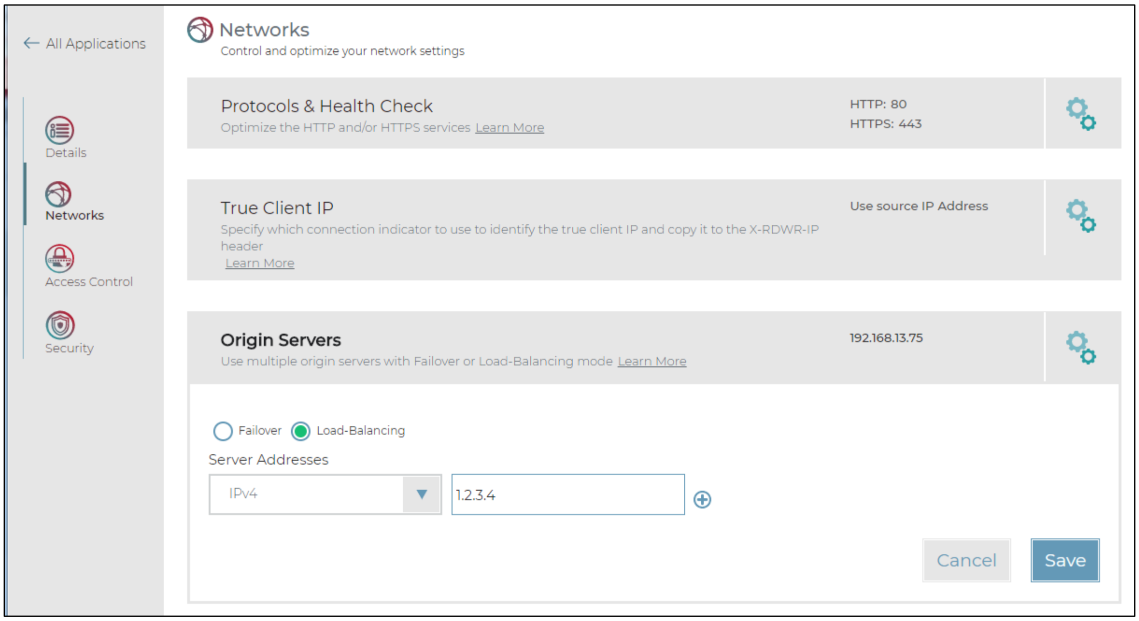
To update how the Application communicates with your origin servers, go to **Settings > Applications > [select application] > Networks > Origin Servers**.

Each Application uses one or more origin servers that serve the Application requests. A single server represents an IP address or Fully Qualified Domain Name (FQDN) of a single entity, which can be a single server or a cluster of servers.

The specified **Application Mode** determines how the Application communicates with your origin servers.

Cloud WAF supports the following Application Modes:

- **Failover**—The Application uses a primary and a secondary origin server. When the result of the health check for the primary origin server is *Not Available*, the secondary origin server begins addressing the application requests.
- **Load-Balancing**—The Application uses one or more origin servers. Up to eight servers can be set. When more than a single origin server is set, Cloud WAF uses the round-robin method to choose the available server.



Networks

Control and optimize your network settings

Protocols & Health Check

Optimize the HTTP and/or HTTPS services

HTTP: 80
HTTPS: 443

True Client IP

Specify which connection indicator to use to identify the true client IP and copy it to the X-RDWR-IP header

Use source IP Address

Origin Servers

Use multiple origin servers with Failover or Load-Balancing mode

192.168.13.75

○ Failover ● Load-Balancing

Server Addresses

IPv4 ▼ 1.2.3.4 ⊕

Note: Server addresses can be specified using IP address or FQDN.

Updating the Application Protocols Settings

To update the Application's network protocol support, go to **Settings > Applications > [select application] > Networks > Protocols & Health Check**

You can update the following parameters to control the Application's supported protocols:

- **HTTP**—Select this checkbox to specify that the application is accessible to clients over HTTP.

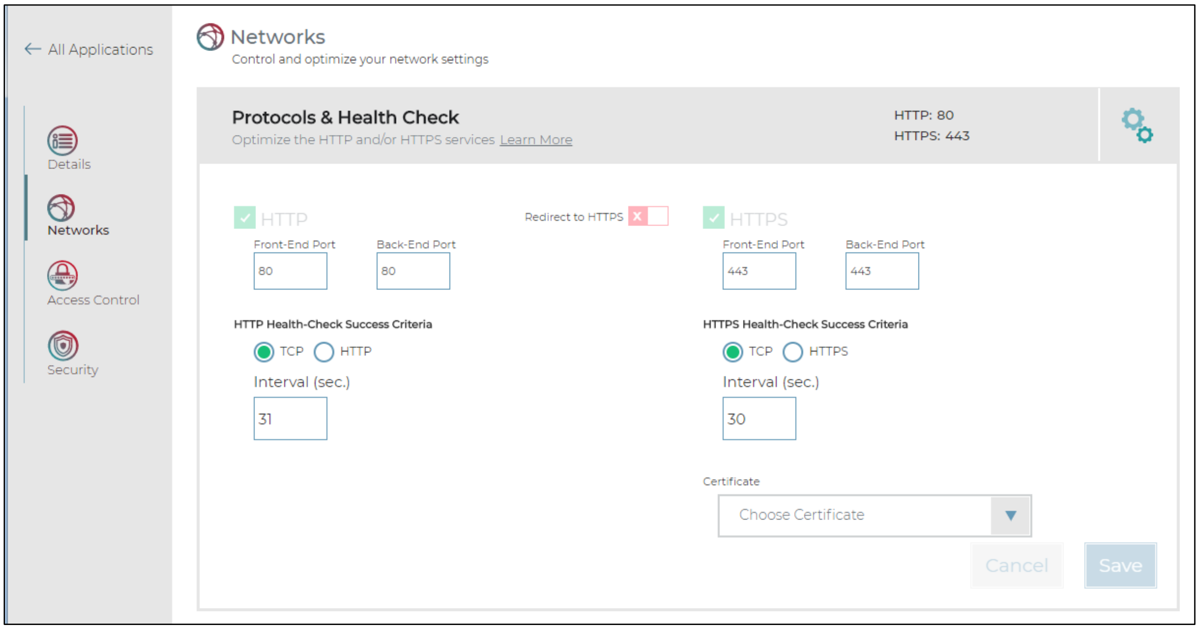
  When the **HTTP** checkbox is selected, you can configure the following related parameters:

  - **Redirect to HTTPS**—Enable this parameter to drive all traffic to the secure channel (SSL). When enabled, clients accessing your application using HTTP over port 80 are redirected to HTTPS port 443.
  - **Backend Port**—The TCP port for the origin-server HTTP connection.
  - To learn more about setting health check parameters, see below.

- **HTTPS**—Select this checkbox to specify that the application is accessible to clients over HTTPS.

  When the **HTTPS** checkbox is selected, you can configure the following related parameters:

  - **Backend Port**—The TCP port for the origin-server HTTPS connection.
  - **Certificate**—The certificate to be used for the application.
  - ***Health-check parameters***—To learn about setting health-check parameters, see below.



Networks
Control and optimize your network settings

Protocols & Health Check
Optimize the HTTP and/or HTTPS services Learn More

HTTP: 80
HTTPS: 443

☑ HTTP

Redirect to HTTPS ☒

Front-End Port: 80
Back-End Port: 80

HTTP Health-Check Success Criteria
● TCP ○ HTTP

Interval (sec.): 31

☑ HTTPS

Front-End Port: 443
Back-End Port: 443

HTTPS Health-Check Success Criteria
● TCP ○ HTTPS

Interval (sec.): 30

Certificate: Choose Certificate ▼

If you are using a CDN or another proxy in front of Cloud WAF, and your application needs to see the true client IP address, see here.

Updating Application Health Checks

To update how the Application's health is checked with each protocol, go to **Settings > Applications > [select application] > Networks > Protocols & Health Check**.

You can update the following parameters to control the Application's health checks—for HTTP and for HTTPS:

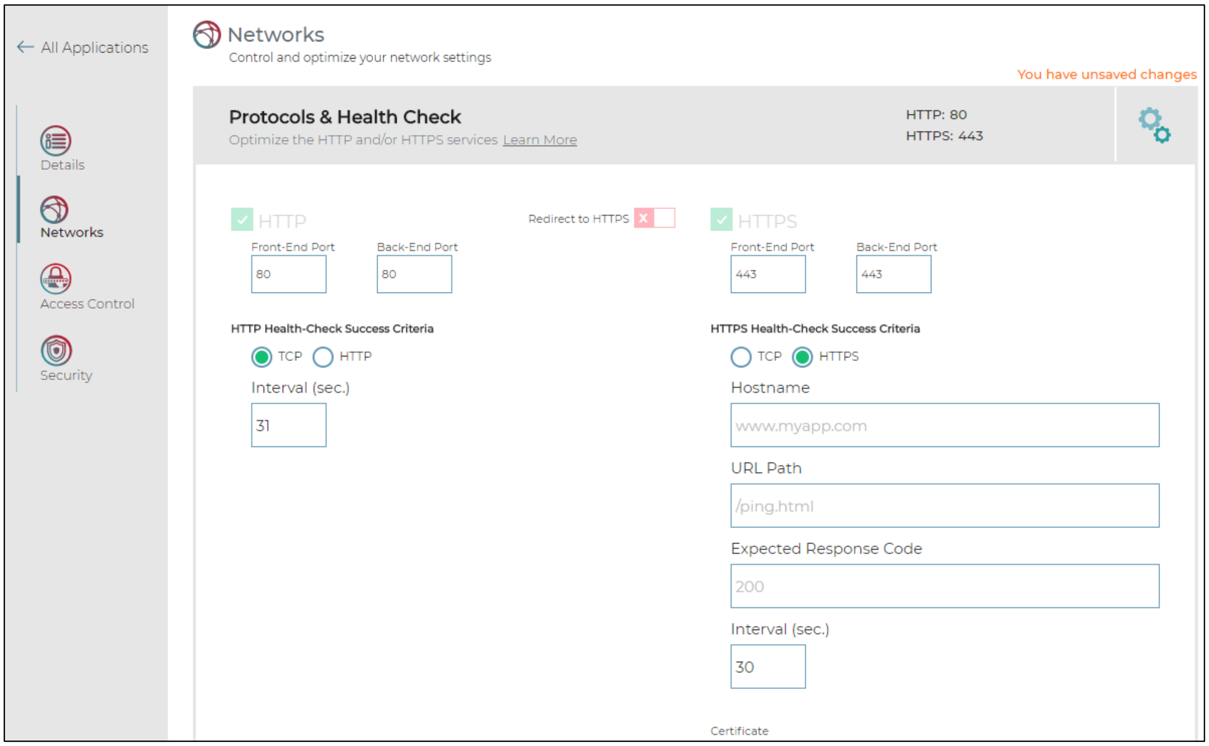
- **Health-Checks Success Criteria**—TCP or application-level check (HTTP or HTTPS). This defines the success criteria for determining whether the Application is available for the specified protocol. The health-checks are tested against the origin servers.

  For TCP Health check:

  - **Interval**—The time, in seconds, between health checks.

  For HTTP/S Health check:

  - **Hostname**—The host header in the health-check HTTP request. Example: **www.myapp.com**
  - **URL Path**—The HTTP/S path that is checked on the origin server. Example: **"/index.html"**
  - **Expected Response Code**—The expected HTTP response code from a healthy origin server.
  - **Interval**—The time, in seconds, between health checks.



Networks

Control and optimize your network settings

You have unsaved changes

Protocols & Health Check

Optimize the HTTP and/or HTTPS services Learn More

HTTP: 80
HTTPS: 443

☑ HTTP

Redirect to HTTPS ☒

Front-End Port: 80
Back-End Port: 80

☑ HTTPS

Front-End Port: 443
Back-End Port: 443

HTTP Health-Check Success Criteria

● TCP ○ HTTP

Interval (sec.): 31

HTTPS Health-Check Success Criteria

○ TCP ● HTTPS

Hostname: www.myapp.com

URL Path: /ping.html

Expected Response Code: 200

Interval (sec.): 30

Certificate

Configuring True Client IP Support

When forwarding requests to your origin servers, Cloud WAF changes the source IP address in the request.

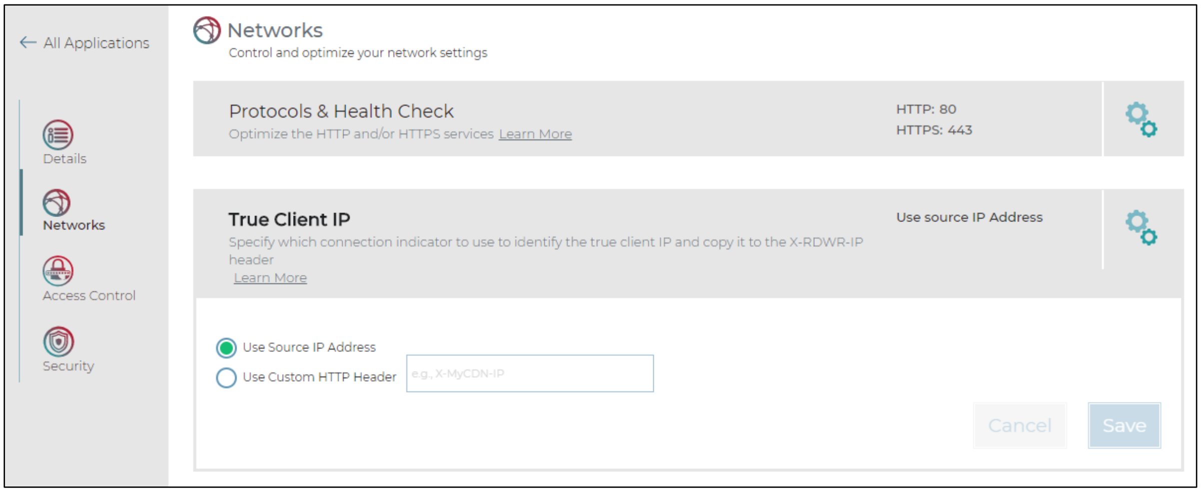
By default, Cloud WAF adds the following headers to each transaction that is forwarded to the origin-servers:

- **X-RDWR-PORT**—Specifies the TCP port of the incoming transaction. Example: 15234
- **X-RDWR-IP**—Specifies the source IP address of the incoming transaction. Example: 1.2.3.4

When using a CDN, or some other proxy in front of Cloud WAF, the origin server may need to know the true client IP address, rather than the IP address of the transaction that was received by Cloud WAF.

In the **Settings > Applications > [select application] > Networks > True Client IP** section, you can choose one of the following options to specify how Radware Cloud Service populates the **X-RDWR-IP** header:

- **Source IP Address** (default)—Radware Cloud Service populates the **X-RDWR-IP** header with the source IP address.
- **Custom HTTP Header**—Radware Cloud Service populates the **X-RDWR-IP** header with value from the specified HTTP Header. For example, when set to **CUSTOM-CDN-FORWARDED-FOR**, the value of this header is in the client request as received by Cloud WAF is used for X-RDWR-IP.



Networks

Control and optimize your network settings

Protocols & Health Check

Optimize the HTTP and/or HTTPS services Learn More

HTTP: 80
HTTPS: 443

True Client IP

Specify which connection indicator to use to identify the true client IP and copy it to the X-RDWR-IP header

Learn More

Use source IP Address

● Use Source IP Address
○ Use Custom HTTP Header [e.g., X-MyCDN-IP]

Note: The value of the True Client IP will be copied to the Radware X-RDWR-IP header value and forwarded to the origin-servers. Additionally, IP-based features in Cloud WAF, such as the Access Rules, will be classified based on the value of the True Client IP.

Update a Certificate

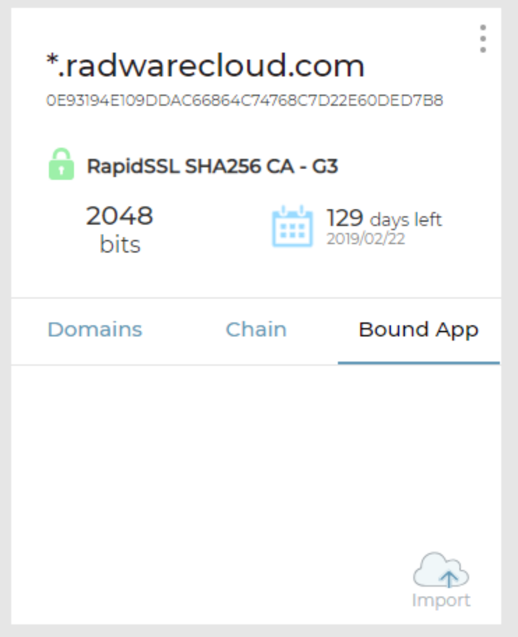
Sometimes, it is required to update the certificate used for an existing Web application—typically, when a certificate expires, or due to some other reason. You can use the Cloud WAF portal to do this yourself.

You can update a certificate from the following two places:

- **Settings > Applications > [select application] > Networks > Protocols & Health checks**. When the HTTPS protocol is selected, use the **Certificate** drop-down list, choose a certificate, and save the changes. The selected certificate bundle will be bound to the application.
- You can replace the certificate used by an application, for example, when the certificate expires.

To replace the certificate bound to one or more of your applications

1. Go to **Settings > Certificates** and select the new certificate.



*.radwarecloud.com

0E93194E109DDAC66864C74768C7D22E60DED7B8

RapidSSL SHA256 CA - G3

2048 bits

129 days left 2019/02/22

2. Select **Bound App**, and then click the **Import** icon.
3. From the **Certificate** drop-down list that is displayed, choose the certificate to be replaced.
4. Save the changes. The applications from the selected certificate will be associated to the current certificate bundle, and will stop using their previously bound certificates.

Note: An Application can have only one Certificate bound to it. You can bind a Certificate in the list to one or more of your Applications.

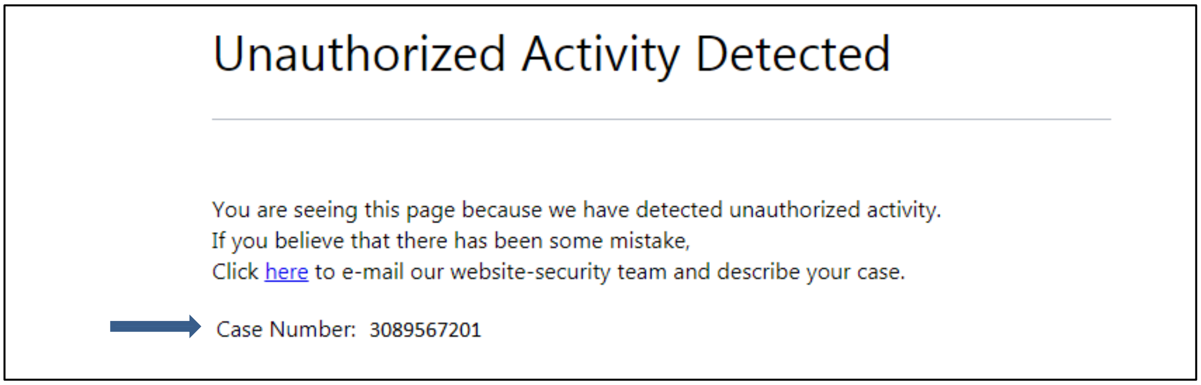
Setting Exceptions to Handle False Positives

It may happen that Cloud WAF mistakenly identifies a valid client request as an attack, and the request is blocked. This is called a *false positive*. In such cases, you must create an exception for the legitimate request, so that the request is allowed, and not blocked.

Cloud WAF lets customers address false positives of application-level attacks in a simple, self-service action, through the Cloud portal.

Allowing Requests that Were Blocked

When a user is blocked, the user receives a page that looks like the following:



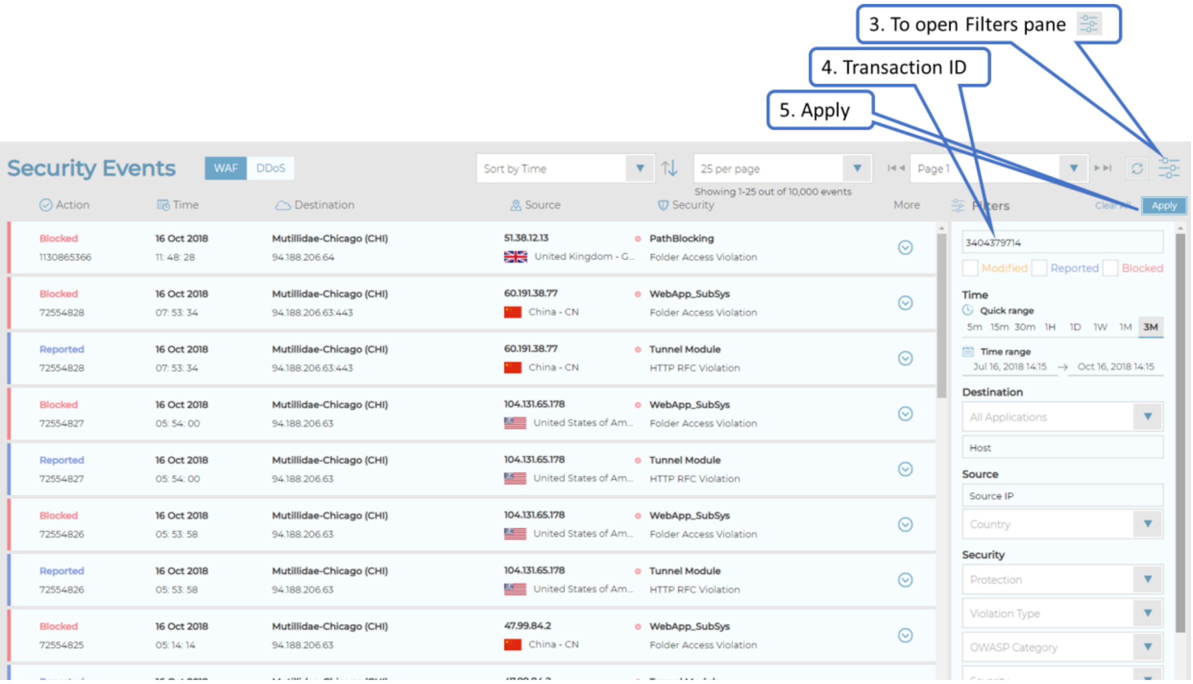
Unauthorized Activity Detected

You are seeing this page because we have detected unauthorized activity.
If you believe that there has been some mistake,
Click here to e-mail our website-security team and describe your case.

Case Number: 3089567201

To allow requests that Radware Cloud WAF blocked

1. Copy the Case Number to the clipboard—as shown in the figure above.
2. Go to the *Security Events* screen.
3. Click the filter button (⚙).
4. In the *Filter* pane, paste the Case Number into the **Transaction ID** field.
5. Click **Apply** to filter the events. Make sure that the time filter at the top of the screen shows the correct time that the event happened.



3. To open Filters pane

4. Transaction ID

5. Apply

Security Events — WAF | DDoS — Sort by Time — 25 per page — Page 1

Showing 1-25 out of 10,000 events

Action	Time	Destination	Source	Security	More
Blocked 1130865366	16 Oct 2018 11: 48: 28	Mutillidae-Chicago (CHI) 94.188.206.64	51.38.12.13 United Kingdom - G...	PathBlocking Folder Access Violation	⌄
Blocked 72554828	16 Oct 2018 07: 53: 34	Mutillidae-Chicago (CHI) 94.188.206.63:443	60.191.38.77 China - CN	WebApp_SubSys Folder Access Violation	⌄
Reported 72554828	16 Oct 2018 07: 53: 34	Mutillidae-Chicago (CHI) 94.188.206.63:443	60.191.38.77 China - CN	Tunnel Module HTTP RFC Violation	⌄
Blocked 72554827	16 Oct 2018 05: 54: 00	Mutillidae-Chicago (CHI) 94.188.206.63	104.131.65.178 United States of Am...	WebApp_SubSys Folder Access Violation	⌄
Reported 72554827	16 Oct 2018 05: 54: 00	Mutillidae-Chicago (CHI) 94.188.206.63	104.131.65.178 United States of Am...	Tunnel Module HTTP RFC Violation	⌄
Blocked 72554826	16 Oct 2018 05: 53: 58	Mutillidae-Chicago (CHI) 94.188.206.63	104.131.65.178 United States of Am...	WebApp_SubSys Folder Access Violation	⌄
Reported 72554826	16 Oct 2018 05: 53: 58	Mutillidae-Chicago (CHI) 94.188.206.63	104.131.65.178 United States of Am...	Tunnel Module HTTP RFC Violation	⌄
Blocked 72554825	16 Oct 2018 05: 14: 14	Mutillidae-Chicago (CHI) 94.188.206.63	47.99.84.2 China - CN	WebApp_SubSys Folder Access Violation	⌄

Filters — Clear All — Apply

3404379714

□ Modified □ Reported □ Blocked

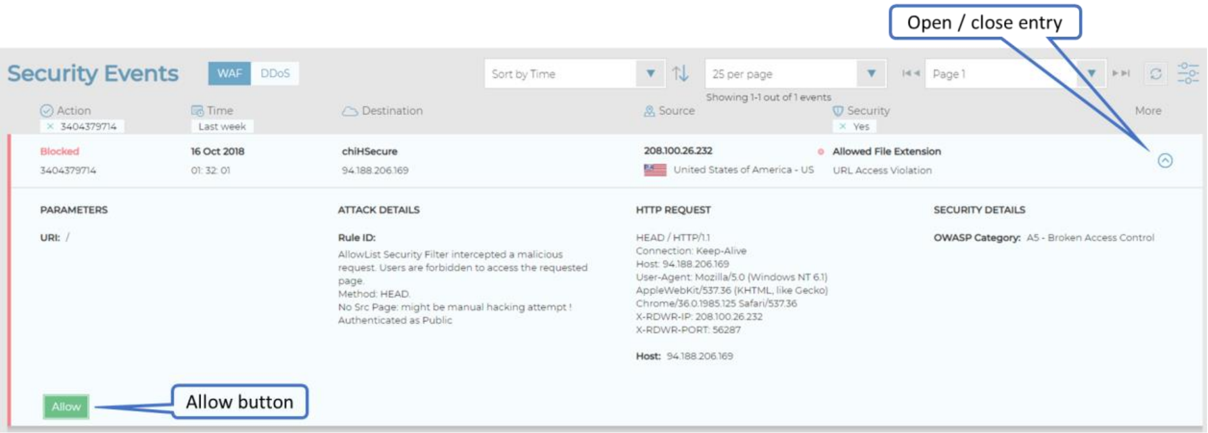
Time
Quick range: 5m 15m 30m 1H 1D 1W 1M 3M
Time range: Jul 16, 2018 14:15 → Oct 16, 2018 14:15

Destination
All Applications
Host

Source
Source IP
Country

Security
Protection
Violation Type
OWASP Category

6. Click ⌄ to open the event entry.
7. If the event can be allowed, click **Allow** on an event to add an exception for transactions of the same type to the relevant module on the WAF policy.


Open / close entry

Blocked
3404379714
16 Oct 2018
01: 32: 01
chiHSecure
94.188.206.169
208.100.26.232
United States of America - US
Allowed File Extension
URL Access Violation

PARAMETERS

URI: /

ATTACK DETAILS

Rule ID:
AllowList Security Filter intercepted a malicious request. Users are forbidden to access the requested page.
Method: HEAD.
No Src Page: might be manual hacking attempt !
Authenticated as Public

HTTP REQUEST

```
HEAD / HTTP/1.1
Connection: Keep-Alive
Host: 94.188.206.169
User-Agent: Mozilla/5.0 (Windows NT 6.1)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/36.0.1985.125 Safari/537.36
X-RDWR-IP: 208.100.26.232
X-RDWR-PORT: 56287
```

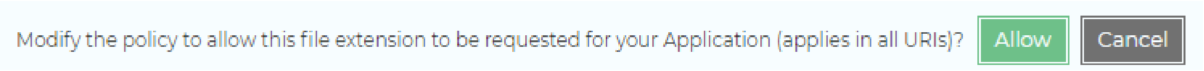
Host: 94.188.206.169

SECURITY DETAILS

OWASP Category: A5 - Broken Access Control

Allow button

You will get a confirmation request, depending on event type it can be something like the following:


Modify the policy to allow this file extension to be requested for your Application (applies in all URIs)?

Once confirmed, the following is displayed: **Allow request was sent. Status: loading**

After the allow request is implemented, the following is displayed: **Allow request was sent. Status: succeeded**

8. As necessary, you can monitor the Activity Log to see status of Allow requests.

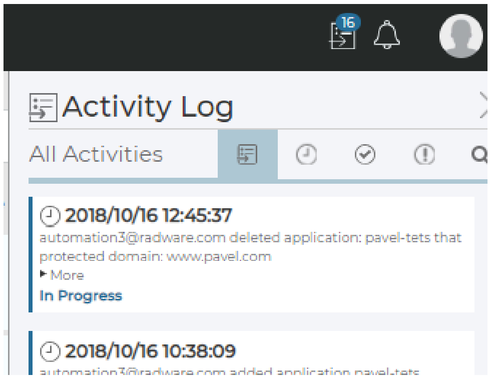
Which Events Can Be Allowed?

Each event has a searchable preference called **Can Be Allowed** with the following values:

- **Yes—**Events that were identified as injections, cross-site-scripting, vulnerabilities, and more will display the **Allow** button that supports this feature.
- **No—**Events that do not support this feature from Cloud WAF portal can be allowed by contacting the support team (support@radware.com).
- **Was Allowed—**Events for which an **Allow** request was already sent.

Monitoring the Status of Allow Requests

You can monitor status of *Allow* requests and other activities in the Activity Log by clicking the ▤ icon on the left side of the screen.



Activity Log

All Activities

2018/10/16 12:45:37
automation3@radware.com deleted application: pavel-tets that protected domain: www.pavel.com
▸ More
In Progress

2018/10/16 10:38:09
automation3@radware.com added application pavel-tets

After an action succeeded or failed, you can see the status within the event details.

Note: After an Allow request is sent, the maximum time for policy-change enforcement is 10 minutes.

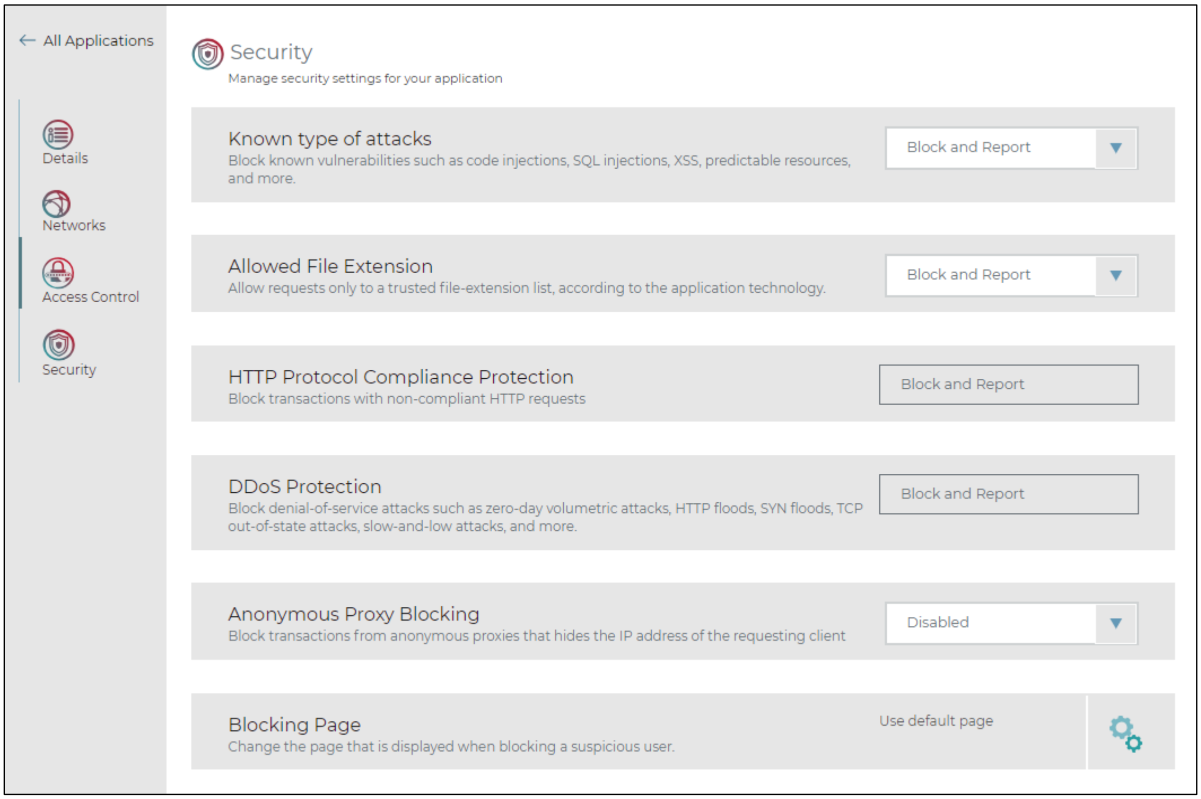
Managing Security Settings Applied to Your Application

You can manage which security modules are applied to your applications and specify the mode of each security module: *Blocking* mode or *Report Only* mode.

In *Blocking* mode, the security module actively protects your application, blocking requests and responses to your application that have been identified as malicious.

When a security module is working in *Report Only* mode, Cloud WAF monitors traffic to your application servers and responses to clients, learns legitimate traffic patterns, and generates events for detected security breaches. However, application traffic is not blocked.

Using *Report Only* mode allows you to fine-tune the learned security policies before activating them, thus minimizing false positives.



Security
Manage security settings for your application

Known type of attacks
Block known vulnerabilities such as code injections, SQL injections, XSS, predictable resources, and more.
Block and Report ▼

Allowed File Extension
Allow requests only to a trusted file-extension list, according to the application technology.
Block and Report ▼

HTTP Protocol Compliance Protection
Block transactions with non-compliant HTTP requests
Block and Report

DDoS Protection
Block denial-of-service attacks such as zero-day volumetric attacks, HTTP floods, SYN floods, TCP out-of-state attacks, slow-and-low attacks, and more.
Block and Report

Anonymous Proxy Blocking
Block transactions from anonymous proxies that hides the IP address of the requesting client
Disabled ▼

Blocking Page
Change the page that is displayed when blocking a suspicious user.
Use default page

To manage Security Modules

- Go to **Settings > Applications > [select application] > Security**.

Note: In the Events view in the portal, you can see the security module that detected each event, in the Protection parameter.

Controlling the Page Displayed to Blocked Transactions

A Blocking-Page is an error page displayed when a user accessing the application is blocked due to security rules. Radware Cloud WAF Service provides a default out-of-the-box blocking-page. The default blocking-page includes security related information, such as transaction ID, which can be used for further forensics, and accurate handling of false positives.

The application owner may prefer to customize the blocking-page, and provide extended information. For example, the page textual content can help the user to understand that their request was identified as an attack, and can point them to the relevant contact person who can help the user resolve false positives, using the cloud portal.

To manage the page displayed to blocked transactions

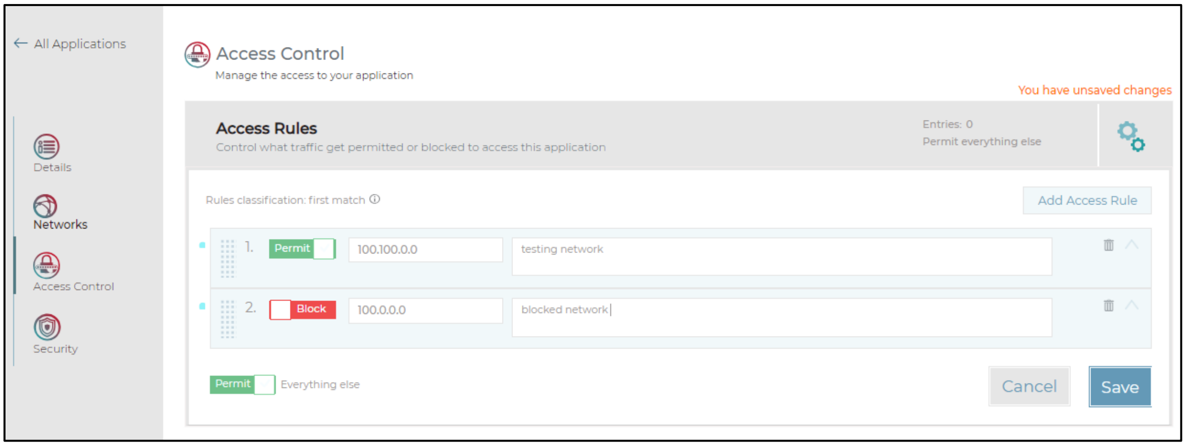
- Go to **Settings > Applications > [select application] > Security**.

Controlling Who Can Access Your Application

Using *Access Control*, you can control who gets access to your application. You can define rules to block or permit incoming traffic, classified by a specified order. Each entry sets the behavior for incoming traffic sources. You can configure an entry as an IP address (for example, 1.1.1.1) or a CIDR (for example, 1.1.1.0/24), and whether that traffic is blocked or allowed. The rules are classified according to their order. Once rules are set, you can change their order using drag and drop. You can also set the default behavior when traffic does not match any entry (*Block* or *Permit*).

To manage Access Rules

- Go to **Settings > Applications > [select application] > Access Control**.



Access Control

Manage the access to your application

You have unsaved changes

Access Rules

Control what traffic get permitted or blocked to access this application

Entries: 0
Permit everything else

Rules classification: first match ⓘ

1. Permit | 100.100.0.0 | testing network

2. Block | 100.0.0.0 | blocked network

Permit Everything else

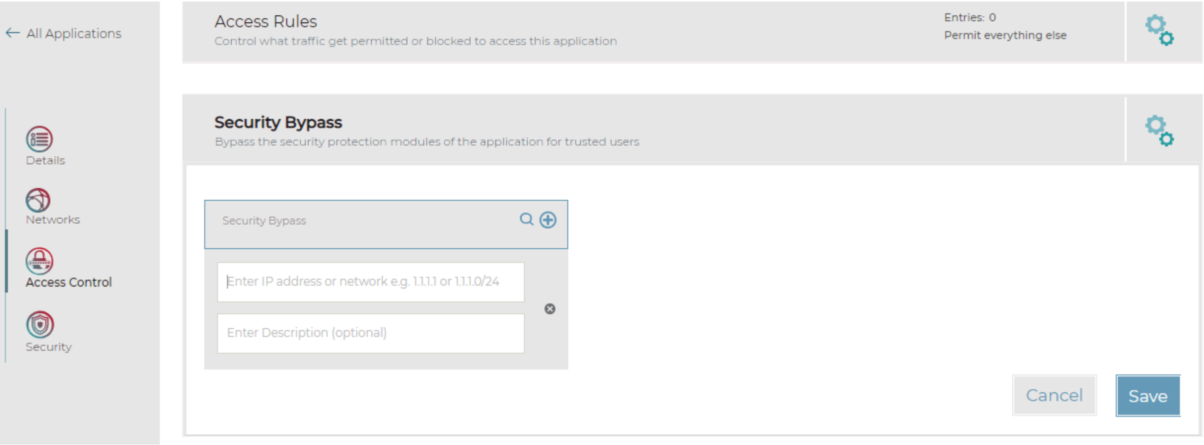
The Security Bypass feature allows specified IP addresses to bypass the service protection modules. Transactions coming from IP addresses that match the Security Bypass configuration bypass the WAF protections modules and are sent directly to the application origin servers.

The Security Bypass feature supports the following use cases:

- **Security testing**—Allow specific IP sources to access the application and bypass the security in order to test the origin server.
- **Troubleshooting**—Allow specific IP sources or all IP sources to access the application while bypassing the WAF module.

To manage Security Bypass

- Go to **Settings > Applications > [select application] > Access Control**.



Control what traffic get permitted or blocked to access this application

Bypass the security protection modules of the application for trusted users

Distributing Security Policies Between Applications

Using *Policy Distributions*, you can distribute security-policy configurations across your applications. The security-policy configurations include the Application protection states and all the changes that occurred on the policy due to “Allow” activity and due to learning period.

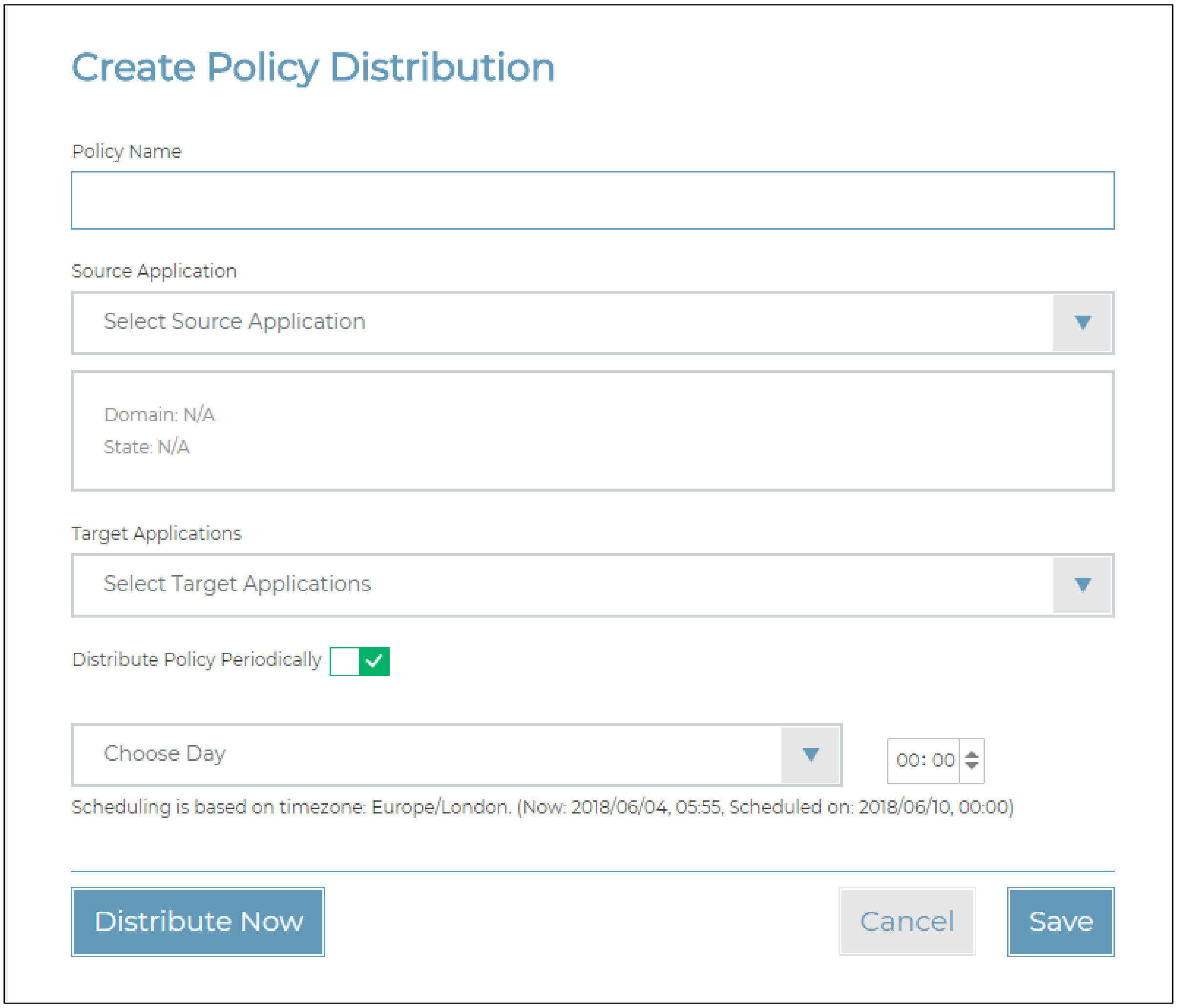
With the Policy Distribution feature, you can manage application-security configurations across an organization—for example:

- Distribute configuration from QA/staging to production
- Distribute configuration between similar functioning applications

To conform to the organization’s development and deployment processes, Security Policy Distributions can be initiated manually—in an on-demand manner, or scheduled on a weekly basis, on a day, and at a time of your choosing.

To manage Policy Distributions for your applications

- Go to **Settings > Policy Distributions**.



Create Policy Distribution

Policy Name

Source Application

Select Source Application ▼

Domain: N/A
State: N/A

Target Applications

Select Target Applications ▼

Distribute Policy Periodically ✓

Choose Day ▼ 00: 00

Scheduling is based on timezone: Europe/London. (Now: 2018/06/04, 05:55, Scheduled on: 2018/06/10, 00:00)

MONITORING PROTECTED APPLICATIONS

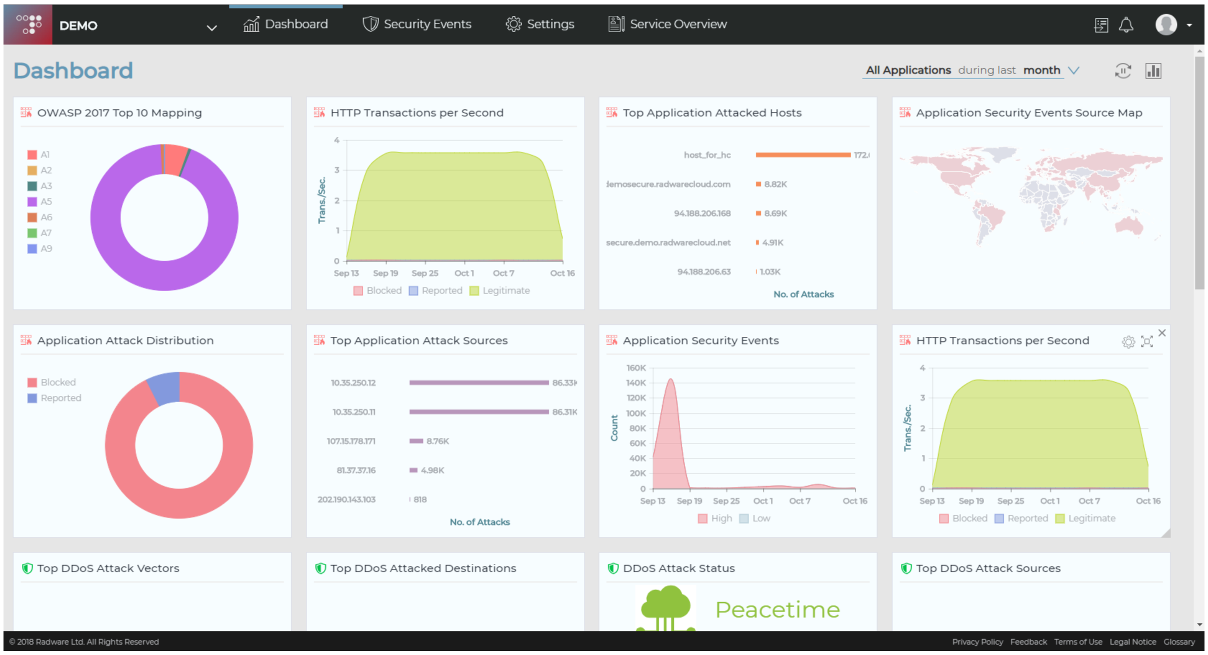
You can monitor your protected applications using the following methods:

- Real-time dashboard—Continuously displays up-to-date security metrics
- Reviewing security events—Enables you to drilldown to security events, to understand the threats behind the events, and allow security-policy exceptions to handle false positives.
- Application Insights—Aggregated and groups events into application activities for improved readability and handling.
- Generating periodic reports—Keeps you up to date with security threats.
- Receiving proactive alerts—Informs you of changes detected in the threat landscape of your applications.
- Exporting events to an external SIEM system—Enables you to correlate Security Events to other events coming from different tools/vendors.
- Viewing your service plans—One screen that shows service plans, their usage, and utilization.

Real-Time Dashboard

The portal *Dashboard* displays various widgets that enable visibility into Cloud WAF statistics and convey meaningful metrics and monitoring.

You can configure the display of the data. You can display all your applications, focus on a specific application, control the timeframe displayed, and more.



Available widgets include:

- *HTTP Transactions per Second* graph, over time
- Application Security Events
- Top attack sources
- Top attack destinations
- OWASP 2017 Top 10 Mapping
- Application Attack Distribution
- Application Security Events Source Map

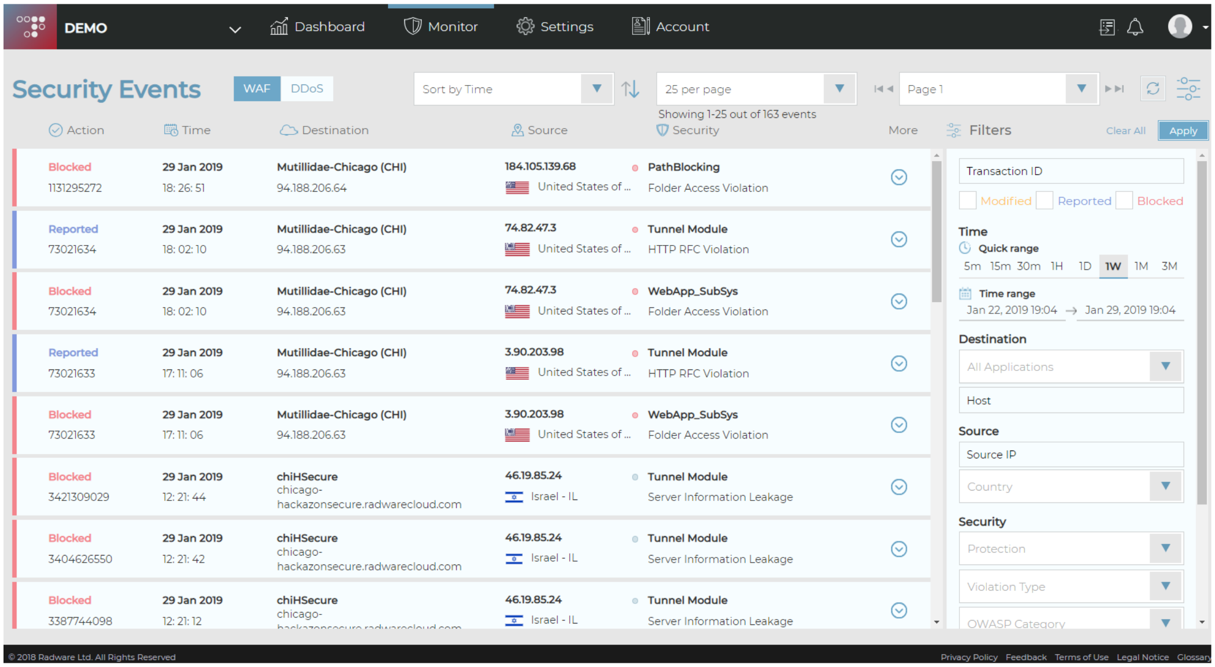
Reviewing Security Events

The *Security Events* screen displays the security events generated by Cloud WAF, enabling sorting, filtering, and reviewing each event in detail.

In the *Security Events* screen, you can do the following:

- **Filter events**—To filter events, click the ☰ button, configure the filtering criteria, and click **Apply**.
- **Sort events**—To sort events, use the left drop-down menu.
- **See detailed data about the events**—To see detailed data about an event, open click the ⌄ icon on the right side of the event.

Each event displayed may be further expanded to expose additional details, and also to allow specific events in cases of false positives.



Showing 1-25 out of 163 events

Action	Time	Destination	Source	Security
Blocked 1131295272	29 Jan 2019 18: 26: 51	Mutillidae-Chicago (CHI) 94.188.206.64	184.105.139.68 United States of ...	PathBlocking Folder Access Violation
Reported 73021634	29 Jan 2019 18: 02: 10	Mutillidae-Chicago (CHI) 94.188.206.63	74.82.47.3 United States of ...	Tunnel Module HTTP RFC Violation
Blocked 73021634	29 Jan 2019 18: 02: 10	Mutillidae-Chicago (CHI) 94.188.206.63	74.82.47.3 United States of ...	WebApp_SubSys Folder Access Violation
Reported 73021633	29 Jan 2019 17: 11: 06	Mutillidae-Chicago (CHI) 94.188.206.63	3.90.203.98 United States of ...	Tunnel Module HTTP RFC Violation
Blocked 73021633	29 Jan 2019 17: 11: 06	Mutillidae-Chicago (CHI) 94.188.206.63	3.90.203.98 United States of ...	WebApp_SubSys Folder Access Violation
Blocked 3421309029	29 Jan 2019 12: 21: 44	chiHSecure chicago-hackazonsecure.radwarecloud.com	46.19.85.24 Israel - IL	Tunnel Module Server Information Leakage
Blocked 3404626550	29 Jan 2019 12: 21: 42	chiHSecure chicago-hackazonsecure.radwarecloud.com	46.19.85.24 Israel - IL	Tunnel Module Server Information Leakage
Blocked 3387744098	29 Jan 2019 12: 21: 12	chiHSecure chicago-	46.19.85.24 Israel - IL	Tunnel Module Server Information Leakage

Transaction ID

□ Modified □ Reported □ Blocked

Time

Quick range: 5m 15m 30m 1H 1D [✓ 1W] 1M 3M

Time range: Jan 22, 2019 19:04 → Jan 29, 2019 19:04

Destination

All Applications

Host

Source

Source IP

Country

Security

Protection

Violation Type

OWASP Category

© 2018 Radware Ltd. All Rights Reserved

Privacy Policy Feedback Terms of Use Legal Notice Glossary

Application Insights

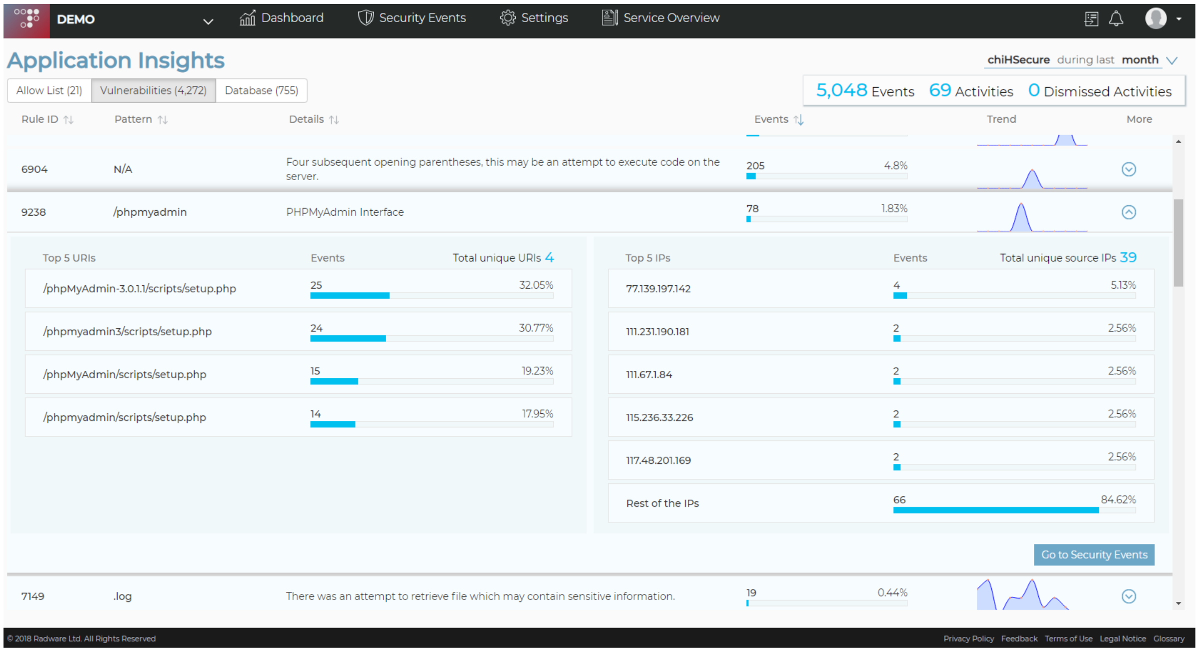
Application Insights aggregate and group events into application activities for improved readability and handling.

Using Application Insights enables you to gain:

- **Visibility**—Application Insights consolidates a large number of events into a small number of manageable activities.
- **Agility**— Application Insights reduces log overload and helps administrators focus on high-priority alerts.
- **Control**—Application Insights gives context regarding an application's behavior for rapid troubleshooting.

To access Application Insights

- Navigate to **Security Events > Application Insights**, and select an application.



Application Insights

chiHSecure during last month

5,048 Events 69 Activities 0 Dismissed Activities

Rule ID	Pattern	Details	Events		Trend	More
6904	N/A	Four subsequent opening parentheses, this may be an attempt to execute code on the server.	205	4.8%		
9238	/phpmyadmin	PHPMyAdmin Interface	78	1.83%		
7149	.log	There was an attempt to retrieve file which may contain sensitive information.	19	0.44%		

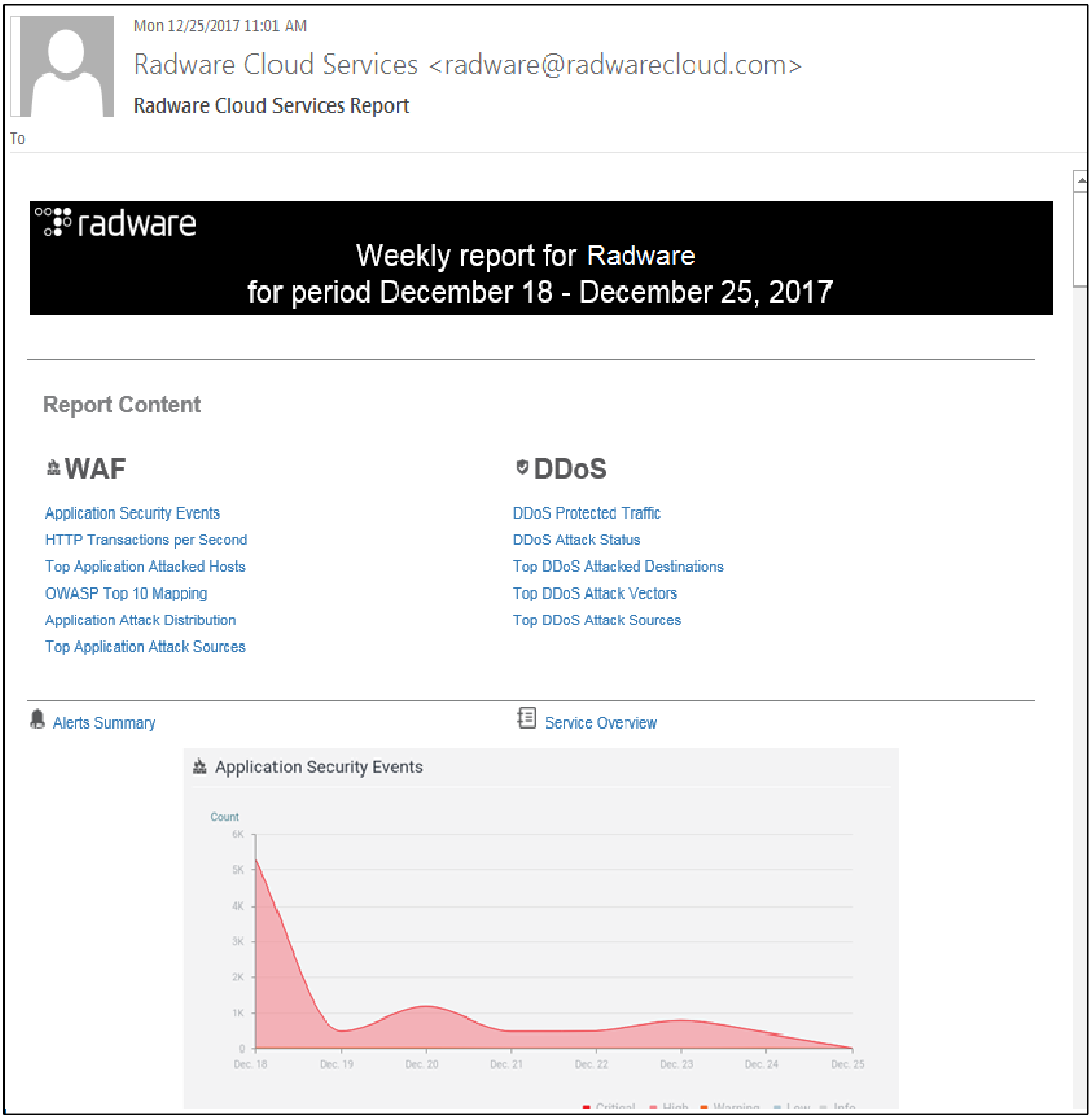
Top 5 URIs	Events	Total unique URIs 4
/phpMyAdmin-3.0.1.1/scripts/setup.php	25	32.05%
/phpmyadmin3/scripts/setup.php	24	30.77%
/phpMyAdmin/scripts/setup.php	15	19.23%
/phpmyadmin/scripts/setup.php	14	17.95%

Top 5 IPs	Events	Total unique source IPs 39
77.139.197.142	4	5.13%
111.231.190.181	2	2.56%
111.67.1.84	2	2.56%
115.236.33.226	2	2.56%
117.48.201.169	2	2.56%
Rest of the IPs	66	84.62%

Generating Periodic Reports

Radware Cloud WAF Service customers can receive periodical reports to gain visibility and insight into security threats to their applications over the last week or month. Reports are generated automatically according to the preferred time period, and provide an easy-to-read, up-to-date graphical display of the WAF and DDoS protection provided.

Customers can set the time period of the scheduled reports—weekly or monthly, and update the list of e-mail recipients. Reports can be scheduled and sent by e-mail.



Mon 12/25/2017 11:01 AM

Radware Cloud Services <radware@radwarecloud.com>

Radware Cloud Services Report

To

radware

Weekly report for Radware
for period December 18 - December 25, 2017

Report Content

WAF

- Application Security Events
- HTTP Transactions per Second
- Top Application Attacked Hosts
- OWASP Top 10 Mapping
- Application Attack Distribution
- Top Application Attack Sources

DDoS

- DDoS Protected Traffic
- DDoS Attack Status
- Top DDoS Attacked Destinations
- Top DDoS Attack Vectors
- Top DDoS Attack Sources

Alerts Summary

Service Overview

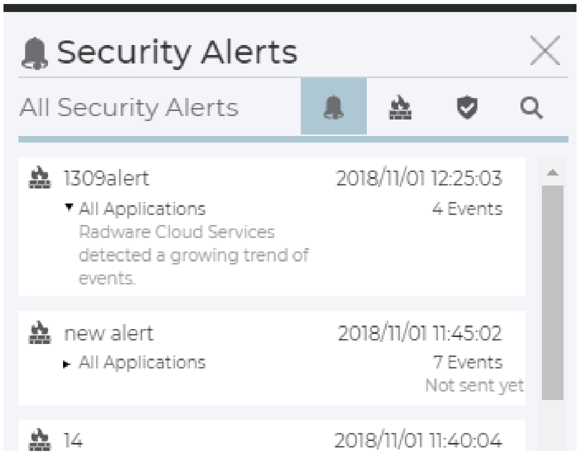
Application Security Events

Receiving Proactive Alerts

You can configure Alerts to notify you when the service detects a rising trend of Security Events or a growing trend of DDoS-attack traffic.

To detect anomalies, Radware Cloud WAF monitors and learns the baseline rate of WAF events and the volume of DDoS-attack traffic.

An alert is triggered when there is a steep rise in the rate of WAF events or the volume of DDoS-attack traffic. Cloud WAF sends alerts as e-mail notifications. The alerts are also visible through the portal dashboard, by clicking the 🔔 button



Security Alerts

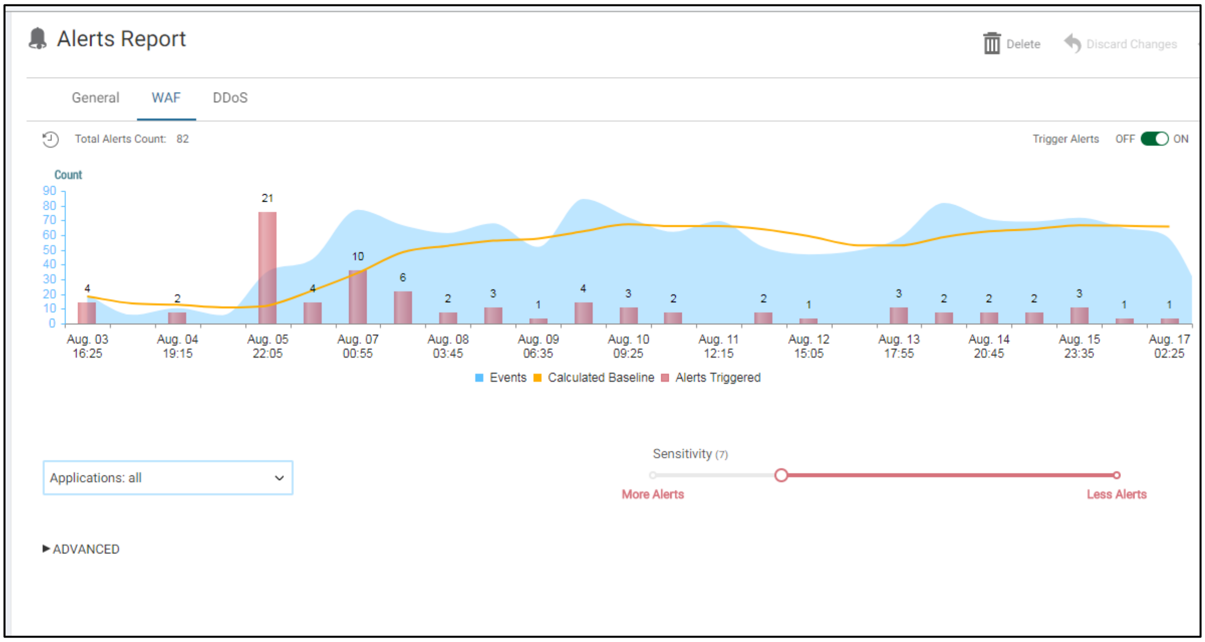
All Security Alerts

1309alert 2018/11/01 12:25:03
▾ All Applications 4 Events
Radware Cloud Services detected a growing trend of events.

new alert 2018/11/01 11:45:02
▸ All Applications 7 Events
Not sent yet

14 2018/11/01 11:40:04

The alerts configuration is available under **Settings > Alerts**.



Alerts Report

Total Alerts Count: 82

Trigger Alerts OFF ON

Applications: all

Sensitivity (7)

Exporting Events to a SIEM System

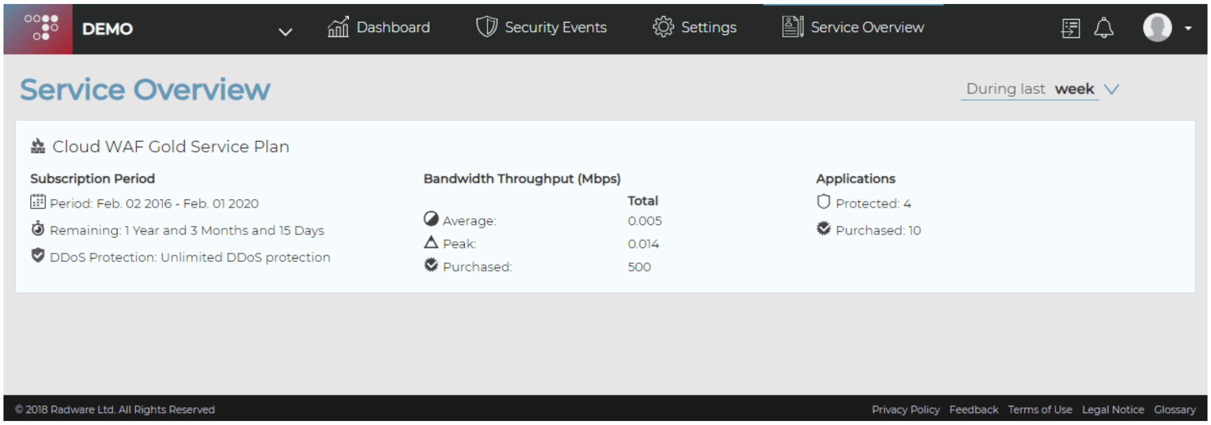
Radware Cloud WAF continuously collects detailed security logs to track security events and activities in customer applications. SIEM integration enables organizations to download the data from the cloud infrastructure, gain visibility into the data within their SIEM solution, and get a comprehensive view of security events across their network in a centralized manner.

Log data for both WAF and DDoS events are provided to the customer system in near real-time. The data includes in-depth event information, such as geo-location of the attack origin, details of HTTP request, the OWASP Top-10 category, and much more.

For more information on SIEM integration and operation, see the SIEM Operation Guide.

Viewing Your Service Plans

You can view your current service plans in the *Service Overview* pane in the portal. You can see your current service plans, including the time remaining in the subscription, the usage of applications, and bandwidth usage.



Service Overview

During last week

Cloud WAF Gold Service Plan

Subscription Period
Period: Feb. 02 2016 - Feb. 01 2020
Remaining: 1 Year and 3 Months and 15 Days
DDoS Protection: Unlimited DDoS protection

Bandwidth Throughput (Mbps)

	Total
Average:	0.005
Peak:	0.014
Purchased:	500

Applications
Protected: 4
Purchased: 10

© 2018 Radware Ltd. All Rights Reserved

APPENDIX: CLOUD SECURITY RELATED FAQ

This appendix contains the following sections:

- How Do You Keep My Certificates Secured?
- Ongoing Security Measures
- Security Standards Compliance and Certifications
- Caching and Storing of Personally Identifiable Information (PII)

How Do You Keep My Certificates Secured?

The customer uploads the required certificate-bundle data to the Radware Cloud WAF portal. The certificate-bundle data includes the following:

- **Private Key**—The certificate private key.
- **Certificate**—The certificate that signs the application.
- **Certificate Chain** (optional) —A certificate chain contains one or more intermediate certificates concatenated.
- **Passphrase** (optional)—The passphrase in cases where the key is encrypted.

The portal receives the data from the customer and passes it to the backend server. All data transfer happens over a secure channel (HTTPS).

The backend server validates the data (verifies that the certificate is valid, matches the private key, is signed by the intermediate CA, and so on).

Once validated, the backend server uploads the data to a secure vault over a secure channel (HTTPS). In the secure vault, the sensitive data is encrypted at rest with AES 256, and the encryption key for this encryption is stored on a dedicated physical hardware security module (HSM).

Ongoing Security Measures

To maintain the security level against new threats, authorized organizations perform network scans on the Cloud WAF network quarterly. In addition, very few individuals have authorization to access our system infrastructure.

Security Standards Compliance and Certifications

Radware’s Cloud Security services are certified and fully compliant with the strictest security standards, including the following standards specifically relating to the protection of private data in the cloud:

- ISO 27001:2013 (Information Security Management Systems)
- ISO 27032:2012 (Security Techniques -- Guidelines for Cybersecurity)
- ISO 27017:2015 (Information Security for Cloud Services)
- ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds)
- ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain)
- PCI-DSS v3.1 (Payment Card Industry Data Security Standard)
- US SSAE16 SOC-2 Type II
- US SSAE16 SOC-1Type II

Caching and Storing of Personally Identifiable Information (PII)

No copy of any customer data passing through Radware’s Cloud WAF and Cloud DDoS Protection Services is ever cached or stored, and no personally identifiable information (PII) of any kind, such as user names, addresses, credit cards, social security numbers, and so on, is ever cached or stored by Radware’s Cloud WAF and Cloud DDoS Protection Services.

The only information stored in the Radware Cloud Security portal database is the metadata of the traffic throughput statistics (that is, bits per second, packets per second, connections per second, and so on), and the security alerts and events of the underlying WAF and DDoS mitigation appliance (source and destination IP addresses of suspicions flows, detected attack vectors, actions taken, and so on). This information is stored in the database of Radware Cloud WAF portal to provide the customer with real-time visibility and for generating reports. This information is stored for a limited period of time (three months, by default), and is then permanently deleted from the Radware Cloud Security portal database.

There is no data in the Radware Cloud Security portal database that is personally identifiable information (PII) or that may be associated with a specific person, other than the credentials of the users of Radware Cloud Security portal, which are limited to username, password, and an email address to retrieve forgotten passwords.

North America
Radware Inc.
575 Corporate Drive
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: 972 3 766 8666