radware **DefensePipe** Data Sheet

Protect the Internet Pipe with Radware's Cloud Scrubbing Service

Radware's cloud scrubbing service - DefensePipe - protects against Internet pipe saturation caused by cyber attacks. It is activated only when the attack threatens to saturate the organization's Internet pipe. Based on the built-in synchronization between the data center, Radware's attack mitigation device and cloud scrubbing service, the in-the-cloud mitigation can start immediately.

Radware's attack mitigation is a hybrid solution integrating on-premise detection and mitigation with cloud-based volumetric attack scrubbing and 24x7 Emergency Response Team (ERT) support. It provides organizations the most integrated and comprehensive solution to fight today's cyber security threats.

> 15% of DDoS attacks handled by Radware's ERT saturated the Internet pipe.

Radware's solution helps organizations fight attacks on all fronts and achieve end-to-end protection with a single point of contact. This results in a shorter time to protect and a complete security solution from a single provider.

Solution Overview

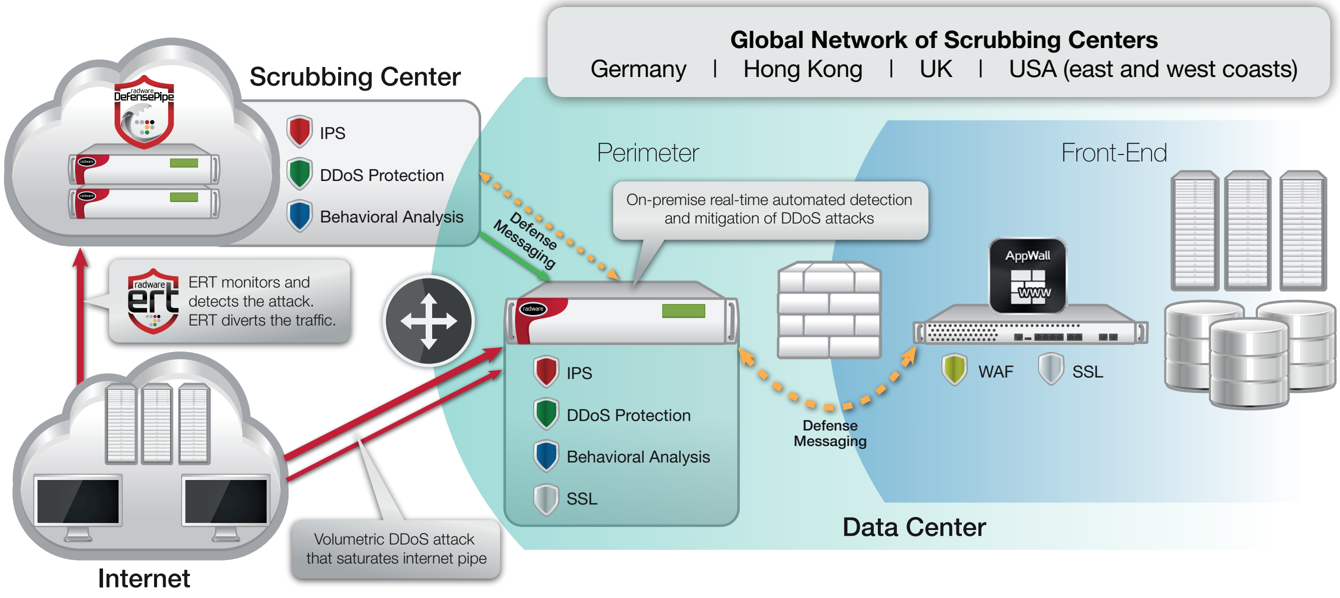
An on-premise attack mitigation system is the most effective approach to fight today's threats including application layer attacks, low & slow stealthy attacks, network layer attacks and SSL based attacks. However, once the attack turns into a volumetric flood attack that threatens to saturate the Internet pipe of the organization, the mitigation needs to move to the cloud. According to Radware's Emergency Response Team (ERT), only 15% of DDoS attacks were based on volumetric attacks that actually blocked the Internet pipe.

Radware's attack mitigation solution provides both on-premise attack mitigation and cloud-based protection, sharing essential information about threats and attacks over a defense messaging mechanism. During an attack that threatens to saturate the Internet pipe of the target organization, the on-premise attack mitigation device (DefensePro) alerts the cloud scrubbing service (DefensePipe) operations that the pipe is about to get saturated. The alert includes multiple characteristics of the attack that helps DefensePipe start the mitigation in the cloud faster and more accurately.

Once the mitigation is moved to the cloud, all traffic is diverted to the scrubbing center in the cloud, where it is cleaned before it is sent back to the organization.

Benefits

- Cloud based service that protects organizations against Internet pipe saturation
- Complements the on-premise DefensePro capabilities
- Activated only when attacks threaten to saturate the Internet pipe
- Multiple scrubbing centers in the cloud provide global coverage
- Single point of contact for emergency response
- Post attack and full report analysis

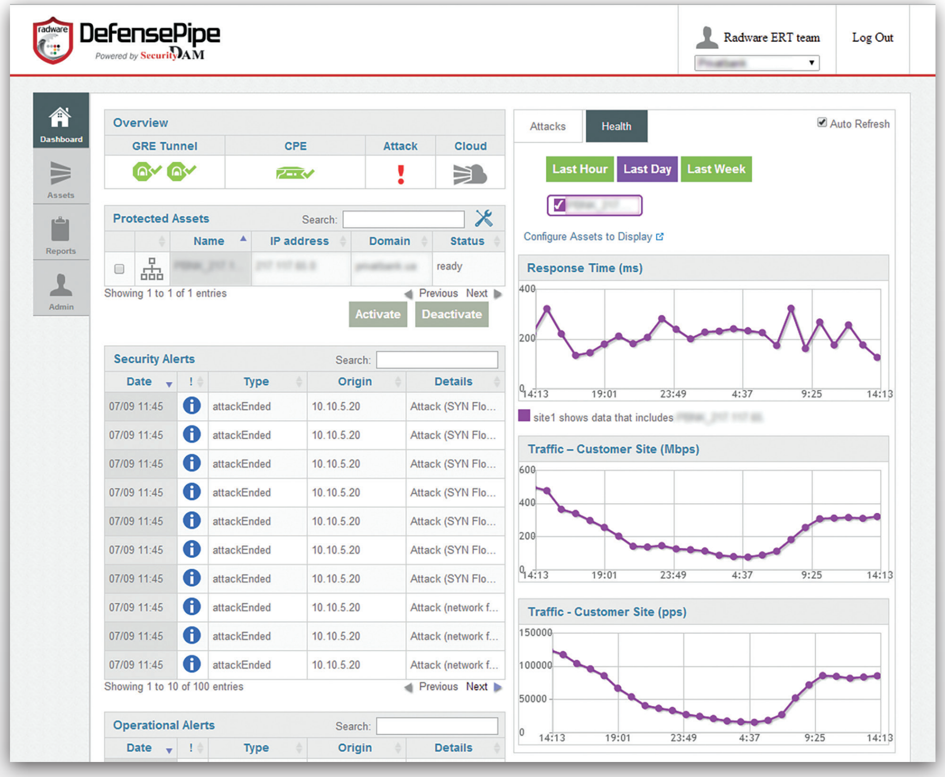

Global Network of Scrubbing Centers
Germany | Hong Kong | UK | USA (east and west coasts)
Scrubbing Center
radware DefensePipe
IPS
DDoS Protection
Behavioral Analysis
Defense Messaging
Perimeter
Front-End
On-premise real-time automated detection and mitigation of DDoS attacks
AppWall
WWW
radware ert
ERT monitors and detects the attack. ERT diverts the traffic.
IPS
DDoS Protection
Behavioral Analysis
SSL
WAF
SSL
Defense Messaging
Data Center
Volumetric DDoS attack that saturates internet pipe
Internet

Attack Mitigation Solution: Hybrid Network Defense

Attack Mitigation Online Customer Portal

Radware provides customers complete visibility in all DDoS protection layers with an intuitive web based control center that is comprised of:

- Real-time monitoring (traffic statistics, attack information, attack alerts)
- Management of cloud service and on-premises equipment monitoring
- Traffic diversion activation/deactivation
- Collection of attack data from on-premise and cloud equipment
- Real-time alerts and comprehensive reporting features



Overview

GRE Tunnel	CPE	Attack	Cloud
✓ ✓	✓	!	

Protected Assets Search:

		Name	IP address	Domain	Status
□		[redacted]	[redacted]	[redacted]	ready

Showing 1 to 1 of 1 entries

Security Alerts Search:

Date	!	Type	Origin	Details
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (SYN Flo...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (network f...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (network f...
07/09 11:45	i	attackEnded	10.10.5.20	Attack (network f...

Showing 1 to 10 of 100 entries

Operational Alerts Search:

Date	!	Type	Origin	Details

Attack Mitigation Service Portal Dashboard

Attack Mitigation Solution Benefits

- **Widest security coverage**: Radware attack mitigation solution offers a multi-vector attack detection and mitigation, handling attacks at the network layer, server based attacks, malware propagation and intrusion activities. With a unique patented mechanism, Radware's solution is capable of automatically creating a real-time signature of the attack, which can be used to mitigate the attack where it should be mitigated in the most effective way. This can occur either by the cloud scrubbing service or the on-premise attack mitigation device.
- **Minimal time to mitigate**: The always-on protection capability ensures that the organization is fully protected constantly, and time to mitigate is measured in seconds. In case of an attack that requires the traffic to be diverted to the cloud-scrubbing center, the protection continues with no destruction or gaps.

Radware's Emergency Response Team (ERT), who provide 24/7 security services for customers facing a denial-of-service (DoS) attack or malware outbreak, help fight the attack with the customers during the entire campaign both on-premise and in the cloud.

- **Single contact point**: Whether the attack needs to be mitigated on-premise or in the cloud, Radware's ERT fights the attack with the customer during the entire attack campaign. This means that customers do not need to work with multiple vendors or services during an attack and do not need to transfer responsibilities between vendors or to ensure that the vendors are synchronized.

- **Traffic is diverted only as a last resort**: Unlike cloud scrubbers and MSSPs that divert the entire customer's traffic to their scrubbing centers during an attack, Radware attack mitigation solution diverts the attack traffic only when the volumetric attack threatens to saturate the Internet pipe. In all other attack cases, the on-premise attack mitigation system mitigates the attack without the need to divert the traffic.

- **Integrated reporting system**: Provides information both from the on-premise mitigation and in the cloud mitigation. This enables the customer to perform more efficient forensics, better understand the threats it is facing and plan its mitigation strategy for future threats.

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.