Denial-of-Service (DoS)
Secured Virtual Tenant Networks (VTN)
Value-added DoS protection as a service for Software Defined Network (SDN)
– a solution paper by Radware & NEC Corporation of America – Whitepaper
Table of Contents

Abstract ..................................................................................................................................................... 3

Introducing NEC ProgrammableFlow Network ................................................................................................ 3

DDoS Threat is Growing and Evolving ........................................................................................................... 4

Introduction ......................................................................................................................................... 4

Attackers are getting sophisticated ........................................................................................................ 4

Overview of Radware DefensePro Attack Mitigation Solution .......................................................................... 5

Introduction ......................................................................................................................................... 5

DefensePro Protection Modules ............................................................................................................. 6

DoS Secured VTN – Joint NEC and Radware Solution .................................................................................... 6

Introduction ......................................................................................................................................... 6

Solution Architecture ............................................................................................................................ 6

Per Tenant Provisioning ........................................................................................................................ 8

How it works ........................................................................................................................................ 8

Per Tenant Monitoring and Reporting ..................................................................................................... 8

Conclusion: Fully-virtualized Per-tenant Anti-DoS Solution ......................................................................... 8

Summary: The Solution Advantages ............................................................................................................. 9

Appendix A: DefensePro Technology Overview .............................................................................................. 10

Adaptive Multi-Dimension Decision Engine ................................................................................................ 10

Cutting-edge Security Technologies ....................................................................................................... 10

Hardware Architecture Tailored for Attack Mitigation .............................................................................. 11
Abstract

Enterprise data center IT managers, as well as IT managers in service providers, are moving services into cloud models that rely on virtual data center technologies to significantly reduce their overall costs while improving their business agility. Software Defined Network (SDN) technology removes legacy networking technology limitations while contributing to network abstraction, cost reduction, business agility and dynamic policy management – aligned with server virtualization trends.

In an era where DDoS attacks have become a major threat to online businesses and data centers, Radware and NEC join forces to embed DDoS protection service into SDN technology. The joint solution delivers an innovative breed of DDoS attack protection solutions with the following benefits:

- Fully virtualized, per tenant Anti-DoS solution service
- State-of-the-art highly accurate attack detection and mitigation within seconds
- Provisioned as a virtual service per tenant network

This paper introduces NEC ProgrammableFlow Network logical abstraction plane Virtual Tenant Networks (VTN), the evolution of DDoS attacks and Radware DefensePro attack mitigation solution. It then introduces an innovative solution for DoS secured VTN service that is based on Radware’s DDoS detection and mitigation engines integrated into NEC’s ProgrammableFlow SDN OpenFlow solution. Following a solution description, this paper summarizes the key advantages of the solution.

Introducing NEC ProgrammableFlow Network

In a cloud environment, the network is a critical resource that connects various distributed and virtualized components- servers, storage elements, appliances and applications. For example, it is the network that allows aggregation of physical servers, efficient virtual machine migration, and remote connection to storage systems, effectively creating the perception of a large infrastructure resource pool. Furthermore, it is also the same network that enables delivery of cloud based applications to end users. Yet, while every component in a cloud is getting virtualized, the physical network connecting these components is not.

NEC’s ProgrammableFlow Network is a network virtualization solution where multiple interconnected switches can be virtualized into a large common network resource pool with unified and dynamic control on the switch forwarding behavior. The aggregated and virtualized resource pool acts like a big switch providing layer-2 to layer-4 functionalities. The ProgrammableFlow network solution follows some of the SDN paradigms: a) Decoupling the control plane from the data forwarding plane and b) Separation of the logical network plane design from the physical network plane operation.

The uniqueness of the ProgrammableFlow network design is in exposing a logical abstraction plane called the Virtual Tenant Network (VTN) framework, which enables deployment of a logical plane on top of any underlying physical network topology (see figure 1).

Figure 1: The ProgrammableFlow VTN framework allows multiple virtual networks to co-exist on top of one physical network.
Specifically, ProgrammableFlow VTN framework can automatically map a logical plane design into underlying physical network functionalities. These physical network functionalities are dynamically enabled by creating or modifying flow rules at individual switches leveraging the OpenFlow control protocol. The logical plane definition not only hides the complexity of the underlying physical network but also provides abstracted management of network resources, achieving significant reduction in time to reconfigure network services and minimizing network configuration errors.

**DDoS Threat is Growing and Evolving**

**Introduction**

Cyber-hacktivism has become so prevalent that every online business, financial service, government agency, or critical infrastructure is likely a target. Financially motivated attackers are still a threat; however, their activity is not on the news since just recently, they have received much less publicity.

Cyber attacks have become the weapon of choice for hacktivists seeking to leverage the impact of conflicts and social protests. Recent examples are the Anonymous group joining the Occupy Wall Street protesters to launch cyber attacks on major financial institutions in New York, attacking Sony®, and other companies affiliated with the copyright industry for revenge as part of Operation Mega-upload. In addition, the Nightmare group works with the hacker “0xOmar” to escalate their cyber war against Israel.

**Attackers are getting sophisticated**

An analysis of cyber attacks throughout 2011-2012 by Radware’s Emergency Response Team (ERT), notes that companies that relied only on a ‘one-size-fits-all’ in-the-cloud managed security, or on-premise security solutions alone, could not withstand the coordinated attack campaigns. The Radware ERT review of the attack traffic from multiple reported cases shows that:

- Attackers are deploying multi-vulnerability attack campaigns, targeting all layers of the victim’s IT infrastructure. This includes the network, servers, and application layers.

- Attackers who previously used distributed denial of service (DDoS) attack tools that focused on networks are now relying more on DDoS tools focusing on applications.

- Attackers are using “low & slow” attack techniques that misuse the application resource rather than resources in the network stacks.

- Attackers are using evasion techniques to avoid detection and mitigation including SSL based attacks, changing the page request in a HTTP page flood attacks and more
Overview of Radware DefensePro Attack Mitigation Solution

Introduction
Radware’s award-winning DefensePro® is a real-time network attack mitigation hardware-designed device that protects against all type of L3-L7 DoS & DDoS attacks including:

- **Network DDoS flood attacks** – Attackers flood the victim with a high volume of packets, consuming networking equipment resources or bandwidth resources. Examples are: SYN flood attacks (high packet-per-second attacks), large UDP packet floods (bandwidth attacks), ICMP floods, and more.

- **Application DDoS flood attacks (including encrypted SSL attacks)** – These attacks generate complete sessions and target the application resources. Examples are HTTP Get or Post flood attacks, or DNS flood attacks. The uses of encrypted SSL flood attacks aim to consume more CPU resources during the encryption and decryption of the content in order to amplify the resource overload effect.

- **Low & slow DoS attacks** – attacks that exploit application implementation weaknesses and design flaws. Examples are Slowloris, a tool that allows a single machine to take down another machine’s web server with minimal bandwidth, and Circle cache-control (Circle-CC), which floods a website by scanning the site across multiple pages systematically.
 DefensePro Protection Modules
DefensePro is comprised of several protection modules that are well optimized for DDoS attacks and multi-vulnerability attack campaigns:

- **DoS Protection** – Prevent all type of network DDoS attacks including UDP flood attacks, SYN flood attacks, TCP flood attacks, ICMP flood attacks, IGMP flood attacks, and Out-of-state flood attacks.

- **Network Behavioral Analysis (NBA)** – The network behavioral analysis module prevents application resource misuse and zero-minute malware spread. Users are protected against the following attacks: HTTP page flood attacks, DNS flood attacks, SIP flood attacks, brute force attacks, network and port scanning, as well as malware propagation.

- **Intrusion Prevention System (IPS)** – This module protects against application vulnerabilities and exploits as well as known DoS attack tools including low & slow DoS attack tools.

An overview of DefensePro detection and mitigation technologies including the real-time signature engine is available in appendix A.

DoS Secured VTN – Joint NEC and Radware Solution

**Introduction**
The DoS secured VTN is a fully virtualized network solution that enables the operator to assign a virtual DoS protection service per virtual tenant network. It relies on Anti-DoS application and shared DefensePro mitigation resource that are coupled with NEC ProgrammableFlow Controller and NEC ProgrammableFlow Switches respectively. The result is complete abstraction of the Anti-DoS resource provisioning and alignment with VTN network operations to provision, manage and monitor DoS protection as a tenant service within the VTN ecosystem.

**Solution Architecture**
NEC and Radware composed a native SDN solution based on both companies’ products to offer comprehensive and cost-effective protection against emerging DDoS attack campaigns in NEC ProgrammableFlow networks. The DoS Secured VTN solution includes the following functions that work toward protecting networks, servers and applications against all type of DoS attacks:
DoS Secured Virtual Tenant Networks (VTN) Whitepaper

- **Traffic baselines** – the essence of attack detection is to look for anomalous trends in traffic patterns when compared to normal patterns. The solution collects network traffic statistical information to create and store client, server and application behavioral baselines.

- **Attack detection** – an attack is detected by comparing real-time statistical information collected from tenant networks to the stored baselines, looking for anomalous traffic patterns. The solution needs to make a decision whether the anomaly is a flash of legitimate user traffic or an attack.

- **Traffic diversion and injection** – dynamically change the switching fabric so suspicious traffic is diverted to the DoS mitigation device for cleansing and then inject the clean traffic to its original destination.

- **Attack mitigation** – mitigating all types of DoS & DDoS attacks using a high performing attack mitigation device that deploys cutting edge security technologies.

- **Traffic Path Roll-over**: when the solution confirms that attack traffic is non-existent, it alerts the controller to divert the traffic back to its normal path.

Figure 7 provides the high level solution architecture illustrating the solution components and the interaction among the set of components.
The following Radware components are introduced into the NEC VTN framework to deliver DoS secured VTNs:

- **Anti-DoS application**: a software module that is responsible for the following roles:
  - Create traffic baselines
  - Attack detection using the fuzzy logic multi-dimension decision engine
  - Calling the ProgrammableFlow controller to perform: a) traffic diversion and injection; b) traffic path roll-over revert back to normal network forwarding

**Per Tenant Provisioning**
The network abstraction simplifies the service provisioning as it eliminates the need to physically configure switches and applications. To provision Anti-DoS service the admin is required to:

1. Assign a user or customer (represented by a VTN) to the Anti-DoS service.
2. Configure and select the protection policy the customer is associated with.
3. Define the protected application servers IP address ranges.
4. Define the protected network bandwidth.

**How it works**
1. The Anti-DoS application, in collaboration with the ProgrammableFlow controller, uses the OpenFlow protocol to monitor and collect packet level statistics from all switches in the OpenFlow Network. The monitoring is specific to a set of matching conditions to ensure the monitoring does not lead to unnecessary overhead.
2. The Anti-DoS Application uses the information to:
   a. Build the protected network traffic baselines.
   b. Compare real time network statistics with the stored baselines to determine abnormal traffic patterns.
   c. Upon anomaly detection determine if it is an attack or not.
3. Upon attack detection, the Anti-DoS Application calls the ProgrammableFlow controller to establish a traffic path that takes the suspected traffic through the DefensePro mitigation engine (path changed from [1] to [2] & [3]).
4. The DefensePro device starts immediately to clean the attack traffic using its multiple protection modules. The clean traffic only is forwarded to its destination.
5. Once the Anti-DoS Application determines the attack is over, it calls the ProgrammableFlow controller to revert the traffic path back to normal – no need to divert traffic through DefensePro anymore.

**Per Tenant Monitoring and Reporting**
Along with the provisioning of Anti-DoS service per tenant, the system sets automatically the security monitoring and reporting so each tenant gets a unified situational awareness solution for security and compliance. The user is provided with both real-time monitoring and historical reporting on policy violations, non-standard processes, rogue applications, potential financial fraud, identity theft and cyber-attacks.

**Conclusion: Fully-virtualized Per-tenant Anti-DoS Solution**
The DoS Secured VTN solution is a result of collaboration between two companies: NEC - delivering best of breed network virtualization and abstraction technologies; and Radware - delivering best of breed DoS & DDoS attack mitigation technologies.

NEC’s ProgrammableFlow Network provides VTNs – a network and abstraction solution that enables business agility by aligning virtual network infrastructure with the data center virtualization trends while reducing networking costs significantly.
The Anti-DoS service is a value-add service fully integrated into the ProgrammableFlow architecture. It is represented as a logical entity that is assigned per tenant network to the protected application servers. Once the Anti-DoS application detects abnormal activity as an attack, it uses the ProgrammableFlow controller to divert the suspicious traffic to the DefensePro attack mitigation device to remove the attack traffic.

The joint solution allows taking advantage of NEC’s VTN configuration and visualization approach. The network manager can provision any VTN with a DoS protection service to select all or parts of the VTN’s network objects.

**Summary: The Solution Advantages**
The Radware-NEC joint solution is the 1st to market switch fabric infrastructure that includes an integrated DDoS protection solution. It allows the fabric itself to be secured and provision the DoS Protection service per network tenant.

The solution provides the following unique advantages:

**Best DDoS protection solution** – Radware’s unique and field-proven DDoS protection technology together with NEC’s rich experience in the server and networking markets, and its innovative first to market commercial OpenFlow products, provides an advantage for any datacenter and/or clouds managed security providers that consider transition to SDN frameworks.

**Shortest time to protect** – By having almost near real-time packet statistics and dynamic traffic control, the solution achieves fast reaction to imminent attack traffic within seconds.

**High Availability** – The DoS mitigation engine (DefensePro appliances) can be located in different network redundant locations in order to provide a fully redundant architecture that works in conjunction with the NEC VTNs. If one of the DefensePro appliances fails, the system detects and automatically assigns another appliance to perform the mitigation actions when needed through seamless flow redirect actions. The same process can be done in order to increase the capacity of the mitigation engines, i.e., redirect the suspicious traffic through more than one DefensePro appliance per defined SLA.

**Scale with Traffic** – Any service inserted into the network has to ensure that it can scale with ever increasing traffic volume. Diverting the suspicious traffic only to the DefensePro allows assigning multiple VTNs to the Anti-DoS service with the need to increase DefensePro capacity proportional to the aggregated traffic bandwidth of the assigned VTNs.

**Dynamic Service Provisioning** – The DDoS attack mitigation service can be dynamically provisioned per VTN enabling operators to apply it as an on-demand service for their commercial offering. The provisioning does not require any manual configuration process and benefits from reduced complexity thanks to the abstraction of the network operations.

**Simplified Network Control** – There are no complex requirements or additional overheads for route controls as found in other Netflow based and tunneling mechanisms. A fully Anti-DoS application integrated with the ProgrammableFlow Controller ensures a highly and efficiently coordinated network aware solution.

**Highly reduced costs** – the DefensePro attack mitigation device is a shared resource that is virtualized per tenant and used only when under attack. This means tremendous CapEx and OpEx savings when compared to standard inline or out-of-path DDoS mitigation solutions.
Appendix A: DefensePro Technology Overview

Adaptive Multi-Dimension Decision Engine

The main challenge in mitigating DoS and DDoS attacks is to detect traffic anomalies and filter out only the attack traffic while maintaining the uninterrupted flow of legitimate traffic. Filtering out malicious traffic must be performed with caution, particularly since false positives may occur which could block real user traffic.

Radware’s Fuzzy Logic algorithm overcomes traffic analysis difficulties that Internet communications usually present. The Fuzzy Logic module includes adaptive capabilities and the sensitivity of the module is being continuously tuned to match the characteristics of the protected networks.

Typically, the Fuzzy Logic decision engine uses two categories of traffic behavioral parameters to generate a degree of attack:

- **Rate-based** behavioral parameters such as packet rate, Mbps, connection rate, application request rate, application response rate, etc.

- **Rate-invariant** behavioral parameters such as protocol breakdown, TCP flag distributions, application request/response ratio, connections distribution, URL hits probability functions and more.

The Fuzzy Logic decision surface (illustrated in the Figure 5) shows a correlation between both rate-based and rate-invariant behavioral parameters, before generating a degree of attack.

Cutting-edge Security Technologies

Radware DefensePro uses multiple technologies to provide complete attack protection against all types of DoS & DDoS attack campaigns:

- The **DoS Protection module** is based on several technologies: signature detection, behavioral based real-time signatures, and a SYN cookies mechanism that challenge new connections prior to establishing a new session with the servers.
The **Network Behavioral Analysis (NBA) module** employs patented behavioral-based real time signature technology. As shown in figure 6, it creates baselines of normal network, application, and user behavior. When an anomalous behavior is detected as an attack, the NBA module creates a real-time signature that uses the attack characteristics and starts blocking the attack immediately.

The **Intrusion Prevention System (IPS) module** is based on stateful static signature detection technology with periodic signature updates, and emergency updates in cases of newly discovered high risk attacks.

**Hardware Architecture Tailored for Attack Mitigation**

The main advantage of DefensePro’s hardware architecture rests in its ability to completely separate the mitigation tasks, each one in a different dedicated hardware component, thus preventing internal resource cannibalization that typifies other attack mitigation products.

Repelling the multi-million PPS L2-L4 DDoS attack is done solely by the DME (DoS Mitigation Engine) hardware component, while attacks that need to be mitigated through DPI (Deep Packet Inspection) utilize the L7 RegEx acceleration ASIC. At the same time, legitimate traffic that should continue to be processed by the stateful analysis modules and feed the statistical analysis modules in the system is being processed by the multi-purpose (multi-cores) CPU’s.

This hardware architecture provides higher and more predictable performance figures than other attack mitigation systems.

© 2012 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.