



Intelligent Application Switching Solutions

# Security Activation



# Radware security solutions safeguard your business by providing Gigabit speed intrusion prevention and Denial of Service protection while guaranteeing that all your security tools are activated and fully protecting mission critical data and resources.

## Why Radware is Needed for Security

Enterprises depend on point security tools including firewalls, VPNs, Intrusion Detection Systems, anti-virus and application security for protection against attacks and malicious activity.

Each security tool however introduces single points of failure, performance degradations and overloads that undermine your site wide defense and cause security breaches.

Without eliminating downtime, resolving combined security application vulnerabilities and addressing poor security performance, it is impossible to safeguard your enterprise.

Radware is the only solution capable of ensuring the availability and high performance of combined security tools, for optimized and complete operation of any defense architecture.

Eliminating security failures from enterprise networks, Radware delivers continuous, fault tolerant, scalable defense while providing complete application security.

## How Does Radware Security Work?

### 1. Highest Performing Defense

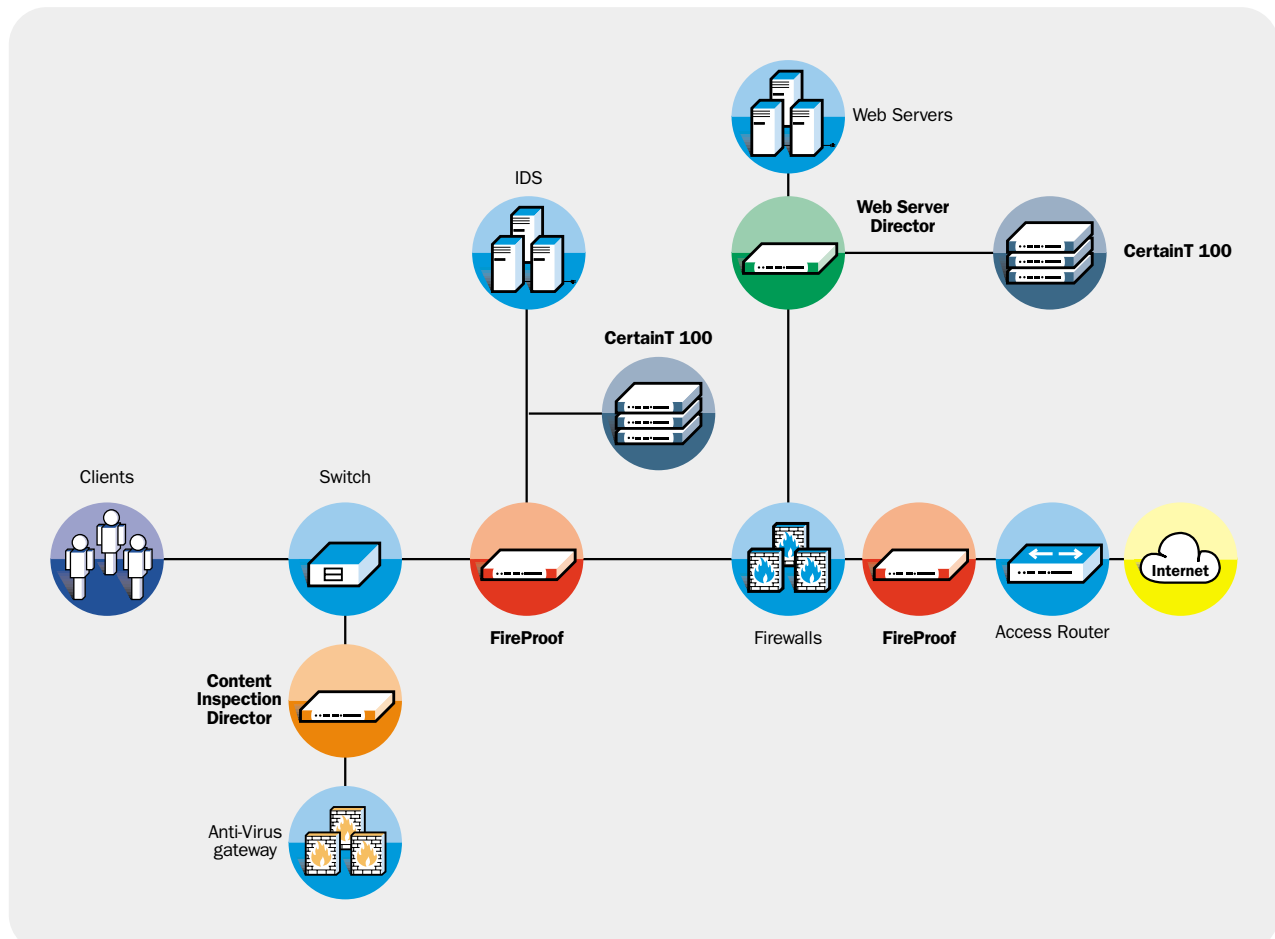
Radware security switching architecture delivers security at Gigabit speeds for high performing firewalls, intrusion prevention devices, anti-virus gateways and SSL transaction processing, eliminating the performance-security tradeoff.

### 2. Real-Time Application Level Security

Application security provides intrusion prevention, continuously identifying and blocking suspicious traffic at Gigabit speeds, to safeguard core enterprise applications from Nimda, Code Red, and over 1000 attack signatures.

### 3. Denial of Service (DoS) Protection

DoS Shield detects and mitigates Denial of Service attacks at Gigabit speed for the continuous protection of all network operations and resources in high throughput environments.



#### 4. Fault Tolerant Security Across Combined Security Services

Advanced health monitoring and traffic redirection guarantee full availability and the best performance of all combined security tools:

**FireProof** ensures the non-stop operation of firewalls, VPNs, Intrusion Detection Systems to safeguard your network and applications.

**Content Inspection Director** delivers continuous and streamlined anti-virus and content filtering for full content security.

#### 5. Cost Effective Security Operation and Scaling

Load balancing dynamically distributes traffic loads across security tools, maximizing utilization of existing infrastructure for immediate ROI, while enabling effective security scaling across enterprise networks:

**FireProof** extends high performance and service scaling of firewalls and Virtual Private Networks. Aggregating IDS services across network segments, FireProof reduces sensor deployment requirements, for cost effective IDS deployment and operation.

**Content Inspection Director** pre-screens all content, directing only relevant traffic to anti-virus services, while bypassing all other traffic to optimize, accelerate and scale content security.

**CertainT 100** offloads Secure Socket transaction processing to an ASIC based hardware accelerator, while compressing content and reverse caching it to free expensive server CPU cycles for immediate ROI and unlimited SSL transaction scaling.

#### 6. End-to-End Security Visibility

Configware Insite provides site wide management and full visibility of all combined enterprise security operations, for real-time and historical views of defense performance by application, traffic type, source, destination and other parameters.

### How Do Radware Security Solutions Pay for Themselves?

Radware's security solutions provide rapid return on investment (ROI) based on reduced security operating costs and security deployment and scaling savings:

#### Security Operation Failure:

Radware eliminates debilitating and costly effects of defense service downtime and failed application protection across networks:

Avg. annual cost of 1 Hr network service downtime:  
\$892,640

*(Source: Network Computing, April 2002)*

Avg. annual cost of malicious activity and attacks:  
\$283,000

*(Source "2002 CSI/FBI Computer Crime and Security Survey" 2002)*

Avg. total annual cost of Security Operation Failure:  
\$1,175,000

Avg. capital expense of Radware end-to-end security:  
\$100,000

Avg. annual Opex security savings with Radware:  
\$1,075,000

#### ROI after 31 days of operation

#### Security Service Scaling

By optimizing security service operations and attaining high utilization Radware cuts the cost of scaling security services across the enterprise:

Avg. cost reduction for IDS sensors deployment and scaling: 75%

*(Cross segment traffic aggregation reduces sensor deployment requirements)*

Avg. cost reduction for anti-virus server deployment and filtering services: 40%

*(Content bypassing, decreases loads on AV servers, enabling larger volume handling)*

Avg. cost reduction for SSL transaction processing: 80%

*(Offloading of server CPU; transaction rate acceleration and content compression scale SSL operations)*

Radware's security solutions enable the full protection and enforcement of defense strategies across key businesses and industry networks, including finance, retail and e-commerce, healthcare, government, media, education, transportation, services and others.



**FireProof**  
Defense, Non-Stop



**Content Inspection Director**  
Complete Content Security



**CertainT 100**  
SSL Transaction Acceleration

**Gigabit Speed Security Switching** – Eliminating the performance-security tradeoff

**Fault Tolerant Access Control** – Full availability of firewalls for non-stop, high performing and scalable access control

**Maximum Performance VPN** – Virtual Private Network service acceleration, for fast and cost effective secure enterprise communications

**High Speed Intrusion Detection** – High availability, load balancing and traffic aggregation across network segments for fault tolerant, high performance and cost effective IDS

**Gigabit Speed Intrusion Prevention** – Intrusion detection and instant blocking of Buffer Overflows, Trojans, Nimda, Code Red, Goner and over 1000 attack signatures automatically protect your enterprise from hacking attacks and security violations

**Real-time Denial of Service Protection** – Detection and blocking of DoS attacks at Gigabit speeds, for continuous protection of all network operations and resources

**Guaranteed Security Service Levels** – Complete control over bandwidth allocation and traffic prioritization, guaranteeing security performance levels by applications and users

**Security Service Scaling** – Site wide optimization of defense resources through load balancing, enabling cost effective utilization and economical security service growth

**Maximum Performance Anti-Virus and URL Filtering** – Gigabit speed content filtering for high throughput and maximum performance content security

**High Availability Content Inspection** – Full availability of anti-virus gateways for fault tolerant anti-virus scanning and continuous blocking of malicious content

**Anti-Virus Service Scaling** – Unlimited growth in scanning traffic volume capacities through full load balancing for high performance anti-virus services and economical service scaling

**Content Pre-Screening** – Traffic bypassing and direction of relevant traffic only to anti-virus services for a 500% performance improvement per content scanning gateway

**Combined Anti-Virus Service Support** – Transparent deployment and operation of best of breed content filtering for complete vendor freedom, applying multiple tools for enhanced security and fully customizable anti-virus services, with no integration overhead

**Comprehensive Filtering Flow Management** – Complete traffic classification by volume, users and content, for flexible and granular control over scanning operations, service prioritization and performance

**Guaranteed Content Delivery Service Levels** – Complete control over anti-virus service bandwidth allocation and traffic prioritization, guaranteeing filtering performance levels by content and users

**Gigabit Speed Intrusion Prevention and DoS Protection** – Real-time protection of anti-virus gateways against debilitating Denial of Service attacks, Buffer Overflows, Trojans, Nimda, Code Red, Goner and over 1000 attack signatures

**SSL Transaction Processing Offloading** – Offloading of Secure Socket transaction processing and certificate management to an ASIC based hardware accelerator frees expensive CPU cycles translating into immediate ROI

**High-Performance SSL** – Encryption/decryption of SSL traffic at Gigabit speeds for maximum performance and high throughput SSL transaction processing

**SSL Service Fail-Over (with WSD)** – SSL Service fail-over ensures continuous SSL service availability and secure transaction completion

**Secure Processing Scalability** – Seamless service volume growth up to 20,000 SSL transactions per second in CertainT 100 clusters, delivers unlimited scalability for SSL transactions

**Content Acceleration** – HTTP compression and reverse caching reducing bandwidth requirements and accelerating response time to end users by more than 500%

Copyright Radware Ltd. 2002.

All Rights Reserved. The copyright and all intellectual property rights in this article belong to Radware Ltd. It is strictly forbidden to copy, multiply, reproduce or otherwise use this article or any part thereof in any way shape of form without the prior written consent of Radware Ltd.

