

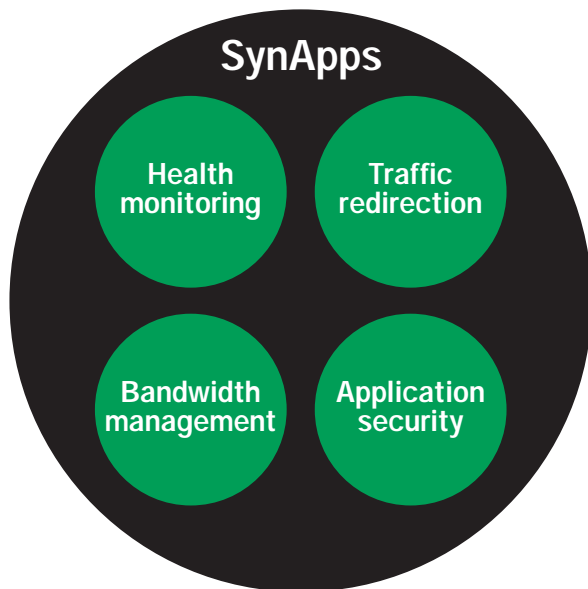


radware

SynApps Architecture

Next Generation Traffic Management

SynApps Architecture™ redefines the role of Intelligent Traffic Management (ITM) by providing optimal, personalized, continuous and secure service that eliminates network uncertainty. Radware's SynApps Architecture is the only solution that combines application health monitoring, traffic redirection, bandwidth management, and application security in a powerful, ASIC-based switch platform. Combined, these four elements optimize the user experience from click to content by managing traffic according to application needs. Let Radware help you and your customers get certain.



Health Monitoring

Ensuring end to end availability of network services is a complex task. If a failure occurs at any point on the path, from the user to the content provider, the end user will not receive the needed content. That is why Radware checks multiple, user definable points within the application to ensure that the entire logical path is operational. SynApps health monitoring software continuously checks the health of critical network resources such as servers, firewalls, cache servers and routers. Monitoring methods vary from the physical testing of servers to dynamic content verification. If a problem is detected, SynApps directs traffic to an alternate resource and sends a notification of resource failure to the network administrator.

— IP Based Monitoring

SynApps health monitoring includes IP, TCP and UDP application checks. In addition, server agent MIB variables can be monitored to reflect server health. All parameters are user defined and can be adjusted on the fly, in real time. These tools enable the complete customization of network health monitoring. IP based monitoring allows for the detection of physical failures, OS failures and UDP application failures, such as directory services (LDAP).

— Web Health Monitoring

SynApps includes application health monitoring through web page verification. This mechanism monitors the HTTP codes returned from the server to ensure that the web application is functioning correctly. Web health monitoring detects if a web server is unavailable, is not serving pages, or a given URL is not found.

— Content Health Monitoring

Content health monitoring is accomplished by checking for the presence or absence of user defined strings within the returned text. This is useful in dynamic environments where HTML content is pulled from a database that sits logically behind application servers. A positive user experience is guaranteed by verifying the content within the return string. If invalid content is detected the entire application path is disabled, and the user is redirected to a valid data source.

— Transaction Based Health Monitoring

Transaction based health monitoring ensures that users can perform a transaction as expected. As a result, all the resources required to complete the transaction are monitored and checked to ensure that they are healthy. SynApps monitors all the various networking and server resources, such as routers, firewalls, web servers, application servers and databases, which complete the transaction path. Whenever a failure is detected in one of these resources, SynApps automatically and transparently directs the traffic to a healthy path, thereby providing the user with guaranteed service.

Traffic Redirection

Traffic on the Internet and within organizations is not consistent. In a functioning system of networks there are inevitably peak loads. Yet when providing a service and creating e-relationships with end users, companies need to be sure that a fast, solid and continuous level of service can be maintained. The SynApps traffic redirection component ensures exactly that. Traffic is always sent to the most available and optimal resource for serving the particular user, whether the resource is a server, data center, firewall or router. SynApps' Application Switch provides a robust, fast and flexible traffic management solution for users' networks and is designed to integrate seamlessly into existing networks.

— Layer 4 Switching

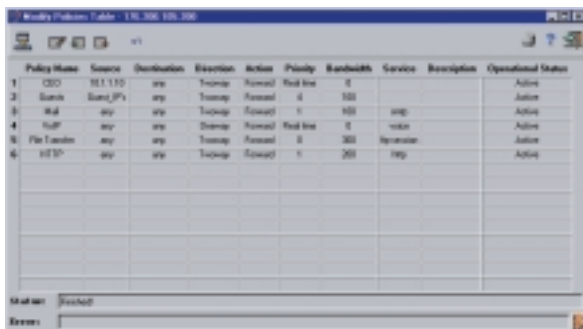
This super set of layer 4 level of traffic redirection is comprised of decisions made based on virtual IP addresses and on port numbers. These two techniques ensure persistence in cases where users need to be continuously serviced by the same server, or group of servers, based on IP or port information. SynApps combines specific support for various protocols and applications such as streaming, passive FTP, HTTP, e-mail, DNS, VoIP, Telnet, Rshell, TFTP and more.

— Web Switching Capabilities

Traffic redirection decisions can be made based on the URL and the HTTP GET request. This provides opportunities for more refined redirection to the optimal resources. SynApps can direct traffic according to URL addresses, and more specifically, based on field information in the URL itself. Traffic is directed to a particular group of servers, providing efficient service and optimizing server resources.

— Content Switching Capabilities

Traffic redirection decisions can be made based on session content. This enables the allocation of different server resources for different types of data. For example, requests for GIF and JPEG files may be directed to one group of servers while CGI scripts are redirected to another. The SynApps traffic redirection module is content aware and can make redirection decisions based upon file type, cookie, SSL ID and content, ensuring the successful completion of any e-business transaction. Some e-applications require persistence to ensure transaction success. Persistence is defined as maintaining user association with a logical server for the duration of the transaction. SynApps architecture fully supports session persistence.



Policy Name	Source	Destination	Evention	Action	Priority	Bandwidth	Service	Description	Operational Status
1. QOS	10.1.1.1/24	any	Transmit	Forward	1	100			Active
2. Bandw	Bandwidth	any	Transmit	Forward	4	100			Active
3. Mail	any	any	Transmit	Forward	1	100	any		Active
4. VoIP	any	any	Transmit	Forward	1	100	VoIP		Active
5. File Transfer	any	any	Transmit	Forward	2	300	Non-voice		Active
6. HTTP	any	any	Transmit	Forward	1	200	any		Active

Bandwidth Policies Table

Bandwidth Management

The ability to differentiate levels of service and to control an organization's bandwidth usage is key to providing consistent, high quality service. SynApps bandwidth management allows companies to define and enforce their own bandwidth management policies based on any combination of users, servers, applications and content. For example, SynApps enables a company to guarantee that critical business traffic, such as ERP traffic or e-commerce transactions, receive higher priority than do non-critical traffic, while guaranteeing a specific amount of bandwidth to VoIP traffic. It also enables the definition of different service levels and provision of content to different types of customers, such as platinum, gold and silver level customers. This assures that each class of user or application gets the best level of service according to company policy.

— Robust Classification Engine

Traffic can be classified according to any combination of source and destination IP addresses and groups of addresses, application port, content/URL, and/or cookies. This enables the differentiation of traffic types according to any of the above parameters, and enables the definition of appropriate traffic class management.

— Allocate and Prioritize Traffic

Traffic can be prioritized based on each traffic classification. There are 8 priority levels in addition to a real time, top priority level for real time applications such as VoIP or streaming. Each class can be assigned a static bandwidth level or can be assigned a limited bandwidth range. A combination of prioritization and bandwidth limitation can be assigned to each traffic class, which ensures the most accurate implementation of traffic policies.

— Bandwidth Policy Enforcement

SynApps ensures that each class receives the appropriate level of service according to a defined policy that is implemented based on three algorithms. SynApps provides two scheduling mechanisms that control packet forwarding: Class Based Queuing (CBQ) and Weighted Round Robin (WRR). WRR provides the greatest flexibility, and is used to configure policies that provide simple packet prioritization. CBQ is used to configure policies that provide limited bandwidth ranges. It also includes a mechanism that ensures that there is no starvation of any class by borrowing bandwidth between classes so low priority traffic doesn't wait endlessly. In addition to WRR and CBQ, SynApps includes Random Early Detection (RED) which prevents queue overflow, a common occurrence when there is more traffic than bandwidth. RED automatically detects trends toward queue overflow and drops TCP packets according to their priority. This ensures high performance and service levels for high priority traffic, regardless of the over subscription of bandwidth.

Application Security

Application security provides a line of defense for critical network resources that complements and expands those typically deployed in network designs. SynApps automatically detects and protects networks and applications from more than 450 known attack signatures such as Denial of Service attacks (DOS), Distributed Denial of Service attacks (DDOS), Buffer Over Flow (BOF), exploits and vulnerabilities, mis-configuration, default installation, back door/Trojans and port scanning.

The Application Security module monitors both network and application traffic in order to detect and prevent attacks in real time by terminating the suspicious sessions as they enter the network.

Again, the application security module is not intended to replace existing network security devices; rather it provides additional, focused security. Just as valuables in private homes are commonly protected by a series of security devices, so should network resources. In your network, firewalls are used to prevent break-in attempts. Analogously, houses are equipped with locked doors and alarm systems. However, in your home the real valuables are kept in a safe, and the thief who successfully enters your home must break into this as well. SynApps architecture is analogous to the combination of the safe. It is an additional, focused layer of protection that sits directly in front of your critical assets, such as your servers and firewalls, adding an additional level of focused security for your critical resources. With a firewall the thief may get into your house, but with SynApps your valuable assets remain protected in the safe.

— Anti-Scanning Capabilities

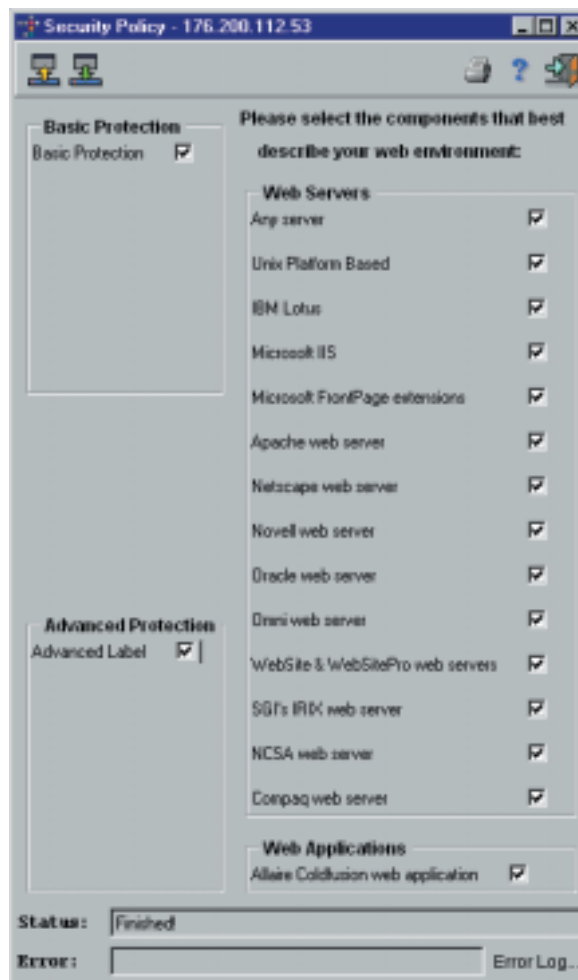
SynApps can detect and prevent network based scanning such as stealth and connect scanning, as well as web based application scanning. TCP connect, TCP SYN and TCP FIN scanning methods are detected in real time and prevented.

— Bi-directional Inspection

Application security monitors all traffic, both inbound to the network and outbound from it, in search of attack signatures. This allows you to deploy security policies on traffic direction and specifically helps prevent new exploits that may enter on the way in, but are detected and prevented on the way out. This capability can also assist in preventing threats from inside the network.

— Flexible Topology and High Performance

Built into Radware's multi-layered switching architecture, the SynApps application security module is an extremely high performance application. As an integrated module in the switching architecture, application security can protect multiple network segments without requiring the installation of a separate unit for each segment. It is extremely flexible and transparent, does not require network or server agents, and runs independently of server hardware and operating systems. All of these capabilities make the Application Security a truly unique and valuable addition to your network security scheme.



Security Policy Screen

Copyright Radware Ltd. 2000.

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.

Radware Inc.

575 Corporate Drive, Lobby 2
Mahwah, NJ 07430
Tel: +1-201-512-9771
Fax: +1-201-512-9774
U.S. Toll Free: 1-888-234-5763
email: info@radware.com

Radware Ltd.

22 Raoul Wallenberg Street
Tel Aviv 69710, Israel
Tel: +972-3-766 8666
Fax: +972-3-766 8655
email: info@radware.co.il



radware get certain