



Check Point IP Appliance Advantages

Contents

What is IP Appliance?	3
IP Appliance Software Features and Advantages	3
Security-hardened platform	3
Routing Implementations	4
Support for Flash-based systems.....	4
High Availability	4
Image and Package Management	5
Quality of Service	7
Software Acceleration using SecureXL	7
Firewall/VPN Hardware Acceleration	7
Management Interfaces	7
Monitoring Enhancements.....	8
Multi-processor Support	10
Conclusion	10

What is IP Appliance Software?

IP Appliances come with software that supports key network needs, such as dynamic and multicast routing, IPv6 routing, VLANs and Link Aggregation, making integration into complex networks transparent. IP Appliances also support key capabilities that include:

- Flash-based storage support
- High availability features including VRRPv2 and VRRP Monitored Circuits, and IP clustering
- Image and software package management
- Quality of Service (QoS)
- Software acceleration using SecureXL
- Firewall/VPN hardware acceleration
- Management interfaces including Voyager Web GUI, OS command-line interface (CLI), SNMP MIBs (both standard and enterprise (proprietary))
- Monitoring enhancements
- Multi-processor support

Check Point VPN-1 package is preinstalled on the IP Appliance with features, such as software and hardware acceleration, dynamic and multicast routing, and high availability.

IP Appliance Software Features and Advantages

Security-hardened OS

IP Appliances are scalable, robust and secure. They are optimized for route processing and packet forwarding. The platform started with no binaries and libraries and then added different elements to provide a compact and secure system. 'inetd.conf' routing infrastructure starts empty, and services must be added through the web interface, or command line interface (CLI). For security, the IP Appliances do not support these services or utilities:

- Sendmail; only send-only mail system that does not accept connections on port 25.
- Known insecure utilities such as rsh, rlogin, rexec
- Remote user information daemons and services such as finger, who and talk
- Exportable file systems such as NFS
- Development environment so intruders cannot build binaries
- BIND (DNS) server or dependence on external DNS service for anything
- News server, printing server, NIS, POP, IMAP or X Window system
- Extraneous CGI programs on the system

IP Appliances offer the ability to configure role-based access for element administration. The web interface or CLI are used by administrators to define roles and assignments for different users. IP Appliances provide additional logging facilities such as audit log trail and syslog messages. IP Appliances log under syslog the following messages:

- Voyager, shell, CLI, console and modem logins and logouts
- Every maintenance operation (upgrade, reboot, backup, etc.)
- Every change to any configuration data
- Interface up and down transitions
- VRRP and IP clustering transitions
- SNMP traps
- File system mounts and unmounts

Routing Implementations

IP Appliances support the following routing options:

- Static routes
- OSPF
- RIPv1/v2
- IGRP
- IGMP (multicast)
- DVMRP (multicast)
- VRRP (for high availability)
- PIM-DM
- PIM-SM
- IGRP (optional)
- BGP4 (optional)

Support for these routing protocols provides customers with the ease and flexibility of integrating IP Appliances into their existing network. IP Appliances also support 802.1Q VLAN tagging. VLAN routing capability provides scalability, security and traffic flow management, and flexibility for network reconfiguration through software instead of physically relocating devices.

Support for Flash-based systems

In addition to disk-based Appliances, IP Appliances come in flash-based version as well. Flash-based Appliances have internal compact flash instead of hard disk drive. As reading from the flash is faster and is less prone to corruption, flash-based systems are more robust. All the installed software and packages are stored in the internal compact flash; this improves the mechanical reliability of the system and avoids failures associated with disk drives.

High Availability

IP Appliances provide a range of high availability technologies, from Virtual Router Redundancy Protocol (VRRP) monitored circuits through the patented high-performance IP Clustering technology that ensure critical services remain live under the most demanding conditions.

VRRP monitored circuit eliminates potential asymmetric routing condition by monitoring multiple interfaces and forcing a complete failover when an interface fails or becomes unreachable. Consequently, all network traffic from both the external network as well as the internal network will traverse to the backup firewall. VRRP monitored circuit does not require using additional dynamic routing protocols such as OSPF to forward traffic in a failover event.

IP clustering technology allows up to four devices to act as a single network entity, sharing internal and external IP addresses. IP packet processing is distributed among all cluster member gateways to achieve equal processing loads. In some cases, IP clustering option improves throughput performance when a stand alone appliance's CPU load is high.

IP Appliances also support External Load Balancers. Customers can choose to use VRRP, IP clustering, or External Load Balancers for their high availability requirements. This flexibility allows accommodating changes as the network environment changes over time.

The table below serves as a guideline for choosing the appropriate high availability solution to meet the needs of the customer.

	HA Mode	Firewall Sync & Failover Time	Recommended Number of Appliances	Redundancy	Performance Scalability
VRRP	Active-Passive or Active-Active	Yes < 1 Second	2	Complete	Some
IP Clustering	Active-Passive or Active-Active	Yes Sub-Second	2 or more; 3 for Good Scalability	Complete	Good
ELB (External Load Balancers)	Active-Active	Yes Sub-Second	2 or more; 4 to 5 for Excellent Scalability	Depends on the ELB	Excellent

Image and Package Management

Check Point provides security application packages and operating system separately, which allows the flexibility of storing more than one version of the installed packages or operating system images at the same time. As the operating system starts up, the selected operating system is identified through a symbolic link. An upgrade of the operating system and/or a security application happens in minutes and only requires a reboot to activate the new software. This also provides total upgrade/fallback, backup/restore or complete new installation within minutes.

IP Appliances provide a mechanism (configuration migration) to migrate the configuration from one IP Appliance to another. When deploying a new IP security Appliance and replacing an old one, the existing configuration does not necessarily map directly to the new appliance.

The following areas may not map:

- On the new Appliance, the interface-naming convention might be different
- The newer Appliance might be flash-based while the old one was disk-based (or vice-versa)
- The new Appliance might not support some deprecated features, network cards, etc.

The configuration migration mechanism addresses the above issues. Instead of re-configuring the new Appliance from scratch, the customer can use the configuration migration wizard through the web user interface for the configuration migration process.

Below are the screenshots of configuration migration wizard.

Map Non-LRG and Non-LAG Interfaces

Interface on Source Platform	Attributes on Source Platform	Interface on Target Platform
eth-s1p2		Choose one
eth-s1p3		Choose one
eth-s2p1	eth-s2p1c0: 10.16.0.2 OSPF VRRP SNMP	Choose one
eth-s2p2		Choose one
eth-s2p3		Choose one
eth-s2p4		Choose one
eth-s4p1	eth-s4p1c0: 10.100.105.2 SNMP speed: 100M	Choose one
eth-s4p2		Choose one
eth-s4p3	eth-s4p3c0: 10.100.101.2 eth-s4p3c1: 10.100.102.2 eth-s4p3c2: 10.100.103.2 eth-s4p3c3: 10.100.104.2 SNMP speed: 100M	Choose one
eth-s4p4	eth-s4p4c0: 10.100.106.2 SNMP speed: 100M	Choose one
eth-s4p5		Choose one
eth-s4p6		Choose one
eth-s4p7		Choose one
eth-s4p8		Choose one

Capabilities of Interfaces on Target Platform

Interface	Capabilities
eth-s1/s1p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s1/s1p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s1/s2p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s1/s2p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s1p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s1p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s2p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s2p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s3p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s3p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p3	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p4	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec

Quality of Service

With the DiffServ implementation in IP Appliances, customers can configure their systems to classify, shape, and prioritize packet streams in conformance with RFCs 2597 and 2598 of the IETF DiffServ Working Group. The native DiffServ QoS is supported with SecureXL acceleration. In earlier versions, when SecureXL is enabled, the traffic bypasses the QoS layer completely. The integration of QoS with SecureXL allows packets to go through the QoS layer for any packet treatment (mark, shape, prioritize) before handing them over to SecureXL for fast forwarding.

Software Acceleration using SecureXL

IP Appliances communicate with VPN-1 Power through the SecureXL API for software acceleration. The API supports the exchange of information between security applications and operating system related to packets and packet streams. This enables operating system to take over the validation of subsequent traffic after the initial validation is done by the security application like VPN-1. IP Appliance either performs this validation natively at the hardware interrupt level on x86 hardware or supervises the execution of further optimized code in attached Accelerated Data Path Service Modules. Both of these approaches involve substantially less computing overhead.

Firewall/VPN Hardware Acceleration

IP Appliance's Accelerated Data Path (ADP) is a key technology that keeps customer's interest in Check Point when it comes to security and high performance networks. ADP technology relies on the network processing module, operating system specific to that module, and SecureXL to achieve throughput and connection rate acceleration. The main function of ADP service module is to forward all packet sizes at the highest possible rate.

IP Appliances also supports VPN accelerator cards to accelerate both site-to-site VPN and client VPN traffic, when the encryption algorithm supported on the hardware accelerator card is used. IP Appliances provide embedded drivers for all the supported VPN accelerator cards:

**NOTE: Both the ADP service module and the VPN accelerator card need to have SecureXL enabled in order to function properly.*

Management Interfaces

IP Appliances web user interface is easy-to-use and provides an extensive depth of configuration and flexibility to facilitate deployment in the most complex networking environments.

Customers can take full advantage of IP Appliances command line interface to provide cost-effective deployment management and maintenance, and remote troubleshooting. Command line interface (CLI) can also be used to collect information and automate reporting using scripting tools that can interact with the CLI.

IP Appliances also support SNMPv2c and SNMPv3 for monitoring network elements for conditions that warrant administrative attention. IP Appliances come with an extensive list of both proprietary MIBs and public MIBs to provide abundant element information to an element management system. SNMP configuration can be easily performed in the web user interface.

Monitoring Enhancements

Monitoring enhancements in the newer IP Appliance Software include:

- Historical reports accessible through the web user interface navigation tree Monitor > Reports.
- Graphs that display the latest snapshot from the table
- Line graphs that are scrollable
- Data points on line graphs displaying the values and timestamps
- Pie graphs that can be rotated to view various slices properly
- Pie graphs that can be viewed in 3D or 2D mode
- Printing of the graphs
- Live monitoring of CPU utilization, memory utilization, load average, and disk utilization
- Live monitoring of ADP service modules

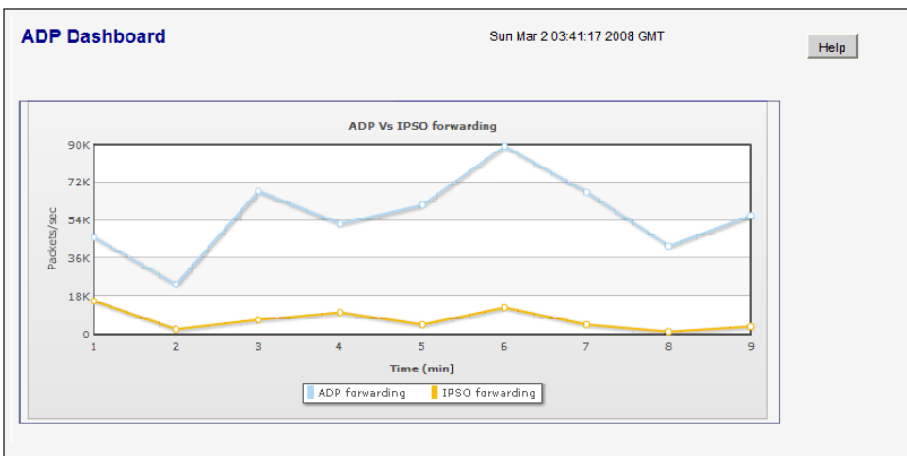
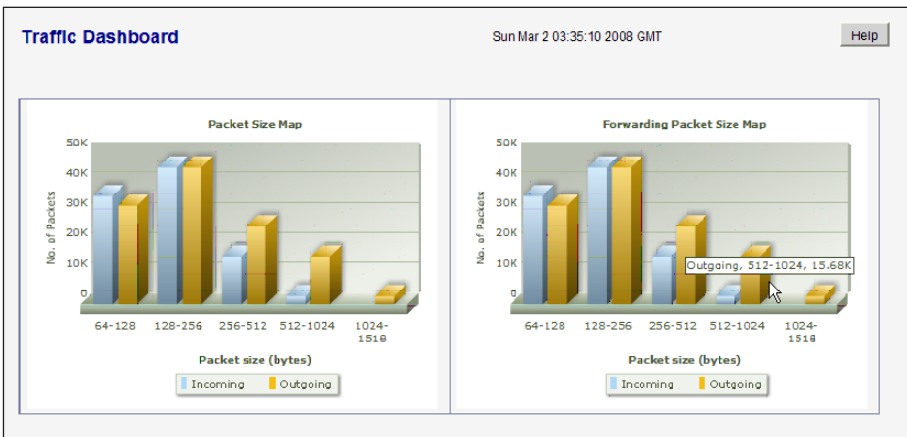
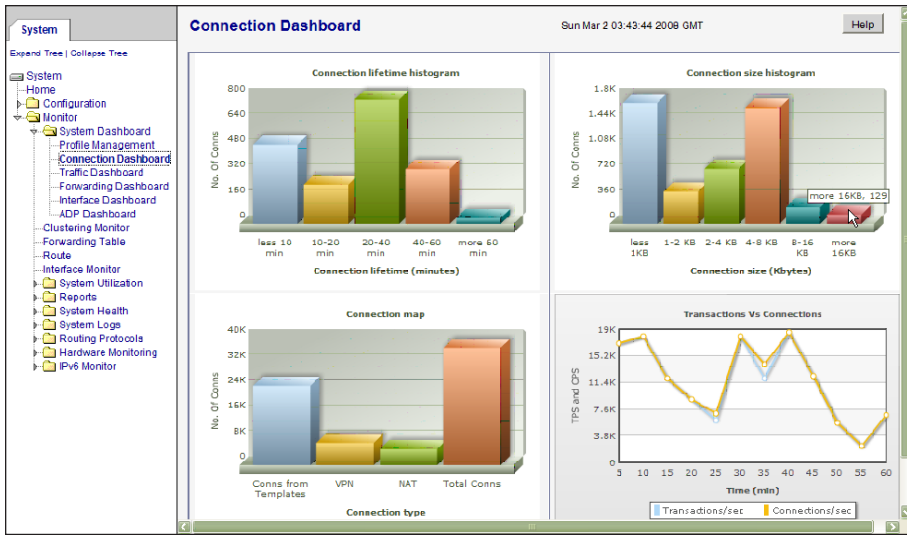
IP Appliances add performance monitoring to provide customers ways to analyze their Appliance for system performance, troubleshooting, capacity planning, traffic policing, and to measure the overall value of the system. This is achieved by providing traffic statistics, data points, and interactive graphs. Traffic statistics include:

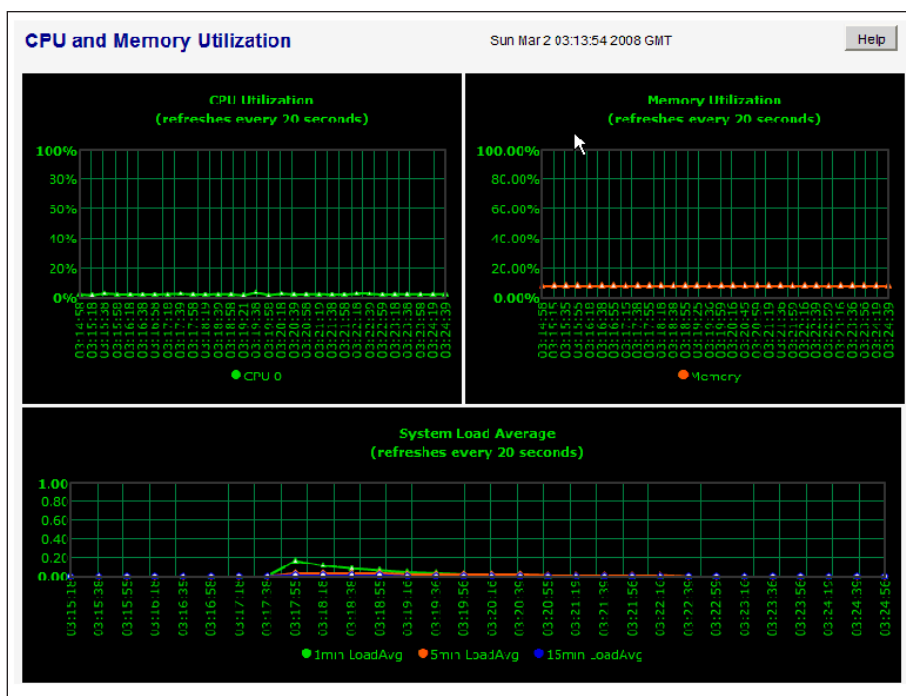
- Connection lifetime
 - Transaction size
- vPacket size at system level
- Connections per second statistics
 - Different types of connection including NAT, VPN, template type connections
 - Link bandwidth utilization
 - ADP forwarding vs. OS forwarding
 - ADP backplane statistics
 - Per core forwarding statistics

IP Appliances also collect new interface error counters statistics displayed through web interface and CLI. The new Rx (input side) error counters that are displayed are:

- RxError (Rx error counter)
- RxNoBuffer (this counter indicates the Rx no buffer occurring)
- CarrierExtnError (carrier extension errors)
- LengthError (Rx length errors)
- AlignmentError (Rx alignment error)
- CRCErrror (CRC error counter)
- DropPackets (Rx dropped packets counter)

Below are the screenshots of enhanced monitoring pages.





Multi-processor Support

IP Appliances provide multi-processor and multi-threading features that function in parallel with Check Point CoreXL technology. CoreXL helps the firewall use multiple cores effectively especially for connections demanding heavy CPU cycles. This is achieved by loading multiple firewall instances into the memory and each firewall instance is assigned to a different core. Each firewall instance maintains its own connection table. A dispatcher in Check Point OS gets all the packets and chooses the instance that will process a given packet. A given connection is restricted to a single core and all the packets belonging to that connection are handled by that particular core.

CoreXL support in IP Appliances provides performance benefits for accelerated connections and non-accelerated connections. Non-accelerated connections (connections not accelerated by SecureXL) in particular are expected to see considerable performance improvements as non-accelerated connections are more CPU intensive.

Conclusion

IP Appliances provide level of design, performance and usability that set the standard on delivering high performance and highly resilient security services to demanding networks. IP Appliances have received less than a handful of CERT vulnerability alerts within last ten years. IP Appliances support for IPv6 demonstrates Check Point's investment in the future as well as focus on compatibility with IPv6 RFCs. IPv6 includes a transition mechanism that allows users to adopt and deploy IPv6 in an easy way and provides direct interoperability between IPv4 and IPv6 hosts. Check Point IP Appliances remain focused on the needs of customers and continue to recruit new technologies to deliver high performance, security and usability.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street

Tel Aviv 67897, Israel

Tel: 972-3-753 4555

Fax: 972-3-624-1100

email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway

Redwood City, CA 94065

Tel: 800-429-4391 ; 650-628-2000

Fax: 650-654-4233

URL: <http://www.checkpoint.com>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMSecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.