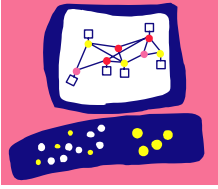
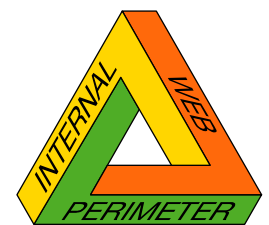


Check Point™
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Web Security Frequently Asked Questions



Intelligent Security

General

1. What is Check Point Announcing?

Check Point is announcing delivery on our Web security strategy with several new products and technologies:

- **Connectra™** is a complete Web Security Gateway with secure remote access. Connectra is a Check Point appliance.
- **Web Intelligence™** is Web application firewall technology that is integrated into Connectra and available as a technology add-on to VPN-1™ Pro and VPN-1 Express.
- **SSL Network Extender** is a browser plug-in that provides full network-level access via SSL without installing software. SSL Network Extender is built into Connectra and is available as a technology add-on to VPN-1 Pro and VPN-1 Express.

2. When will the products be available?

Check Point's Web Security products are orderable immediately.

- **Web Intelligence** will be shipping for VPN-1 in May 2004. Web Intelligence will be shipped within VPN-1 Pro and Express release version R55W.
- **Connectra** will become available in June 2004. Web Intelligence will be included in Connectra when it ships.
- **SSL Network Extender** will be available in July 2004.

3. I already have a firewall, why do I need more Web security?

You may or may not. Check Point Web Intelligence is designed for organizations using Web applications and a Web infrastructure for their business. Web Intelligence is specifically designed to provide protection for Web applications. Check Point Connectra and SSL Network Extender are designed for organizations who need secure connectivity over the Web. Generally, the more Web-enabled an organization, the more Web security is required.

4. Which OPSEC partners will be working with Check Point to deliver integrated Web Security solutions?

Several OPSEC partners are supporting our Web Security launch: RSA, Citrix, VeriSign, Computer Associates, Layer N, and Key Computing.

Web Intelligence Product Questions

5. What is Web Intelligence?

Web Intelligence is Web application firewall technology for Check Point products. It provides:

Malicious Code Protector

Patent-pending technology that catches buffer overflow attacks and other malicious code.

Advanced Streaming Inspection

Extends the inspection and reconstruction capabilities of the INSPECT™ architecture by adding active traffic control of live traffic streams.

Simple Deployment and Management

Built to be quickly deployed to protect Web servers without complex tuning and configuration.

Seamless Integration with Check Point Products

Provides protection for the entire Web environment.

6. What is the difference between Web Intelligence and Application Intelligence?

Application Intelligence is a set of advanced capabilities, integrated into Check Point's FireWall-1 and SmartDefense, which detects and prevents application-level attacks. Web Intelligence offers an additional layer of defense for the Web environment, adding

- Malicious Code Protector
- SQL Injection
- Command Injection
- Granular HTTP Format Sizes
- Granular Allowed HTTP Methods
- HTTP Header Spoofing

7. I am currently using SmartDefense for some Web protection. Will those features go away with the upgrade to R55W?

No. Existing Web security features in SmartDefense will be available in R55W at no additional cost for customers with valid software subscriptions. The features will be available under the "Web Intelligence" tab in the new GUI.

8. I already have an IDS/IPS solution for my Web servers, why do I need more Web protection?

Web Intelligence is designed specifically for Web applications and the Web environment. IDS/IPS solutions are generalists when it comes to Web protection and can't address many of the Web application-specific issues that Web Intelligence solves.

9. What is Malicious Code Protector?

Check Point's Malicious Code Protector is a patent-pending technology that catches buffer overflow attacks and other malicious code. It provides a revolutionary way to provide this protection without the need for signatures. It can detect malicious executable code within Web communications by identifying not only the existence of executable code in a data stream but its potential for malicious behavior. Malicious Code Protector is a kernel-based protection delivering wire-speed performance.



10. Is Malicious Code Protector only available in Web Intelligence, how about other products like SmartDefense?

Today, Malicious Code Protector is available only for Web applications. The same patented technology will be used with other products as well, protecting other applications.

11. How will Web Intelligence impact the performance of a VPN-1 gateway?

Web Intelligence will have a relatively small performance impact on VPN-1 Pro and VPN-1 Express gateways. When used, Malicious Code Protector will have a 5-10 percent impact and Active Streaming a 10-20 percent impact. With Malicious Code Protector and Active Streaming are used together, there is a 20-30% combined impact.

12. What platforms does Web Intelligence support?

On VPN-1 Pro and VPN-1 Express, Web Intelligence requires NG with Application Intelligence R55W. R55W supports all VPN-1 gateway platforms, including SecurePlatform, Linux, Solaris, and Windows Servers in general availability. Nokia IPSO will be supported by the end of May.

Web Intelligence is also included with Connectra and will be integrated into InterSpect before the end of 2004.

13. When will Web Intelligence be available on Nokia?

Web Intelligence will be available on IPSO 3.7 and 3.71 in late May 2004. There are no plans to support Web Intelligence on IPSO 3.8 at this point.

14. When should customers use R55W or R55?

R55W should be used by customers who need Web Intelligence, or who need specific SmartDefense solutions delivered in R55W such as new DNS security or Peer-to-Peer security features. R55 should be used for customers who do not need Web Intelligence or specific SmartDefense protections.

15. How is Web Intelligence managed?

Web Intelligence is managed through SmartCenter today and by Provider-1 in the future. Administrators can define firewall policy, SmartDefense and Web Intelligence configuration from one centralized user console. Web Intelligence logs are also centrally stored and analyzed with the rest of Check Point logs.

16. Does Web Intelligence support High Availability (HA) environments?

Yes. Web Intelligence is integrated with Check Point ClusterXL™ and interoperates with VRRP and other external clustering technologies.

Connectra Product Questions

1. What is Connectra?

Connectra is a Complete Web Security Gateway with Secure Remote Access. It provides:

Secure Web-Based Connectivity

Combines easy SSL VPN Web and network-level access with unmatched protection for the entire Web environment

Integrated Server Security

Delivers strong server protection using Check Point's Stateful Inspection, Application Intelligence, and Web Intelligence

Adaptive Endpoint Security

Accommodates diverse access needs with spyware, integrity, and adaptive access protection

One-Click Remote SSL Access

User Portal and SSL Network Extender SSL-enables internal servers without altering servers or network infrastructure

2. How is IPSec remote access different from SSL VPN?

IPSec VPN and SSL VPN are based on different protocols and each solution has its own unique strengths and weaknesses. In general, IPSec VPN includes a remote access client on an endpoint, while an SSL VPN uses an Internet browser capable of SSL as the remote access client. For additional information see the Check Point White Paper: *IPSec and SSL Deployment Considerations* available on Check Point's Web site.

3. Why do I need SSL VPN?

You may or may not need an SSL VPN. In general, SSL VPN is used by organizations that are looking for the "clientless" remote access. For additional information see the Check Point White Paper: *IPSec and SSL Deployment Considerations* available on Check Point's web site.

4. Is SSL VPN as secure as IPSec VPN?

VPNs, whether SSL or IPSec, are not inherently secure. Both SSL and IPSec VPNs require integrated endpoint and gateway security capabilities in order to be secured. Check Point pioneered both endpoint and gateway security for IPSec VPNs. For SSL VPNs Check Point is the first and only vendor to address the complete security requirement.

5. Can Connectra be used as a Site-to-Site VPN gateway?

Connectra is designed for Web remote access and not site-to-site connectivity. Check Point VPN-1 is the recommended solution for site-to-site connectivity over the Web.

6. Does Connectra come with a firewall? How about SmartDefense and Web Intelligence?

Connectra is a Web Security Gateway specifically intended for connecting remote users over Web-based technologies and performs different functions than a general-purpose firewall. In addition to connectivity, it provides multiple levels of protection, including granular user and application access controls and Web Intelligence for Web traffic. Such integrated protection can be co-deployed with an existing Firewall without compromising perimeter security.



7. On what platforms is Connectra available?

Connectra is available as a Check Point appliance. The current series of the Connectra appliance was developed and manufactured in partnership with Dell.

8. How do I know which Connectra model to choose?

Connectra Model	Target Customer	User License Options	Optional Add-ons
Connectra 1000	Medium Sized Organizations	50, 100, 250	Endpoint Security
Connectra 2000	Medium to Enterprise Organizations	100, 250, Unlimited	Endpoint Security, Dual Power Supply
Connectra 6000	Enterprise to High-End Organizations	250, 500, Unlimited	Endpoint Security (6000 includes SSL Acceleration and Dual Power Supply)

9. On what operating system does Connectra run?

Connectra is based on SecurePlatform™, Check Point's secure, hardened operating system that is widely used by Check Point customers.

10. How is Connectra managed?

Connectra includes Web UI local management based on Check Point's SMART architecture. No separate management server is required to manage Connectra. In addition, Connectra logs can be viewed in Check Point SmartView™ Tracker.

11. Where should Connectra be deployed in a network?

A typical organization will deploy Connectra in a DMZ. With integrated access control and attack protection, Connectra is a secure platform that can also be installed before a perimeter firewall or behind a perimeter firewall.

12. Does Connectra support high availability (HA) environments?

Connectra 1.0 supports HA via separate configuration of two or more devices. In the future more advanced HA configurations will be supported.

13. How do you control what resources users have access to?

The Connectra administration interface allows administrators to define individual applications, Web links, and file shares. Users can access only those resources that they are explicitly allowed to access.

Each resource is also defined with a specific security sensitivity level, as configurable by the administrator. Users are only allowed access to explicitly allowed resources, including granting variable access rights based on the defined security of the endpoint.

14. Does Connectra work with RSA SecureID?

Yes, Connectra can communicate to an ACE server to support SecureID. In addition, administrators can define that certain resources can be accessed only if a user is authenticated using SecureID.



15. How do we address endpoint security?

Connectra provides an integrated set of endpoint security features that were largely developed by Zone Labs, the market leader in endpoint security. Connectra can inspect endpoints for spyware, key stroke loggers, and other malware. In addition, Connectra provides dynamic access controls to associate allowable resources to the security level of the endpoint. For example, a security policy can restrict certain resources to only those users who have passed an endpoint inspection and who use a token for authentication.

16. What browsers does Connectra support?

End users can use IE (5.5 and up), Mozilla, Safari, and Netscape. Administration of Connectra is supported using IE (5.5 and up).

17. Can Connectra be used to support PDAs and cell phones?

Connectra can connect with SSL enabled browsers. Connection to PDAs and cell phones depends on the Web browser used by the endpoint device.



SSL Network Extender Product Questions

1. What is SSL Network Extender?

SSL Network Extender is a browser plug-in that provides full network-level access via SSL without installing software. SSL Network Extender is built into Connectra and is available as a technology add-on to VPN-1 Pro and VPN-1 Express.

2. Do I need SSL Network Extender for all SSL Connections?

No, SSL Network Extender provides SSL VPN capabilities for client/server applications. For Web, email, and file sharing, Connectra comes with a user Web portal that can be accessed over SSL from a Web browser.

3. What Check Point products can integrate with SSL Network Extender?

SSL Network Extender is integrated with Connectra and is an optional add-on for VPN-1 gateways.

4. What applications does SSL Network Extender support?

SSL Network Extender supports any IP-based network application, including TCP, UDP, and applications using dynamic ports such as FTP and VoIP. SSL Network Extender requires a Web plug-in and administrator privileges on the remote endpoint.

5. What are the endpoint requirements for SSL Network Extender?

SSL Network Extender is supported by Windows 2000 and up, IE 5.5 and up.

Support

1. Do I need to activate a license on the User Center to use Connectra?

No. Connectra will already be in the User Center and all Connectra systems are pre-licensed and will work out of the box without the need for license activation. However, users must register Connectra units in the User Center in order to activate the SmartDefense subscription included with each device and in order to upgrade their products. In general, Check Point recommends registering all products in the User Center.

2. What are the warranty terms for Connectra?

Connectra comes with a one-year hardware warranty. Hardware warranty can be extended when purchasing an Enterprise Support agreement.

3. What are the support options for Connectra?

Support options for Connectra are the same as InterSpect™.

	Year 1	Year 2	Year 3
Normal Warranty	Next Business Day On-site	N/A	N/A
Enterprise Software Subscription	Next Business Day On-site	Next Business Day On-site	Next Business Day On-site
Enterprise SS & Standard Support	5 X 10, 4 Hour On-site	5 X 10, 4 Hour On-site	5 X 10, 4 Hour On-site
Enterprise SS & Premium Support	7 X 24, 4 Hour On-site	7 X 24, 4 Hour On-site	7 X 24, 4 Hour On-site

4. When will Connectra demo units be available?

Orders can be placed starting May 3rd. Units will start shipping in June.

5. What is the Return Materials Authorization (RMA) process for Connectra?

The RMA procedure is the same as it has been for InterSpect, VPN-1 Edge and Safe@Office. The Service Request and RMA process are facilitated by Check Point Technical Services (<http://www.checkpoint.com/support>)