



Connectra Link Translation

Contents

Abstract	3
Who should read this white paper?	3
Assumed Knowledge	3
Introduction	3
Link Translation technology overview	4
URL Translation method (UT)	6
Hostname Translation method (HT)	6
Decision to use Hostname Translation or URL Translation	9
Application support in Connectra R66	11
Migration from URL Translation to Hostname Translation	11
Wildcard DNS	12
Wildcard Certificates	12
Summary	13

Abstract

This paper provides an in-depth discussion of Link Translation technology alternatives in Check Point's Connectra SSL VPN security gateway. This paper describes the technology, solution concept and alternatives for deployment and use.

Who should read this white paper?

This paper is intended for a wide audience, including IT system administrators, network administrators, IT managers and security consultants. It benefits those who work with Check Point products such as the Connectra SSL VPN gateway and who are responsible for security decisions and activities in their company.

The purpose of this paper is to provide a deeper understanding of Connectra's Link Translation alternatives, implications and deployment requirements. Administrators who are performing initial deployment of the Connectra gateway will find this paper helpful, as will those who are seeking to migrate from the default URL Translation (UT) to Hostname Translation (HT). This paper describes what is required to deploy Connectra in HT in terms of prior deployment, configuration and security considerations.

This is not intended to serve as a general configuration guide for the Connectra gateway or any other Check Point products. For general Connectra SSL VPN gateway deployment information, see the "Connectra Administration Guide", located at <http://supportcenter.checkpoint.com/> in the "Documentation" section.

Assumed Knowledge

This paper assumes that the reader has the following knowledge and experience with Connectra and Check Point security products:

- Connectra basic administration
- Certificates (enrollment and deployment)
- Understanding / work experience with DNS systems

Introduction

Link Translation is the core technology used in Connectra to enable clientless remote access. Link Translation allows users to access internal data resources from public, unsecured networks while maintaining the security of those internal resources and content. Use of the SSL protocol then protects communication in transit between the client and Connectra.

Since the HTTP protocol does not inherently support clientless remote access, a form of web-content rewriting—Link Translation—is required. Connectra supports two methods of Link Translation for rewriting web content: URL translation (UT) and Hostname translation (HT).

UT is set as the default in a Connectra installation. No additional configuration from the administrator is required to achieve UT functionality.

HT is an alternative to UT. HT supports a broader set of Web sites and applications, has higher performance, and adds even greater security. To deploy a Connectra HT-based environment, the administrator must perform additional configuration and deployment steps.

HT and UT may also be used in conjunction with each other to achieve the most comprehensive Web site and application support. This document describes the differences between the two alternatives including how they function, a comparison of features, and steps for additional configuration.

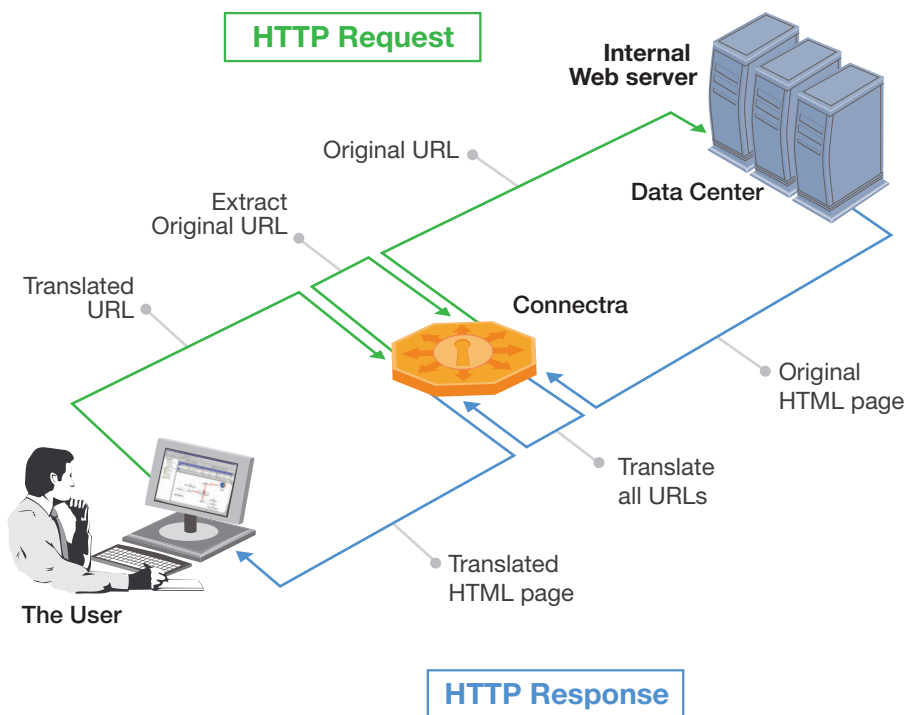
Link Translation technology overview

1. Concept

Link Translation is the key technology in Connectra that enables clientless secured remote access. With Connectra's Link Translation, users can access internal web servers from public networks without needing to install any type of VPN client. Link Translation offers a pure clientless, secure remote access solution.

Link Translation works by converting an internal URL used in the local network address space into a public URL that is valid and acceptable on the Internet. With this translation, a user can securely access internal resources via any Web browser without compromising internal server addresses (URLs) or content.

Users connect over the Internet to Connectra to access internal servers as shown below. This figure illustrates the role of Link Translation within Connectra.



2. Challenge

Internal servers deployed in corporate networks are generally hidden from the public Internet. Typically, their addresses refer only to internal hosts, as in this example:

<http://internal.example.local/page1.html>

The same internal URL might be presented as a link on the front end web server (the server that is accessible from the Internet). Users can connect and view the front end web server's HTML page, and have an internal URL (not accessible via public internet) in the page. Here is an example of an internal URL link that might be on a public web page:

```
<a href="http://internal.example.local/page1.html">page1</a>
```

This presents two problems for users trying to access internal resources from outside the corporate LAN. First, users cannot connect to the internal web server via a direct URL, nor from the front end web server HTML page since the internal servers are not recognized by public DNS servers in the Internet. This essentially leaves internal resources unreachable from outside the corporate LAN. Second, HTTP is an unsecured protocol for data transmission. When HTTP is used, data travels unencrypted on public networks, leaving it vulnerable to unauthorized eyes or "data leakage."

3. Solution

Link Translation overcomes these challenges in the following ways:

- Connectra operates between the Internet and internal servers. Users seeking to access internal web content are forced to pass through the secured Connectra gateway.
- All URLs are translated and converted into the Connectra domain.
- Connectra translates the original URL into a new URL that is accessible from the Internet while hiding the original URL inside the new URL.
- To secure the communications in transit between the user and servers, Connectra enforces use of HTTPS, a secure SSL-based protocol.

For example:

Original URL:

<http://internal.example.local/path1/page1.html>

The URL after translation by Connectra, using URL Translation (UT):

<https://connectra.example.com/representation of the orig. URL>

or:

After translation by Connectra using Hostname Translation (HT):

<https://acxjfkuriew12ds.connectra.example.com/original path>

Note: the above example shows the two alternative methods of Link Translation available within Connectra and described in this document. The underlying concept behind Link Translation—modifying URLs to enable outside access while protecting internal servers—is the same for both methods. There are differences between UT and HT in the details of how this translation is accomplished; these are described in the following sections.

URL Translation method (UT)

UT is the default form of Link Translation set in Connectra. To use UT, administrators do not need to perform any additional configuration or deployment steps. UT enables users to access a broad array of Web sites and applications.

UT works by converting an internal URL into a publicly-accessible one by adding the internal URL content to Connectra's public URL. For example:

If the original internal URL is:

<http://internal.example.local/path/page.html>

And Connectra's Fully Qualified Domain Name accessible from the Internet is:

<https://connectra.example.com>

The translated URL would be:

<https://connectra.example.com/Web/path/page.html.CVPNHost=internal>

UT supports translation of a range of Web applications and content, including:

- HTML / XHTML / CSS
- JavaScript
- VBScript (partially)
- Citrix (web interface)
- SharePoint
- iNotes
- SAP

For a complete list of applications supported, refer to the section, "Application support in Connectra R66," on page 11.

Hostname Translation method (HT)

1. Brief summary

In addition to UT, Check Point Connectra offers an alternative Link Translation method, one that leverages an advanced technology known as Hostname Translation (HT). HT extends the range of applications that can be accessed via remote clientless access, including support for SAP, Siebel, SharePoint, VBScript and others. HT offers higher performance than UT while providing even greater security. Following are important highlights of HT:

- HT provides superior application compatibility, performance and enhanced security.
- Check Point strongly recommends configuring Connectra to work in HT since HT supports a greater number of applications and web sites. Some web sites and applications will only work with HT. Refer to the "Comparison table" on page 11 and the "Application support" table on page 12 for more information.
- A fewer number of Web sites and applications will only work with UT. To accommodate the most-comprehensive clientless remote access coverage, Connectra can be configured to assign a Link Translation method on a per-application basis. To learn more about this option, read the section, "How to configure Link Translation method per application," in the document, "Using and Configuring Link Translation in Connectra".

- To deploy and use HT, administrators must perform a one time configuration and set up. The administrator will also need to establish a DNS server that holds the company domain name. The administrator will need to obtain a wildcard SSL certificate in order to support seamless HT functionality. These requirements are described further in the section, “Migration from URL Translation to Hostname Translation,” on page 11.

2. How HT works

HT works by converting every internal web resource (URL) into a virtual host address that is part of the Connectra domain. This contrasts with UT where translated URLs point to the Connectra hostname with the original URL encoded into the URL path.

When working in HT mode, Connectra’s URLs do not represent a single server, but rather become a sub-domain of multiple virtual servers, each with a unique host name associated with a particular web application. Here is an example:

If Connectra has this address:

<https://connectra.example.com>.... ,

The internal Web application will follow this format:

<https://UniqueHostName.connectra.example.com>....

In the above example, the host “UniqueHostName” represents a virtual sub-domain of Connectra: *.connectra.example.com

The “UniqueHostName” is an encoded internal host name taken from the host portion of the original URL. The resource portion of the original URL is added as a suffix in the Connectra translated URL, for example:

If the original URL is:

<http://internal.example.local:77/path/file>

Connectra access URL:

<https://connectra.example.com>

Connectra’s sub-domain DNS:

https://*.connectra.example.com

The translated URL will be:

<https://-77-internald0tcompany-com.connectra.example.com/path/file>

Note: The “-“is reserved part to separate the different parts of the translated host.

- In order to protect internal resources host names (DNS requests when connecting to Connectra are sent in clear text), the “UniqueHostName” component is obscured by Connectra. Thus, users are not able to see the original Web servers DNS names.
- HT obscures internal resource names on a per-user session basis, meaning that the “UniqueHostName” is different for each user’s session. (This obscured name then remains the same until the session is ended). Administrators can configure the “UniqueHostName” to change every time a user initiates access to the internal web resources and applications. For example, if one session connected to a Web application and server has the following translation:

<https://c78-n96jkahsuyehdjeu10-ma.connectra.example.com/path/file>

the next session would have a completely different “UniqueHostName”, as in:

<https://e99-q16asowu8eiuw11a-po.example.com/path/file>

Note: the ability to obscure uniquely per-user, per-session is enabled by default in Connectra in order to provide maximum security. An administrator can disable the obscuring feature if they wish. To do so, refer to the section, “Advanced HT configuration,” on page 26 in the document, “Using and Configuring Link Translation in Connectra”.

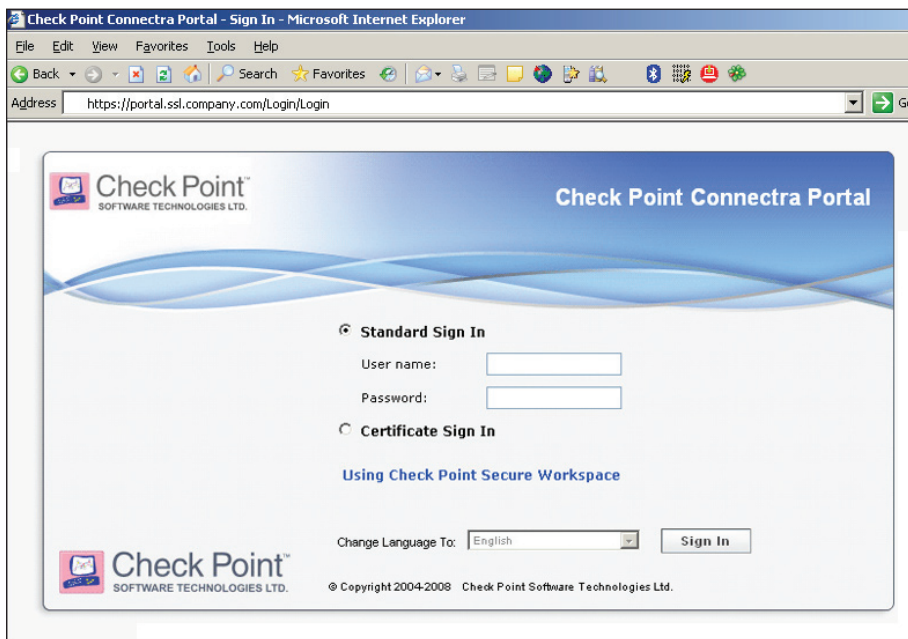
3. Connection flow

A user connects to the Connectra gateway by entering Connectra’s main domain address, for example:

<https://connectra.example.com>

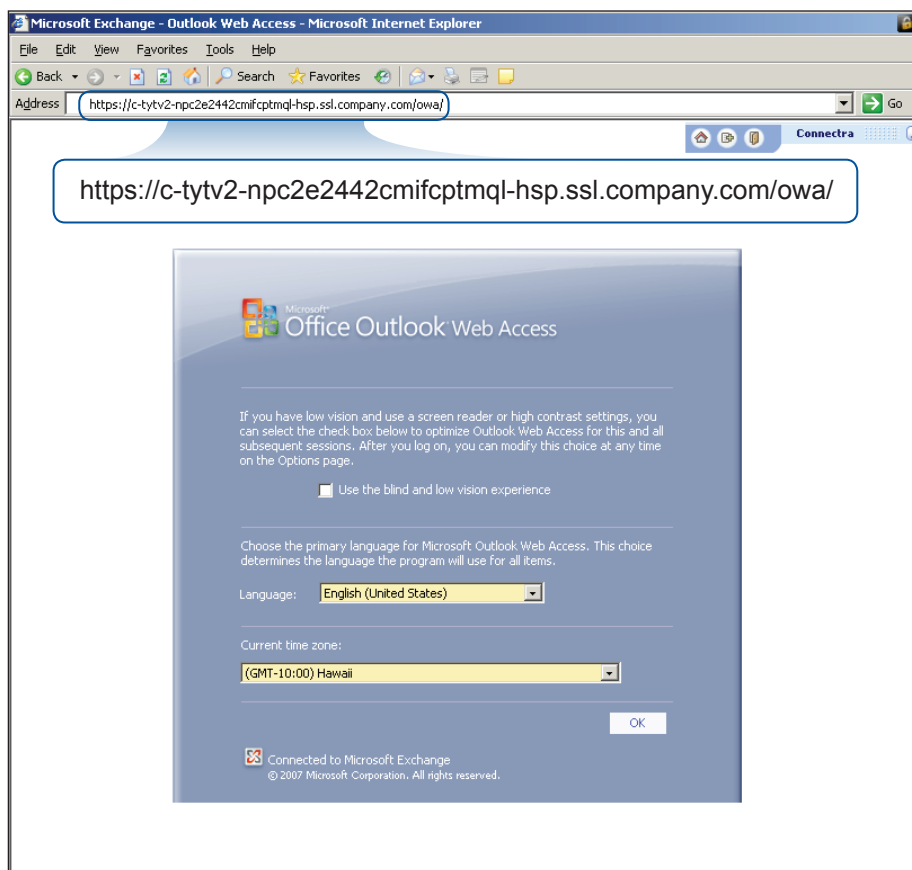
Connectra immediately redirects the user to a Web Portal page, while translating the original URL to the HT-based URL, as follows:

<https://portal.connectra.example.com/Login/Login>



Please note that the “portal” hostname is a reserved fixed host for accessing the Connectra Web Portal. It always points to the portal HTML page. The HT mechanism is aware of this and will refrain from translating the reserved name.

After successful authentication, the user can run any application or access a Web page located in the Connectra Web portal. The next figure provides an example URL of how HT works with Microsoft OWA:



Decision to use Hostname Translation or URL Translation

1. Check Point recommendation

Check Point highly recommends working in HT mode since this method significantly improves performance on both Connectra and the client side. HT provides support for more Web sites and applications while enhancing security. The administrator must, of course, take into consideration prerequisites for deployment of HT in Connectra, including DNS re-configuration and wildcard certificate generation, described in the section, “Migration from URL Translation to Hostname Translation,” on page 11.

2. Comparison table

The following table presents a comparison of UT and HT Link Translation methods across a range of features and specifications. This table is intended to help administrators choose which method is most appropriate for their Connectra environment.

Spec / Feature	URL Translation	Hostname Translation
Initial Deployment	UT is the default Link Translation method in Connectra. It does not require any additional configuration or settings. UT is activated automatically after Connectra installation.	HT requires that the following settings and steps be performed after Connectra has been installed: <ul style="list-style-type: none"> • Configure the DNS server to support the company's sub-domain. • Issue and install a new wild-card certificate in Connectra. • Configure HT to be the default method for Link Translation or define its use on a per-application basis.
Server (Connectra) Certificate	Regular	Wildcard certificate required. For example, issued for: *.connectra.example.com
DNS settings	Regular: connectra.example.com	Requires a wildcard sub-domain DNS, for example issued for: *.connectra.example.com
Security	SSL secured <ul style="list-style-type: none"> • Internal server access protection (private IP address not accessible) • Cross-site request forgery (CSRF) attack prevention • Cookies are saved on server side only 	SSL secured <ul style="list-style-type: none"> • Does not reveal the names of internal web servers by obscuring a hostname in the Link • Cross-site request forgery (CSRF) attack prevention • Cookies can be saved on both server and client side
Performance	Standard Performance	3 times faster than UT, HT provides significantly improved performance over UT.
Save Files from Internet (Including webmail attachments)	Filename Modified	Same as original
IP address based browsing to Connectra gateway	Supported	Not supported
Single Sign On (SSO)	Supported	Supported
Floating Navigation Bar	Supported	Supported
Cookie	On Server (Connectra) side	On Server (Connectra) or Client (Browser) side, according to configuration
Clientless support	Yes	Yes

Application support in Connectra R66

Application	UT	HT
iNotes (Version 6.0, 6.5.1 to 6.5.4 (design template version iNotes 6) 6.5.5 and 7.0.x)	Supported	Supported
Microsoft Outlook Web Access (OWA) (Version 2000, 2003, 2003 SP1 ,OWA 2007)	Supported	Supported
HTML	Supported	Supported
General JavaScript	Supported	More comprehensive support for Java
ActiveX and Java applets	Partial support	More comprehensive support
Domino Web Access 7.0.1	Not supported	Supported
Citrix 3.0-4.0	Supported	Supported
SAP	Not supported	Supported
Siebel	Not supported	Supported
Microsoft SharePoint (except MS Office applications that are using WebDav)	Not supported	Supported
Oracle (depending on version and client applet)	Not supported	Supported
VBscript	Not supported	Supported

Migrating from URL Translation to Hostname Translation

The administrator should perform the following steps prior to either migration or setting up Hostname Translation in Connectra:

- Review the list of Web applications supported and not supported by HT.
- Select a sub-domain for Connectra Access. Make sure that this selected sub-domain is unique and not already associated with other environments. For example: *.connectra.example.com. Users will then access the Connectra Web portal by entering <https://connectra.example.com> in their web browser.
- In the event that your DNS configuration is handled by your local ISP, contact the ISP and request the following definitions. The same actions are required when your DNS system is managed locally:
 - Request a sub-domain for your company.
 - Request setup of a wildcard DNS for the chosen sub-domain (more details below).
- Contact your chosen Certificate Authority (CA) vendor and request the following:
 - Confirm that the vendor provides wildcard certificates.
 - Purchase a wildcard certificate. Generally, a price for a wildcard certificate is higher than for standard certificates; however you can notify the CA vendor that the certificate will be used only to secure a single “virtual domain” of Connectra gateway.
 - Validate that you can request a wildcard certificate with the Fully Qualified Domain Name (FQDN) name that matches your sub-domain e.g. “*.connectra.example.com”
- Refer to the Connectra R66 Admin guide in order to proceed with the configuration of Hostname Translation.

Wildcard DNS

1. Concept

A wildcard DNS record is a record in a DNS zone file that will match all requests for non-existent domain names, i.e., domain names for which there are no records. A wildcard DNS record is represented by an asterisk "*" placed to the left of the domain name, e.g.

***.example.com**

The "*" specifies a sub-domain of the main domain. In the above case, the main domain would be

"example.com".

The wildcard DNS should point to a single host, located in the main domain, for example:

host.example.com

In the example above, a wildcard DNS record will instruct the DNS lookup system to return the DNS record of host.example.com for each request for ANY.example.com.

2. How wildcard DNS is used in Connectra

A wildcard DNS is used in Connectra to support Hostname Translation by utilizing a virtual host address for translation, which is a part of a main Connectra domain.

For instance if the Connectra domain is: **connectra.example.com** a wildcard DNS should be defined as: ***.connectra.example.com**, where the hostname ("*") will be used for translation.

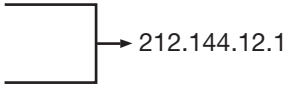
All virtual hostnames will be resolved by a DNS server and mapped to a single IP address for the Connectra gateway.

Example:

Connectra domain: connectra.example.com > IP address 212.144.12.1

Wildcard DNS: *.connectra.example.com

c78-n96jkahsuyehdjeu10-ma.connectra.example.com
 a1e-9a9hwuhd22nnjd1a-1a.connectra.example.com
 i51-kjhdakdhakjdahkja33-9y.connectra.example.com



Wildcard Certificates

1. Introduction

Secure SSL communications requires that Connectra gateways establish trust with endpoint computers by presenting credentials in the form of a Server Certificate.

Connectra, by default, uses a self-signed certificate as its server certificate. When an endpoint computer attempts to connect to the Connectra gateway by presenting the self-signed certificate, a certificate warning messages appears in the browser. In order to prevent these warnings, the administrator must install a server certificate signed by a trusted certificate authority.

In order to work in HT, the administrator needs to obtain a wildcard certificate from the CA vendor.

2. Wildcard certificates overview

The wildcard certificate allows administrators to secure multiple sub-domains on one main domain on the same server. This functionality is achieved by using a wildcard “*” domain pattern, presented in the certificate common name and acknowledged by Internet browsers authenticating a web server when accessing the domain.

For example: *.domain.com

In this case the wildcard certificate issued for this domain will secure any sub-domain of the domain.com server e.g.:

- mail.domain.com
- web.domain.com
- owa.domain.com
- ssl.domain.com

All hosts in the wildcard certificate, when used in Connectra, are virtual and are mapped to a single gateway through DNS.

3. Wildcard certificate security aspects

Appropriate use of wildcard certificates in Connectra will not compromise the security of the Connectra gateway or any other component in your environment.

A wildcard certificate should be installed and used only for Connectra purposes and to protect a sub-domain, which is defined by a wildcard DNS for Connectra HT. The administrator should ensure that there are no other servers defined with the same sub-domain as used for Connectra.

4. How to obtain a wildcard certificate

To obtain a wildcard certificate contact your CA vendor representative or use your corporate account to generate a certificate request. Some CA vendors do not allow clients to generate a wildcard certificate via a corporate account. In such cases the client should contact the vendor and explain the need for such certificates, describing where and how it will be used.

A wildcard certificate is a standard SSL X.509 certificate with the same level of protection and security. Most vendors provide this service on a regular basis, so obtaining a wildcard certificate should not present a problem.

Summary

Connectra offers administrators two viable, secure Link Translation methods for enabling clientless remote web access. Based on considerations discussed in this paper, administrators can choose which is right for their particular environment. Connectra can be set up to use a single Link Translation method, either UT or HT. Connectra can also be configured to use both, assigning them on a per-application basis. This granular configuration enables access to the broadest range of web resources.

Check Point strongly recommends working in HT mode. HT offers significantly improved performance in Connectra. HT also provides support for more Web sites and applications, and enhances the security of Link Translation technology. In addition, Connectra allows for flexible configuration of both HT and UT by application, enabling the option to use both methods of Link Translation on the same box.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

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, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, 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, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, 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, VSX-1, 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.