

## CHAPTER 2: CONNECTRA ENDPOINT-SECURITY FEATURES AND DEPLOYMENT

---

Check Point Connectra is a complete Web Security Gateway that provides remote SSL VPN access. By combining SSL VPN connectivity and security in one solution, Connectra ensures organizations can effectively deploy SSL VPNs, while ensuring the confidentiality and integrity of company information that is critical to business success.

### Objectives

1. Compare and contrast Connectra server-side and client-side security features.
2. Compare the deployment of Connectra in the DMZ versus a LAN.
3. Create the necessary Rule Bases to control communication and traffic for both a DMZ and LAN deployment.
4. Perform an initial installation and configuration of Connectra, based on administrative requirements.

### Key Terms

- Administration Portal
- Web Intelligence
- SmartDefense

## CONNECTRA SECURITY FEATURES

Connectra provides secure remote access to corporate applications, primarily by integrating server and endpoint security, and functioning as a Clientless SSL VPN server. By providing the user with single-point access to applications, Connectra exists as a dedicated Gateway for remote locales. All connections to the Connectra Gateway are SSL encrypted to ensure privacy and data integrity, and are subjected to authentication and authorization. Moreover, both the information and applications made available to authenticated users have been protected, by enforcing security restrictions on the server and client sides. These restrictions are illustrated in the security features listed below.

### Server-Side Security

Administrative control takes place through the **Administration Portal** (admin portal), accessed from anywhere. Connectra employs a suite of Check Point products to ensure thorough management of secure remote access, easily controlled via the admin portal. See below for a detailed list of features:

**Check Point Web Intelligence** — Enables protection against malicious code transferred in Web-related applications: worms, various attacks such as Cross Site Scripting, buffer overflows, SQL injections, command injections, directory traversal, and HTTP code inspection

**Check Point SmartDefense** — Protects organizations from all known, and most unknown network attacks, using intelligent security technology

**SmartDefense Updates** — Adds new defense mechanisms to the SmartDefense and Web Intelligence consoles, and brings existing defense mechanisms up-to-date

**Granular authorization policy** — Limits users granted access to specific applications, by enforcing authentication, encryption, and client-security requirements

**Application support over HTTPS** — For Web-based applications, file shares, and mail support; access is allowed for a specific application set, rather than for full network-level access

**Separate portal for Administrators** — The admin portal is used to configure and control the Connectra Gateway. To access this portal requires Administrator level permissions.



**Fully integrated with the Check Point operating system — SecurePlatform**

**Encryption** — SSL Network Extender, used by Connectra, typically encrypts traffic using the 3DES or RC4 encryption algorithm.

## Client-Side Security

For remote users, Connectra employs strong encryption, scanning, and caching techniques to ensure client communication is secure in typical remote, unsecured environments. With the available Administrator-controlled protection-level settings, Web access can be secured for the retrieval of sensitive material, providing clients with an easily managed, seamless and secure connection to the internal network.

The following lists Connectra's key features for client-side functionality:

**Implements Integrity Clientless Security (ICS) for Connectra on the remote user's machine** — Prevents threats posed by malware types, such as worms, Trojan horses, attackers' tools, keyloggers, browser plug-ins, adware, third-party cookies, etc; organizations define endpoint-security requirements for accessing individual resources. ICS scans various spyware on users' desktops, before allowing them access to the internal network.

**Integrity Secure Workspace protects all session-specific data, accumulated on the client side** — End users can utilize Check Point's proprietary secure browser that prevents data leakage, by encrypting the browser's cache and clearing it at the end of the user session. The Administrator can configure Connectra (via protection levels) to force clients to use the Secure Workspace when accessing sensitive applications.

**Controls browser caching** — When accessing Web applications associated with a given protection level, Administrators can decide what Web content may be cached by browsers. Disabling browser caching can help prevent unauthorized access to sensitive information, thus contributing to overall information security.

**Captures cookies sent to the remote client by the internal Web server**

— Cookies provide a way of maintaining state information between clients and servers. If cookies are stolen, they may be used to impersonate a user. For this reason, Connectra captures the cookies and maintains them on the gateway. Connectra simulates Web server/user cookie transmission, by appending the cookie information to the request that Connectra makes to the internal Web server.

**Supports strong authentication methods** — For example, using SecurID tokens and SSL client Certificates

DRAFT



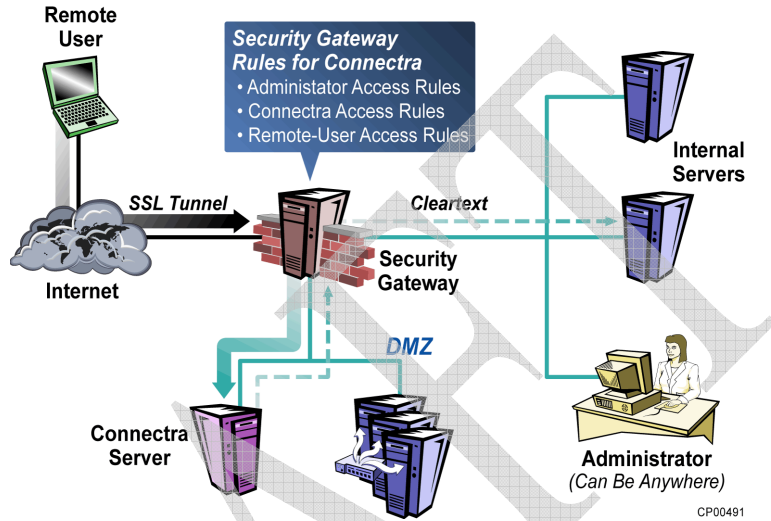
## DEPLOYING CONNECTRA

---

Generally, Check Point recommends that Connectra be deployed in the DMZ, but LAN deployment is also an option. In both deployment scenarios, SSL termination takes place at the Connectra Gateway. Web Intelligence, Application Intelligence, and authentication and authorization schemes are employed on the Connectra Gateway to inspect the traffic for harmful content or unauthorized requests, before it reaches the internal servers. Connectra is unique in that it has gateway-based application-level and network-level protection. Either deployment scheme requires appropriate rule base settings in the Gateway.

### Deploying Connectra in the DMZ

When Connectra is placed in the DMZ, traffic initiated both from the Internet and from the LAN is subject to firewall restrictions, as shown in the figure below. By deploying Connectra in the DMZ, direct access from the Internet to the LAN is avoided, as remote users initiate an SSL connection to the Connectra Gateway. The Gateway is configured to allow traffic from the user to the Connectra server, where Web Intelligence and Application Intelligence inspection, authentication and authorization take place. Requests are then forwarded to the internal servers via the Gateway. Administration traffic is always SSL encrypted.



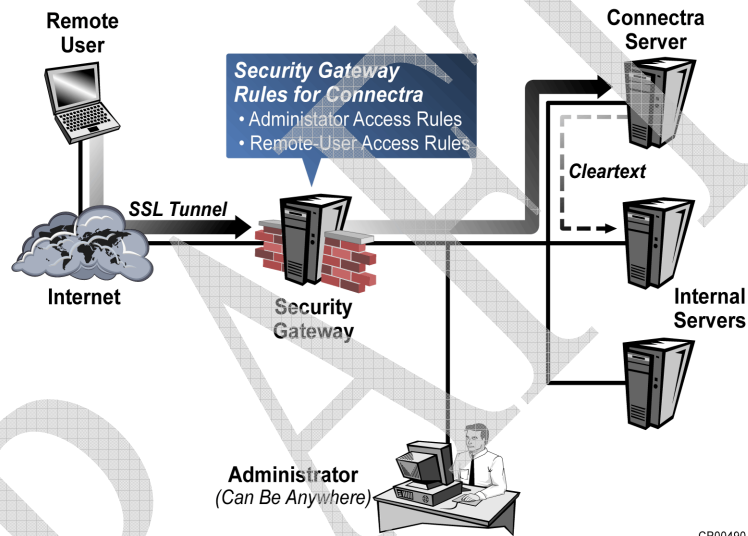
Deploying Connectra in DMZ



Internal requests from Connectra to the Web servers can also be SSL encrypted, if this is supported by the internal servers.

## Deploying Connectra in the LAN

Connectra can be deployed in the LAN alongside the internal servers, as shown in the following figure:



CP00490

### Deploying Connectra in the LAN

The remote user opens a browser and initiates an HTTPS request to the Connectra Gateway. Sessions initiated using HTTP are redirected automatically to HTTPS. The SSL connection is terminated within the LAN, and the cleartext requests are forwarded to the internal servers. The internal servers reply “in the clear” to Connectra, which encrypts the back connection to the remote user. In the scenario shown above, the perimeter Gateway must be configured to allow encrypted SSL traffic to access Connectra.

Since the SSL VPN traffic passes through the Gateway as encrypted traffic, it is unavailable for inspection by traditional solutions. Connectra provides the extra protection needed with Application Intelligence and Web Intelligence.

## DMZ vs. LAN Deployment

Although Connectra is effective handling traffic securely while residing in the internal network, Connectra adds another layer of access security to internal resources when it resides in the DMZ. If Connectra is deployed in the DMZ, all remote access to the internal network is through Connectra's IP address, and traffic is authenticated in cases where SSL Network Extender is used.

## Configuring Gateway Access Rules

Neither the DMZ nor LAN Connectra deployment is complete without properly configuring the Security Gateway's Rule Base to allow Connectra access to the LAN. During installation, the Administrator creates the Rule Base, then accesses the admin portal for network maintenance and user configuration. The exact set of rules depends on the selected setup and services that Connectra will provide. A typical Rule Base configuration for Connectra access is as follows:

### RULE BASE WHEN CONNECTRA IS IN THE DMZ

Rule	Source	Dest	Service	Action	Comment
1	Admin Host	Connectra	HTTPS (TCP/443)	Accept	Administrator access (encrypted)
2	Any	Connectra	HTTP (TCP/80) HTTPS (TCP443) SSL (TCP/444) (or port on which the SSL Network Extender server is configured)	Accept	End-user access to admin portal: <ul style="list-style-type: none"> <li>• Web applications</li> <li>• File sharing</li> <li>• Web mail</li> </ul>

Rule	Source	Dest	Service	Action	Comment
3	Connectra	LAN	HTTP (TCP/80) HTTPS (TCP/443) nbssession (TCP/139) microsoft-ds (TCP/445) nbdatagram (TCP/138) nbname (TCP/137) IMAP (TCP/143) SMTP (TCP/25) All additional network applications that are made available, via the SSL Network Extender	Accept	Connectra to LAN for: <ul style="list-style-type: none"> <li>• Web applications</li> <li>• File sharing</li> <li>• Web mail</li> </ul>
4	Any	Connectra	POP3 (TCP/110) POP3-SSL (TCP/995) SMTP (TCP/25) SMTP-SSL (TCP/465)	Accept	End-user access for native mail clients (Client settings must be defined to require secure connection, i.e., SSL.)
5	Connectra	LAN	POP3 (TCP/110) SMTP (TCP/25)	Accept	Connectra to LAN for native mail clients (unencrypted)

Other rules to take under consideration, depending on the configuration are as follows:

- Connectra may require access to DNS and/or WINS servers.
- Connectra may need access to TFTP or SCP servers for backups.
- Connectra may need access to a Customer Log Module (CLM) or other remote log server, in order to send logs.
- Connectra may need access to authentication servers, such as LDAP, RADIUS, and ACE.

#### **CONNECTRA LAN RULE BASE**

When deploying Connectra in the LAN, rules 3 and 5 are not necessary.

DRAFT