

SSL Network Extender Frequently Asked Questions

1. What is SSL Network Extender?

SSL Network Extender™ delivers SSL VPN remote access via the Web for VPN-1 and UTM-1 gateways so that employees and partners can easily access enterprise resources. It delivers spyware disablement, ensures session confidentiality, and enforces network access policy. As an integrated component of VPN-1 and UTM-1, SSL Network Extender provides a secure, highly manageable, and cost-effective remote access solution.

- **Network-level connectivity over SSL VPN**
Reduces remote access costs and simplifies deployment
- **Support for all IP-based applications**
Supports an extensive range of enterprise applications
- **IPSec and SSL VPN deployment flexibility**
Eliminates the need to deploy separate solutions for both IPSec and SSL VPN
- **Integrated endpoint security**
Stops identity, password, and data theft on remote endpoints

2. How does SSL Network Extender deliver SSL VPN access on VPN-1 and UTM-1?

SSL Network Extender is a Web browser plug-in that enables the tunneling of network applications over SSL. It provides full network level connectivity over SSL VPN. This includes remote access for all IP-based applications (TCP, UDP, and ICMP). It also supports Office Mode (similar to Check Point SecureClient™) by giving users individual internal IP addresses as well as passing DNS and WINS information so that users can enter host addresses inside their network. In addition, SSL Network Extender supports static Office Mode IP and IP from DHCP or Radius. Network Mode requires a user to have administrator privileges for a one-time install, but is also available as an MSI package. SSL Network Extender is also available with Connectra™.

3. What is the difference between SSL Network Extender Application Mode (AM) and SSL Network Extender Network Mode (NM)

SSL Network Extender utilizes two different technologies utilizes two different technologies called **SSL Network Extender Application Mode (AM)** and **SSL Network Extender Network Mode (NM)** which are both automatically downloaded via an on-demand ActiveX component or Java applet.

SSL Network Extender AM provides access to corporate resources through most TCP/IP applications, including non-Web applications and does not require administrator privileges.

Unlike SSL Network Extender NM, SSL Network Extender AM works directly with the application itself to tunnel application traffic. This solution avoids the operational disadvantages of common port forwarder, which examines the packet header and forwards it after rewriting the header. In addition, SSL Network Extender AM is non-intrusive, and therefore does not need to rewrite host files, an action that requires admin rights or configure an application to point to local addresses that are the impediments of port-forwarding technology.

SSL Network Extender NM is used when users have administrator privileges on the client machines. In addition, SSL Network Extender NM enables administrators to specifically assign private IP addresses for SSL Network Extender connections as well as pass internal DNS and WINS information. SSL Network Extender NM enables remote access to native applications such as FTP, Telnet, and terminal services. Virtually any IP-based protocol can be tunneled through SSL Network Extender NM.

4. What is the difference between SSL Network Extender for VPN-1/UTM-1 and Connectra?

Connectra includes SSL Network Extender but also adds the Connectra Web Portal. In Connectra, users log on to the Connectra Web Portal for native Web-based access and can then use SSL Network Extender. In addition, SSL Network Extender in Connectra offers Integrity Secure Workspace (ISW), SSL Network Extender Application Mode, and On-Demand application delivery.

In VPN-1 and UTM-1, users navigate to the VPN-1 or UTM-1 gateway with their browsers, which gives them access to SSL Network Extender. In addition, SSL Network Extender in VPN-1/UTM-1 includes Integrity Secure Browser (ISB). Connectra, VPN-1, and UTM-1 all have integrated endpoint security as well as Web Intelligence™ and Application Intelligence™ inspections for application security.

5. What browsers and platforms support SSL Network Extender?

SSL Network Extender is supported on Windows 2000, XP, Vista, Linux, and Mac OS X 10.4 (Power PC and Intel-based) is also supported on Check Point NGX R65. Supported browsers include Internet Explorer 5.0+, Firefox, and Safari.

6. VPN-1 or UTM-1 is used as a client for IPSec VPN. Is this the same client used for SSL VPN as well?

No, for SSL VPN, the Web browser SSL VPN capabilities are used, the IPSec VPN client is not necessary.

7. How is SSL Network Extender licensed?

As a licensed add-on to VPN-1 or UTM-1 installations, SSL Network Extender requires a license based on total users. Users are counted by the number of configured remote access users.

8. How many users are supported on VPN-1 and UTM-1?

SSL Network Extender can be added to multiple enforcement points in an organization. Each enforcement point can accept up to 1,000 concurrent users, depending on the processing capacity of the VPN-1 or UTM-1 enforcement point used. Cluster support for SSL Network Extender requires VPN-1 NGX.