# Remote Public Access Connectivity Information

January 2022
Financial Services Division

# TABLE OF CONTENTS


1. **Overview of Connectivity Options** 3
   - **Option #1 – SSL-Enabled TN3270**
   - **Option #2 – Business-to-Business Virtual Private Network (VPN)**
2. **SSL-Enabled TN3270 Specifications** 5
3. **Business-to-Business Virtual Private Network (VPN) Specifications** 6
4. **Glossary of Acronyms & Definitions** 10

## 1. Overview of Connectivity Options

The North Carolina Administrative Office of the Courts (AOC) has two options for the public to access the enterprise server. This document provides an overview of these options. Also, *estimated* costs have been provided where it is realistic to do so. Actual costs may vary. The AOC only allow IP addresses within the United States to access RPA data.

### OPTION #1 – SSL-Enabled TN3270

This option is designed to provide a connection for individual workstations using an SSL-enabled TN3270 (terminal emulation) client over the Internet. It is a standards-based solution that utilizes various protocols for authentication and encryption. This option may be the most affordable choice for small businesses and individuals.

**Basic Customer Requirements**:

- An Internet connection
- SSL-enabled TN3270 client software that supports **transport layer security (TLS) 1.2 or higher** with 128-bit encryption installed on each workstation requiring access

NOTE: Many vendors sell SSL-enabled TN3270 client software. The approximate cost is $50 to $300 per workstation. The cost depends on which vendor you select and how many licenses you need. To find a vendor, you can google “TN3270 Emulation Software.” Many vendors also offer free 30-day trials.

### OPTION #2 – Business-to-Business Virtual Private Network (VPN)

This option is designed for business-to-business (or site-to-site) VPN connections and is not intended to provide connections for individual workstations. It provides a secure method for customers to access the AOC enterprise server over the Internet. It is a standards-based solution that utilizes various protocols for authentication and encryption. It allows a secure “tunnel” from the Remote Public Access customer’s network to the AOC’s network. This option may be the most affordable choice for medium to large businesses.

**Basic Customer Requirements**:

- An Internet connection
- A VPN-capable device
- SSL-enabled TN3270 client software that supports **transport layer security**

- **(TLS) 1.2 or higher** with 128-bit encryption installed on each workstation requiring access

**NOTE:** VPN connectivity could be free of hardware/software costs if a customer already has a VPN-capable device. Estimated costs are not provided for this option due to the wide range of hardware and software configurations available.

***The AOC does not provide installation, support services, or technical consulting for public access customers. The AOC will provide the minimum technical reference information required for successful connectivity. Customers without sufficient technical resources are encouraged to obtain the assistance of a vendor or consulting company.***

## 2. SSL-Enabled TN3270 Specifications

**Background:**

The AOC provides the public with access to its enterprise server via an SSL-enabled TN3270 service. "SSL" is short for "Secure Sockets Layer." It is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. It employs various protocols and algorithms to provide a high level of security. This protocol has been approved by the Internet Engineering Task Force (IETF) as a standard.

**Requirements:**

- Customers must have their own Internet connection. There are numerous Internet Service Providers through which to obtain this connection. Prices will vary.

- Customers must purchase an SSL-enabled TN3270 client for each workstation requiring access. Many vendors sell these clients at a relatively low cost ($50 to $300).

**Configuration Specifications:**

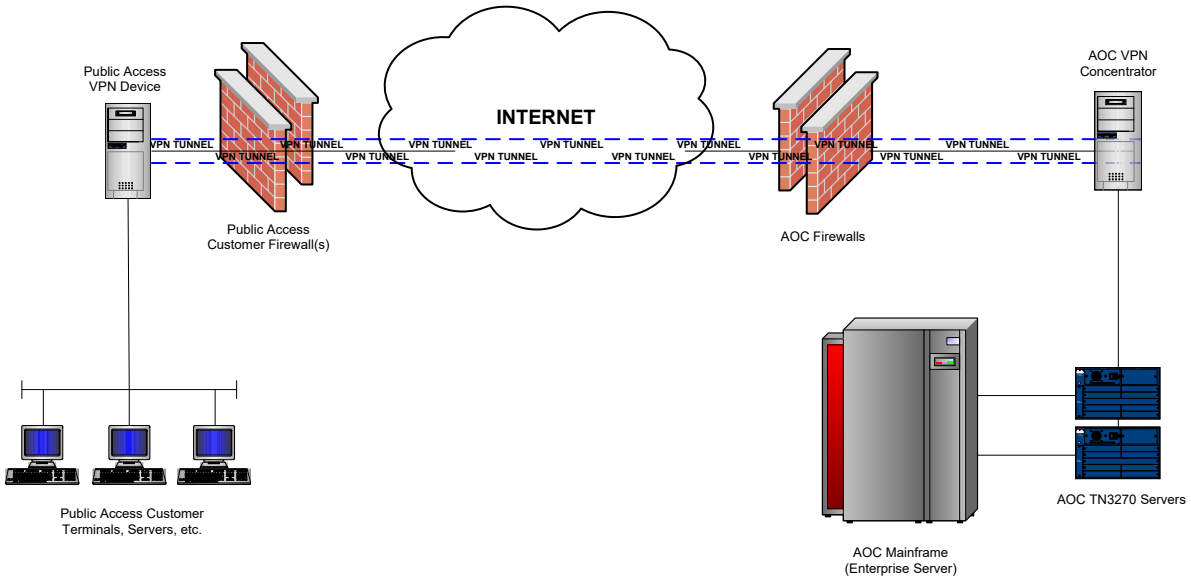
- The **Host Name** should be set to **ssl3270.nccourts.org**.
- The **TCP port number** should be set to **2023**.
- The TN3270 client must support **128-bit encryption**.

## 3. Business-to-Business VPN Specifications

**Background:**

This section gives an overview of the technology and architecture that the AOC has put into place to support VPN connectivity to the AOC enterprise server over the Internet. The VPN technology creates an encrypted tunnel between a VPN device at the Remote Public Access customer's facility and the VPN concentrators implemented at the AOC facility. Data that travels through the tunnel will be encrypted, thus protecting it from being read or manipulated.

Any VPN architecture comprises two VPN termination points with a network or group of networks in between. The AOC will provide one of the VPN termination points, and the Remote Public Access customer will provide the other. The Internet will be the network that ties the two VPN termination points together. See drawing below:




AOC Public Access VPN Overiew Diagram

The AOC currently supports only network-to-network VPN connections. Client-based VPN software will not work with this particular implementation of VPN services.

**Requirements:**

- An Internet connection
- A VPN capable device- Hardware and software compatible with the VPN system installed at the AOC. In order to connect to the AOC VPN service, the Remote Public Access customer's VPN configuration must support the technologies listed below with complete adherence to the RFC (Request for Comments) documented standards (www.ietf.org/rfc.html).
- TN3270 client software

**Configuration Specifications:**

- The **Host Name** should be set to **rpavpn3270.nccourts.org.**
- The **TCP port number** should be set to **23**.
- The TN3270 client must support **128-bit encryption**.
- Protocol IKEv2
- Encryption AES 256 or higher
- Hash SHA-256 or higher
- DH-group = 14, 19, 20, 21 (19 is preferred AOC Standard)
- PRF Hash AES256 or higher
- PFS On
- Timeout 480 minutes (8 hours)

For a general description of VPN's, the customer may wish to review the document entitled **"VPN Technologies: Definitions and Requirements,"** published by the VPN Consortium, March 2006:

http://www.vpnc.org/vpn-technologies.html

For a more thorough description of IPSec and associated protocols, the customer may wish to review the following documents:

- RFC 2409: The Internet Key Exchange (IKE)
  ftp://ftp.isi.edu/in-notes/rfc2409.txt
- RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
  ftp://ftp.isi.edu/in-notes/rfc2408.txt
- RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
  ftp://ftp.isi.edu/in-notes/rfc2407.txt
- RFC 2406: IP Encapsulating Security Payload (ESP)
  ftp://ftp.isi.edu/in-notes/rfc2406.txt

- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
  ftp://ftp.isi.edu/in-notes/rfc2404.txt

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
  ftp://ftp.isi.edu/in-notes/rfc2403.txt

- RFC 2402: IP Authentication Header
  ftp://ftp.isi.edu/in-notes/rfc2402.txt

- RFC 2401: Security Architecture for the Internet Protocol
  ftp://ftp.isi.edu/in-notes/rfc2401.txt

IPSec is an open standards technology. Many different products support and utilize IPSec protocols to create and support VPN connections. The AOC has decided to use the above products based on their adherence to IPSec standards. The product choice of the Remote Public Access customer should be based on the product's adherence to the IPSec standards and the product's known ability to function with the Cisco ASA-5500. Following is a link to Cisco's website where documentation can be found on the product and its capabilities: http://www.cisco.com/en/US/products/ps6120/index.html.
Not all VPN products will work with the specific implementation at the AOC. The customer should review all pertinent documentation to ensure compatibility with the AOC's VPN implementation.

**Other Considerations:**

1. Firewall Technologies

   A firewall on the customer's network is recommended. The AOC currently has firewall devices installed at the Internet portal to protect the AOC from potential network attacks. Please be aware that a VPN connection does not protect an Internet connection from potential network attacks. The VPN connection protects only the data that will be flowing between the AOC and the Remote Public Access customer's network. All connectivity to and from the customer's network is the responsibility of the customer.

2. IP (Internet Protocol) Routing Considerations

   A static IP address is required. In order to effectively support the VPN technology, some consideration must be given to IP Routing across the Internet as well as within the AOC and the Remote Public Access customer's private networks. The following guidelines shall be followed in order to effectively support VPN technologies across the Internet:

   - Any device that communicates on the Internet must utilize a valid Internet address.

   - The IP addresses for the VPN termination points must be static. The VPN tunnel is established based on the source and destination IP address. This information must not change.

- The source IP address of the device (i.e., workstation) performing the access must use a valid Internet-routable IP address. This requirement can be accomplished by using valid IP addresses on all workstations or by utilizing Network Address Translation (NAT) technologies. If NAT technologies are used, the packets must be translated before they are encapsulated in the VPN tunnel.

3. Internet Bandwidth

The Remote Public Access customer's available Internet bandwidth must be capable of supporting the application running across it. VPN technologies may add approximately 30% to the bandwidth requirements of an Internet application.

# 4. Glossary of Acronyms & Definitions

**DES (and 3DES)**
Short for "Data Encryption Standard," a popular symmetric-key encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X.3.92. DES uses a 56-bit key and uses the block cipher method, which breaks text into 64-bit blocks and then encrypts them.

3DES is a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with the second key, and the resulting cipher text is again encrypted with a third key).

**ESP**
Short for "Encapsulating Security Payload," the ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header (AH), or in a nested fashion. The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality.

**IETF**
The Internet Engineering Task Force (IETF) is a large, open international community of network designers, operators, vendors, and researchers whose purpose is to coordinate the operation, management, and evolution of the Internet and to resolve short- and mid-range protocol and architectural issues. It is a major source of proposals for protocol standards, which are submitted to the Internet Architecture Board (IAB) for final approval. The IETF meets three times a year, and extensive minutes are included in the IETF Proceedings.

**IKE**
The Internet Key Exchange (IKE) protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IPSec can, however, be configured without IKE.

**Internet**
A worldwide network of computer networks. It is an interconnection of large and small networks around the globe. The Internet began in 1962 as a resilient computer network for the US military and over time has grown into a global communication tool of more than 12,000 computer networks that share a common addressing scheme.

**Internet Service Provider (ISP)**
A business or organization that offers users access to the Internet and related services. Most telecommunications operators are ISPs. They provide services such as Internet transit, domain name registration and hosting, dial-up access, and leased line access.

**IPSec**
Short for "IP Security," a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

**NAT (Network Address Translation)**
An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

**PFS (Perfect Forward Secrecy)**
A key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For perfect forward secrecy (PFS) to exist, the key used to protect transmission of data must not be used to derive any additional keys.

**RFC**
Short for "Request for Comments," a series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

**SSL**
Short for "Secure Sockets Layer," a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message.

**TN3270**
TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.

**VPN**
Short for "Virtual Private Network," a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable a user to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.