



## Compliance Component

### DEFINITION

<i>Name</i>	Virtual Private Networks (VPNs)
<i>Description</i>	<p>Virtual Private Networks (VPNs) are combinations of software and hardware that allow Site-to-Site or Remote Access secure communications over public or unsecured mediums, such as the Internet, to establish a secure private connection with the agency network.</p> <p>A Site-to-Site VPN uses dedicated equipment and strong encryption to secure point to point communications over a public network.</p> <p>Remote Access VPN is a user-to-LAN connection by employees or mobile users who need to securely connect to the agency network from various remote locations. This can be via a regular telephone line, DSL or cable modem which is also commonly called broadband.</p>
<i>Rationale</i>	Virtual Private Networks (VPNs) provide a low-cost alternative to building a private network for Site-to-Site or Remote Access communication. Agencies can cost-effectively extend the agency network to locations that may not have been cost-justified before because they operate across a shared infrastructure rather than a private network.
<i>Benefits</i>	<ul style="list-style-type: none"> <li>• Provide opportunities for increased productivity of mobile employees, telecommuters, business partners and remote sites by allowing access to agency resources</li> <li>• Provide confidentiality and integrity of the data in transport through the public connection</li> <li>• May reduce cost of remote access</li> <li>• Allow traffic to be aggregated into a single connection rather than having multiple independent circuits terminating at the agency access point</li> <li>• May provide bandwidth savings</li> </ul> <p>NOTE: Can pose a high security risk if improperly configured</p>

### ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Technical Controls
<i>List the Technology Area Name</i>	Remote Access Controls
<i>List Product Component Name</i>	

## COMPLIANCE COMPONENT TYPE

*Document the  
Compliance  
Component Type*

Guideline

*Component Sub-type*

## COMPLIANCE DETAIL

*State the Guideline, Standard  
or Legislation*

- VPNs must meet the Cryptography for VPNs CC requirements
  - VPNs must meet applicable requirements in the Securing Remote Computers and Connections CC
  - VPNs must be a subnet of the agency network to allow for manageability, summarization, scalability, and performance of a session
  - Agencies should avoid the application of NAT to VPN traffic unless it is absolutely necessary to provide access
  - An anomaly-identifying software or hardware (IDS) should be in place inside the point in the agency network where VPN traffic is decrypted (see the Network Based IDS CC)
  - Site-to-Site VPNs:
    - Must originate from a static IP, and
    - Must authenticate the tunnel with a:
      - pre-shared key, or
      - certificate;
    - Must utilize Access Control Lists (ACLs) on the VPN device to limit what resources can be accessed by a business partner
    - Must not allow split-tunneling unless an agency-controlled firewall is properly positioned between the agency network and any non-agency or public network (see the Firewall Environments CC)
- NOTE: Split tunneling occurs when concurrent access is allowed to resources on the agency network and a non-agency or public network via the VPN
- Remote Access VPNs:
    - Must authenticate the tunnel with a:
      - pre-shared group name and key, or
      - certificate, and
    - Must authenticate the user with strong authentication (see the Strong Authentication CC), and
    - Must not allow split tunneling (**only one network connection is allowed**), and
    - Should utilize Access Control Lists (ACLs) to limit what resources can be accessed by a remote client (see Access Control Lists CC), and

	<ul style="list-style-type: none"> <li>Must have properly configured personal firewalls (see the Personal Firewall CC)</li> </ul> <p>NOTE: Some VPN clients include a built-in stateful firewall</p>		
<i>Document Source Reference #</i>	NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications; NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems; NIST Special Publication 800-77, Guide to IPsec VPNs		
<b>Standard Organization</b>			
<i>Name</i>	NIST	<i>Website</i>	www.csrc.nist.gov
<i>Contact Information</i>			
<b>Government Body</b>			
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
<b>KEYWORDS</b>			
<i>List all Keywords</i>	Broadband, Cable, DSL, Wireless, Broadband over Power Line (BPL), Power Line Communications (PLC), Satellite, Modem, Internet, Dial-Up, telecommute, mobile, roadwarrior, remote, IPsec, tunnel, site-to-site, site-to-client, Virtual Private Dial-up Network, VPDN		
<b>COMPONENT CLASSIFICATION</b>			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
<b>Rationale for Component Classification</b>			
<i>Document the Rationale for Component Classification</i>			
<b>Conditional Use Restrictions</b>			
<i>Document the Conditional Use Restrictions</i>			
<b>Migration Strategy</b>			
<i>Document the Migration Strategy</i>			
<b>Impact Position Statement</b>			
<i>Document the Position Statement on Impact</i>			
<b>CURRENT STATUS</b>			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>		
<b>AUDIT TRAIL</b>			
<i>Creation Date</i>	02/23/2006	<i>Date Accepted / Rejected</i>	03/14/2006
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			