Global Information Assurance Certification Paper

Steven Abate
GSEC Version 1.1

Choosing and Implementing a Cisco Soft Virtual Private Network (VPN) Client or Cisco Hard VPN Client:

Abstract:

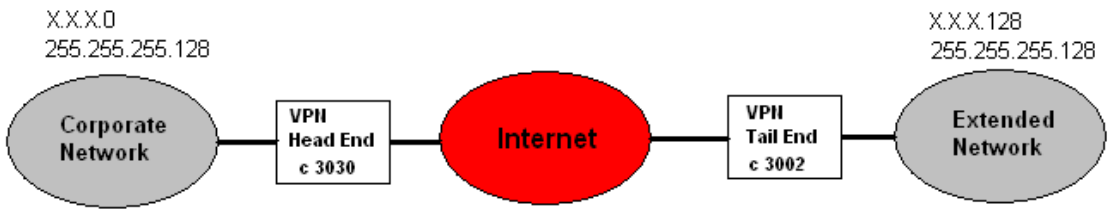
In a very large organization where employees travel, choose to work at home, or work in small groups off campus, the decision must be made on how to securely connect the users to the corporate environment. In today's market there will be many options, from T1s, DSL, ISDN and Cable Modem. T1s can be costly and may not be available to all homes. DSL and ISDN can reach most homes and businesses at a reasonable cost and reasonable speeds. Cable Modem (Broadband) on the other hand also reaches most everywhere from Starbucks WYFI (802.11) to most all local businesses and many remote areas where none of the other options exist. Given that you will take a small speed hit when using VPN technology and the relatively low cost and availability of Broadband, it would appear that Broadband would be best for the bandwidth needs. For the traveler and home users, the VPN of choice would be the soft client. Single-user connection, special VPN configuration and login process would be within tolerance for the user. In a small group off campus, say 15 end nodes, it would not be tolerable to have each user connect on their own. In this situation a hard client would work the best. There would be one connection to create an extended corporate network and nothing special for the user to do or know.

Hard Client Network:

The Hard Client Network may be a medium size workgroup of around 25 devices with a variety of operating systems and application needs. These may include standard desktop function to X11 with protocols like NetBEUI.

With the Hard Client you have a choice of two configurations: The Extended Network and Port Address Translation (PAT)

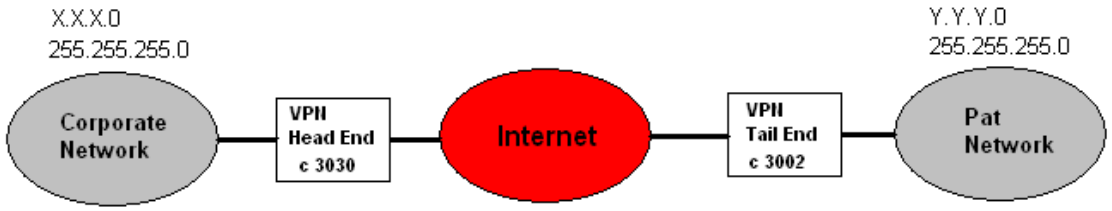
Extended Network



With the Hard Client, you are able to take advantage of the extended corporate network option, which has its pros and cons. The devices that are locally connected to the Hard Client appear to the corporate network as if they were in house. This can be an advantage because with the extended network you would be able to route packets directly to the Internet Protocol (IP) address of the device, which would allow protocols like X11 to connect back to the device and allow remote mounting of drives using NetBios Enhanced User Interface (NetBEUI). When remotely mounting drives, be sure to use strong password protection to reduce the risk of unwanted access to the drives. In this mode, the end nodes would also be vulnerable to attack from the inside. These devices must than follow the security policy of all the other corporate devices. This may include having a personal firewall on each corporate device.

When using the extended network mode, IP addressing can also become an issue. In a large organization there may be more than one access point to the Internet and each access point may use a separate IP address space. For example, the East coast access point would use IP address space X, and the West coast access point would use IP address space Y. To use the East coast IP address space on the Hard Client (Cisco 3002) you must also be sure its Head End VPN concentrator is in the East coast address space. This configuration will work well with asymmetrical providing you do not have a statefull firewall at the inbound access points. If you have statefull firewall at the inbound access points the packets leaving the East coast access point must have the established bit set in order to be allowed back in by the statefull firewall. If the packet were allowed to leave the East coast node and be routed back to the West coast node (asymmetrical routing), the established bit would not be set. If the established bit were not set than the statefull firewall would stop the packet. To protect a network that uses asymmetrical routing is outside the scope of this paper.

Port Address Translation (PAT)



Configuring the Hard Client (Cisco 3002) to use Network Address Translation (NAT) provides PAT on a single global IP address. This means the external network could not see the internal network address space. All the internal network addresses are translated to the selected external address and then passed on to the external network. NAT will also function as a type of firewall, by only allowing established connections from the internal side of the network to

communicate with these NATed devices. NAT also allows the use of very large unrestricted address space for the corporation internal network.

If you were to enable Dynamic Host Configuration Protocol (DHCP) on the Hard Client (Cisco 3002), then anyone who would have physical access to any connection point would be able to plug in and connect to the corporate network. With this configuration there would be a need for a higher level of physical security at the site and it would be good to do some DHCP hardening.

DHCP hardening can be as simple as checking the Media Access Control (MAC) address of the requesting end node against a list of known addresses. Another method may be to disable all unused ports in the switch. These two options are not mutually exclusive. They are normally done together. These measures would help eliminate the threat of any device easily connecting to your network but do not eliminate the possibility of spoofing.

To use spoofing to connect to the network the hacker must first have tools and a bit of prior information. Some of the tools would include:

- Network card - which allows the MAC address to be changed
- Software - which would be able to change the MAC address
- Prior knowledge of the allowable MAC addresses which could be obtained through sniffing on the network or an inside source

Here is a brief overview on configuring a Cisco 3030 and Cisco 3002
The 3030

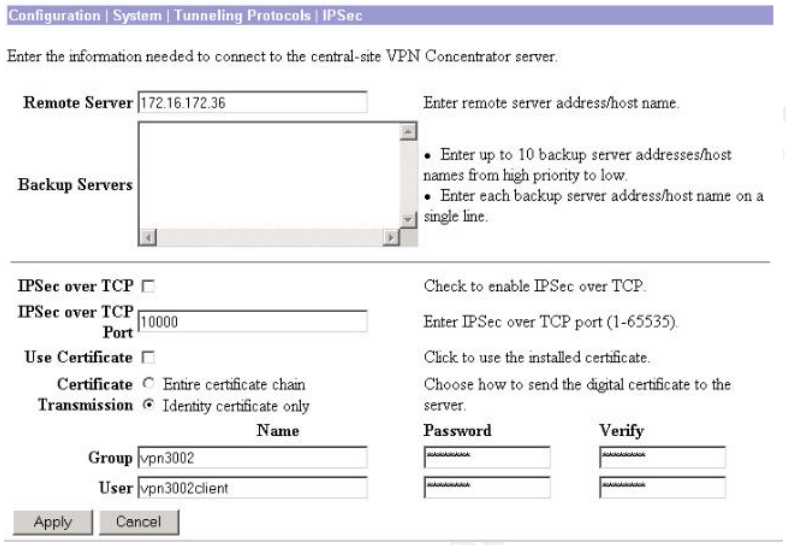
- Under the Identity tab
  - Create a unique group and password
  - To have group validation on the 3030 be sure to select Type=internal
- Under the General tab
  - Enter the max number of Simultaneous Logins
  - Minimum password length
  - DNS address
  - IPSec as the Tunneling Protocol
- Under the IPSec tab
  - Select the group's IPSec Security Association
  - Authentication will be Internal
- Under the Mod Config tab
  - Split Tunneling Policy is set to Tunnel everything
  - Default Domain Name
  - IPSec over UDP Port 10000
- Under HW Client
  - For added security Require Individual User Authentication should be checked
  - User idle Timeout set to 30

Configuring Users on the 3030

- Under the Identity tab
  - User Name and Password
  - Group that the user belongs to
  - If you had selected Require Individual User Authentication you would enter another user and group the same as above

The 3002

- There are no configurations required for the Cisco VPN 3002 Hardware Client. The following screen shot is from the VPN section.

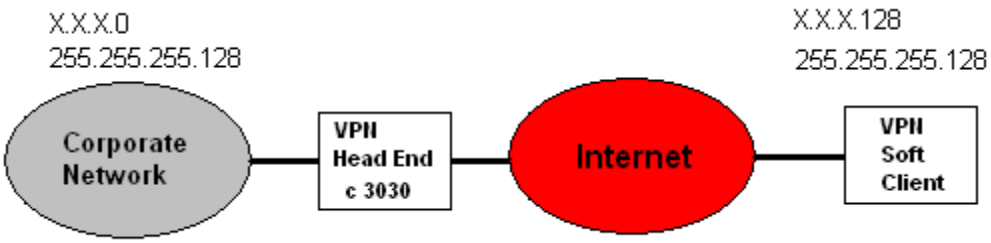


Cisco Systems **"**How to Configure Individual User Authentication for VPN 3002 Hardware Client"
URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_configuration_example09186a0080094297.shtml (Dec 07, 2001)

For step-by-step instructions in configuring a Cisco 3030 and Cisco 3002 go to the above URL.

Soft Client Network:

The Soft Client Network would be a single device with an operating system and application needs. These may include standard desktop function to X11 and protocols like NetBEUI.



To install the VPN Client requires you uninstall any previous version and install the newer version. This is a normal Windows application install. The file downloads as an executable. All you need to do is double click on the file and follow the onscreen help.

For step-by-step instructions to install the VPN client use the following URL:

Cisco Systems "Installing the VPN Client"
URL:http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide09186a00800bd982.html

The Soft Client is much easer and has fewer options to configure than the Hard Client. Cisco has created a very useful wizard, which takes you through all the steps of the configuration. In the Soft Client network the client would be installed on each end node. This would require either each user or your support department to do a complete install.

The installer must know these things:

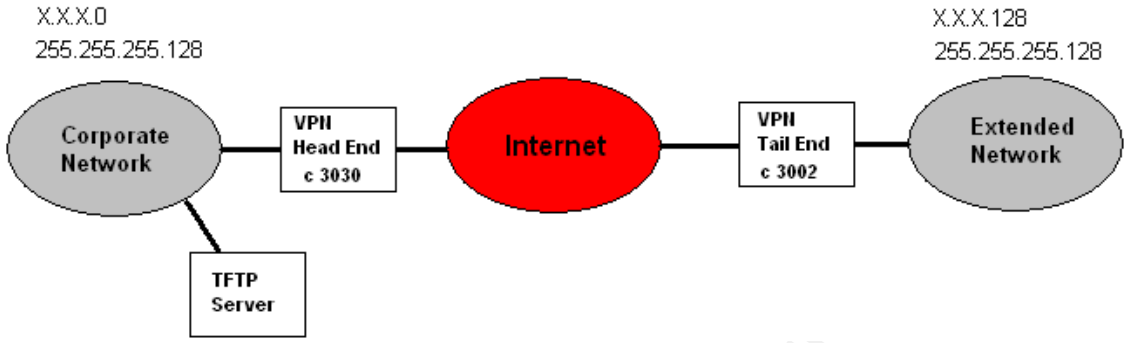
- IP address of the host
- Group name
- Group password
- Personal user name
- Personal password
- Token user name and password if used
- Smart Card user name and password if used
- How to connect device to the Internet. These connections would include DSL, ISDN, Broadband or other organization's LAN.

For step-by-step instructions to configure the VPN client use the following URL:

Cisco Systems "Configuring the VPN Client"
URL:http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_6/user_gd/vc3.htm (Apr 11 2003)

Updating Clients:

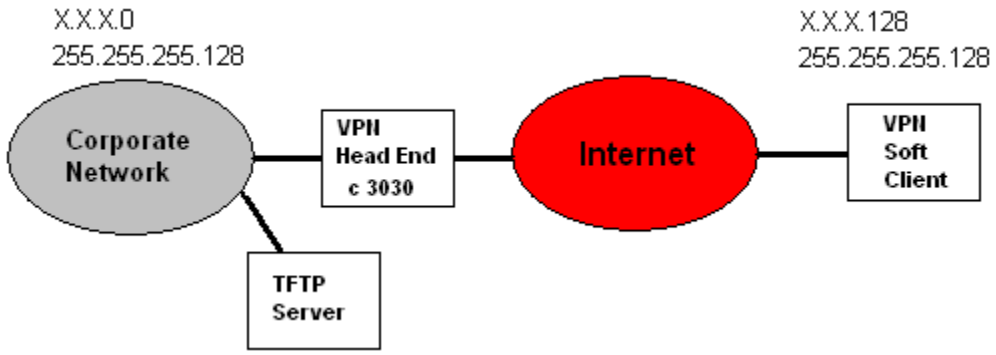
Hard Client:



Cisco Systems **"**Upgrading the VPN 3002 Hardware Client from a VPN 3000 Series Concentrator"
URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_example09186a0080094292.shtml (Sep 03, 2002)

With all systems you have to update the IOS/OS when security patches are released or new features you desire are added. There are often two choices. One would be going to the site and installing it manually and the other would be to push the update out to the remote end from the head end. By adding a Trivial File Transfer Protocol (TFTP) server you only need to make one change to the Head End and all remote ends will receive the update on its next connection. To add another level of security, Cisco created this push method so that the TFTP data stream is sent through the encrypted tunnel. This does force the TFTP server to be on the same network as the concentrator's private interface to enable the encryption to occur. It would be there in most cases anyway.

Soft Client:



To update this client the same process as the Hard Client can be used. When there is a new update to be pushed, the Head End will notify the Soft Client. The Client will then pull down the new upgrade from the TFTP server and install it.

The Secure Connection Process:

The VPN Client works with a Cisco VPN server to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:

- Agreeing on tunnel parameters
- Creating the tunnels according to the agreed upon parameters
- Authenticating users on a Terminal Access Controller Access Control System (TACACS) or Remote Authentication Dial-In User Service (RADIUS) server
- Establishing user access rights from authenticating server
- Encryption and decryption management

Negotiating tunnel parameters:

IKE is a hybrid protocol, which implements Oakley and Skeme key exchanges inside the The Internet Security Association and Key Management Protocol (ISAKMP) framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides automatic authentication of the IPSec peers, negotiates IPSec keys, and security associations.

Some benefits of IKE are:

- Specifies a lifetime for the IPSec security association
- Changes encryption keys during IPSec sessions
- Allows IPSec to provide anti-replay services
- Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation
- Allows dynamic authentication of peers

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

ISAKMP is a protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

Authenticating users:

User authentication is done through a Point-to-Point Tunneling Protocol (PPTP) connection using Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), Challenge-Handshake Authentication Protocol (CHAP), Shiva Password Authentication Protocol (SPAP) or Password Authentication Protocol (PAP). Encryption is accomplished through the use of L2TP over IPSec using Data Encryption Standard (DES) and 3DES.

Key Layer 2 Transfer Protocol (L2TP) Terms

CHAP: Challenge Handshake Authentication Protocol. A Point-to-Point Protocol (PPP) authentication protocol.
L2TP Access Concentrator (LAC): An LAC can be a Cisco network access server connected to the public switched telephone network (PSTN). The LAC need only implement media for operation over L2TP. An LAC can connect to the LNS using a local-area network or wide-area network such as public or private Frame Relay. The LAC is the initiator of incoming calls and the receiver of outgoing calls.

L2TP Network Server (LNS): Most any Cisco router connected to a local-area network or wide-area network, such as public or private Frame Relay, can act as an LNS. It is the server side of the L2TP protocol and must operate on any platform that terminates PPP sessions. The LNS is the initiator of outgoing calls and the receiver of incoming calls. Figure 1 depicts the call routine between the LAC and LNS.
Virtual Private Dial Network (VPDN): A type of access VPN that uses PPP to deliver the service.

Cisco Systems **"**Layer 2 Tunnel Protocol"
URL:http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm (Jul 15 2002)

RADIUS and TACACS:

RADIUS and TACACS protocols work well for authenticating users and follow the Rfc2511 and X.509v3 standards.

The Remote Authentication Dial In User Services (RADIUS) protocol is a software-based security authentication protocol developed by the Internet Engineering Task Force (IETF) RADIUS Working Group. Its main functions are Authentication, Authorization, Configuration and Accounting.

The Terminal Access Controller Access Control System (TACACS) is a security protocol that communicates between network devices and an authentication

database. Cisco Systems wrote the TACACS protocol. Cisco has more than one option for TACACS deployment:

- TACACS supports authentication
- TACACS+ is an enhancement to the TACACS security protocol
- XTACACS (Extended TACACS) supports authentication, authorization, and accounting.

Cisco Secure supports both RADIUS and TACACS authentication with a strong password policy, which includes but is not limited to the following:

- 6 to 8 characters in length
- Does not contain your user name, real name, or company name
- Does not contain a complete dictionary word
- Must contain at least one character from each of the following groups
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols
- Change password every 30 days
- Don't use the same password you used last time
- Don't post passwords on monitor

Hardening Authentication:

For corporations where simple username/password authentication is not enough there are other devices that can be used to strengthen the authentication of the user that follow the ISO standard 7810 "Identification Cards – Physical Characteristics". The Smart Card and Microprocessor Card are two such devices, which generate a new unique one-time password for each authentication attempt.

A smart card is the size of a credit card with an onboard microprocessor chip. Smart card chips come in two varieties:

- Memory-only chips – With storage space for data, and built-in security
- Programmable/updateable - This chip has more memory and has an operating system with the ability to process data onboard.

Microprocessor Cards typically have

- 8-bit onboard processor
- OS, 512 bytes of random-access memory (RAM)
- 16KB read-only memory (ROM)

This card has about the same processing power as the original IBM-XT computer with less memory.

Firewall:

Even with VPN you must consider a firewall. A VPN and Firewall can be configured in a number of ways.

A Firewall application can be placed on the same end node as the Soft Client. This has the disadvantage of the Soft Client and Firewall application sharing the compute cycles thereby reducing the processing power of the end node. Connecting in this way will protect the end node while it is connected to the Internet before the VPN client has created the encrypted tunnel. This configuration has the added advantage of being able to protect itself from any in-house attacks.

If you have a lot of end nodes in one location you may choose to use the Hard Client. You can let the corporate firewall which is placed at the corporate Internet access point protect the end nodes as it would all nodes on the local net. This arrangement would not protect the end node from any in-house attacks.

Key terms:

Client Mode (PAT)
Client mode, also called Port Address Translation (PAT) mode, isolates all devices on the VPN 3002 private network from those on the corporate network. In PAT mode:
IPSec encapsulates all traffic going from the private network of the VPN 3002 to the network(s) behind the Internet Key Exchange (IKE) peer, that is, the central-site VPN Concentrator.

PAT mode employs NAT (Network Address Translation). NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the IP address of the VPN 3002 public interface. The central-site VPN Concentrator assigns this address. NAT also keeps track of these mappings so that it can forward replies to the correct device.
All traffic from the private network appears on the network behind the central-site VPN Concentrator (the IKE peer) with a single source IP address. This IP address is the one the central-site VPN Concentrator assigns to the VPN 3002. The IP addresses of the computers on the VPN 3002 private network are hidden. You cannot ping or access a device on the VPN 3002 private network from outside of that private network, or directly from a device on the private network at the central site.

Client Mode with Split Tunneling
You always assign the VPN 3002 to a tunnel group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec and PAT are

applied to all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator.

Traffic from the VPN 3002 to any destination other than those within the network list for that group on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the assigned IP address of the public interface and also keeps track of these mappings so that it can forward replies to the correct device.
The network and addresses on the private side of the VPN 3002 are hidden, and cannot be accessed directly.

Cisco Systems "Understanding the VPN 3002 Hardware"
URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_getting_started_guide_chapter09186a008012b469.html

Conclusion:

Very large organizations need to connect their remote users to the corporate environment. To accomplish this in an effective and secure manner one could deploy a VPN technology. This may not be an easy task. Time must be spent identifying the remote workload. Then from this workload, network access controls and firewalls can be put in place. There will be user accountability policies instituted as well as standard management procedures.

The VPN network itself will need to be managed from a hardware point of view. You will need a backup set of hardware to role over to if the primary fails. Another method may be multiple VPN hosts for load sharing and use each as the other's backup.

Never lose site of testing all facets of your design before you go into production. You do not want to be chasing security holes put in place by the VPN structure.

User support works its way into all VPN implementations. This support would mostly be in the way of user installs and lost passwords.

A number of Soft Clients will be included with the purchase of the VPN head end but the Hard Client will be an extra charge per site.

Given all of these issues to be concerned with, the VPN Hard Client works the best for medium to large work groups, and the Soft Client works well for the traveler and home user.

References:

D.Piper, “The Internet IP Security Domain of Interpretation for ISAKMP”, Network Working Group, Standards Track, RFC2407, November 1998
URL:http://www.ietf.org/rfc/rfc2407.txt (November 1998)

D.Harkins, D.Carrel, “The Internet Key Exchange (IKE)”, Network Working Group, Standards Track, RFC2409, November 1998
URL:http://www.ietf.org/rfc/rfc2409.txt (November 1998)

Network Working Group “Diffie-Hellman Key Agreement Method”
URL:http://www.faqs.org/rfcs/rfc2631.html (June 1999)

Greene, Tim. “Standards work should reinforce VPNs.” Network World, Nov. 5, 2001.
URL:http://www.nwfusion.com/news/2001/1105specialfocus.html. (Nov 05 2001)

Fowler, Dennis. Virtual Private Networks: Making the Right Connection. San Francisco: Morgan Kaufmann Publishers, Inc., 1999.

Scott, Charlie, Paul Wolfe, and Mike Erwin. Virtual Private Networks (2nd Ed.). Beijing; Sebastopol: O'Reilly and Associates, Inc., 1999.

Cisco Systems “Understanding the Cisco VPN Client.” © 1992-2002
URL:http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_6/user_gd/vc1.htm (Apr 11 2003)

Network Working Group “Internet X.509 Certificate Request Message Format”
URL:http://www.ssh.com/products/security/sentinel/rfc/rfc2511.txt.html (March 1999)

SANS, Nathan Lasnoski “Creating a Secure VPN with Cisco Concentrator and ACE Radius/SecurID” June 30, 2002
URL:http://www.sans.org/rr/encryption/ACE.php (June 30, 2002)

SANS, Gregory J. Ciolek ”Virtual Private Network (VPN) Security” January 4, 2001
URL:http://www.sans.org/rr/encryption/VPN_sec.php (January 4, 2001)

Cisco Systems **“**How to Configure Individual User Authentication for VPN 3002 Hardware Client”
URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_configuration_example09186a0080094297.shtml (Dec 07, 2001)

Cisco Systems **“**Upgrading the VPN 3002 Hardware Client from a VPN 3000 Series Concentrator”

URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_example09186a0080094292.shtml (Sep 03, 2002)

Cisco Systems “Understanding the VPN 3002 Hardware”
URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_getting_started_guide_chapter09186a008012b469.html

Cisco Systems **“**Configuring Internet Key Exchange Security Protocol”
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scike.htm - xtocid40955 (Nov 20 2001)

Cisco Systems **“**Layer 2 Tunnel Protocol”
URL:http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm (Jul 15 2002)

Cisco Systems “Installing the VPN Client”
URL:http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide09186a00800bd982.html

Cisco Systems “Configuring the VPN Client”
URL:http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_6/user_gd/vc3.htm (Apr 11 2003)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event