A

anti-replay
A security service in which the receiving edge device router can reject old or duplicate packets in order to protect itself against replay attacks.

Auditor
A mechanism in VPN Solutions Center that monitors and reports the current state of a VPN service request over its lifetime. The Auditor verifies that a service request is correctly deployed or still exists on the router. The Auditor also provides the reasons why a service request is in its current state. The Auditor saves the state transition (if any) into the VPN Inventory Repository.

authentication
The process of ensuring message integrity and protection against message replays. It includes both data integrity and authenticating data origin.

Authentication Header (AH)
An IPsec protocol that provides data integrity, data origin authentication, and optional antireplay services to IP. AH does not encrypt any portion of the protected IP datagram, nor does AH provide confidentiality.

authoritative SNMP engine
One of the SNMP copies involved in network communication designated to be the allowed SNMP engine to protect against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine’s engine ID and user passwords. When an SNMP message expects a response (for example, get exact, get next, set request), the receiver of these messages is authoritative. When an SNMP message does not expect a response, the sender is authoritative.

C

community string
A text string used to authenticate messages between a management station and an SNMPv1/v2c engine.

configlet
A partial router configuration file that contains a set of Cisco IOS commands created by the VPN Solutions Center provisioning process. The IOS commands in the configlet consist only of the commands necessary for modifying the router’s current configuration to enable service request deployment. VPN Solutions Center downloads the configlet to the router, executing the commands in the configlet to change the router’s configuration. VPN Solutions Center then collects the updated version of the configuration file from the router—it is this version of the configuration file that VPNSC uses to audit service request deployment. A configlet is also referred to as a “VPNSC configlet.”

CoS profile
Represents a set of CoS configurations offered by a provider to its customer. Each CoS profile consists of a set of CoS classes that record configuration information on how traffic is shaped and policed.
CPE
Customer Premise Equipment. In this document, CPE is also referred to as a “edge device router.” A CPE is part of a customer network. A CPE can join any set of virtual private networks (VPNs). Each CPE connects a customer site to another site through the Service Provider cloud, obtaining the VPN service for that customer site, and belongs to exactly one customer. Each CPE can have many configlets and can be configured by multiple service requests.

customer site
A set of IP systems with mutual IP connectivity between them without the use of a VPN. Each customer site belongs to exactly one customer. A customer site can contain one or more (for load balancing) edge device routers.

data integrity
A condition or state of data in which a data packet has not been altered or destroyed in an unauthorized manner.

data origin authentication
The ability to verify the identity of a user on whose behalf the message is sent. This ability protects users against both message capture and replay by a different SNMP engine, and against packets received or sent to a particular user that uses an incorrect password or security level.

DES
Data Encryption Standard (DES) encrypts packet data. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit initialization vector (IV). Cipher Block Chaining (CBC) requires an initialization vector to start encryption. The IV is given in the IPsec packet.

Diffie-Hellman
A public-key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. IKE uses Diffie-Hellman to establish session keys.

DNS
Domain Naming System. In Unix-based networks, DNS is used in the Internet for translating names of network nodes into addresses.

DTD
Document Type Definition. Often used in relationship with the Extensible Markup Language (XML).

encryption
A method of hiding data from unauthorized users by scrambling the contents of an SNMP packet.

Extensible Markup Language
See XML.
G

**GRE protocol**

Generic routing encapsulation. GRE is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

**group**

A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive.

I

**IANA**

Internet Assigned Numbers Authority. An organization operated under the auspices of the ISOC as a part of the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the InterNIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP stack, including BGP autonomous system numbers.

**ICMP**

Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

**IDL**

Interface Definition Language. Generic language for describing APIs for API servers. IDL API files must be compiled using an IDL compiler from an approved CORBA vendor to produce language-specific API files in a CORBA-supported target language. Using the generated target-language files you can add API-supported features to third-party client-application source code.

**IPv4**

Internet Protocol, version 4. A version of IP that support a 32-bit address space.

**IPv6**

Internet Protocol, version 6. A version of IP that support a 128-bit address space.

K

**keepalive parameters**

A Cisco proprietary extension to IKE that detects failures in IKE negotiation. After an IKE session is established, each node sends keepalive packets to its peers. When a peer does not respond, the sending node tears down the IKE/IPsec tunnel with the non-responding peer.
L

L2TP
Layer 2 Tunneling Protocol. A means of providing secure, high-priority, temporary paths through the Internet.

lifetime parameters
Global settings. A Lifetime is associated with each security association, beyond which the SA cannot be used. There are two lifetimes: a timed lifetime, specified in terms of the duration of the SA; and a traffic-volume lifetime, specified the number of bytes secured using this SA. A security association expires after the first of these lifetimes is reached.

loopback interface
This IP address for a loopback interface is defined as the address of the software loopback interface on a switch or router. The loopback interface has no real hardware associated with it, and does not physically connect to a network. It is often used for testing purposes, but a loopback interface can be used as an IP interface on a local machine that is always up and reachable, regardless of the status of the interface hardware.

M

managed device
A device managed by the service provider who uses VPN Solutions Center software to make changes in device configurations. For managed devices, you can specify whether these devices support SA Agent and can therefore collect SLA data.

management interface
The VPN Solutions Center Network Management Subnet resides inside the service provider network, and communicates with edge device routers through an assigned management interface. Configuration changes are managed by VPN Solutions Center software and transported to the appropriate edge devices through the management interface.

MIB
Management Information Base. A database of network performance information that is stored on a network agent for access by a network management station. A MIB consists of a repository of characteristics and parameters managed in a network device such as a network interface card (NIC), hub, switch, or router.

N

network
In IPsec Solution Center software, a network is a collection of targets with unique names.

notification host
An SNMP entity to which notifications (traps and informs) are sent.

notify view
A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group.

O

OID
Object identification number. An element of an SNMP group that maps to a tree structure of MIBs.
P

privacy
An encrypted state of the contents of an SNMP packet, in which the contents cannot be disclosed on a network. The CBC-DES (DES-56) algorithm performs the encryption task.

provider network
A backbone network under the control of a service provider that provides transport services between customer sites.

PVC
Permanent Virtual Circuit. A permanent association between two network nodes. A PVC uses a fixed logical channel to maintain a permanent association. PVCs are widely used in X.25 networks, and they are the basis on which communication takes place in a Frame Relay network.

R

read view
A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group.

response time reporter
Former name of the Service Assurance Agent (SA Agent) in VPN Solutions Center software. See also SA Agent.

RIP
Routing Information Protocol. The simplest Interior Gateway Protocol (IGP) in the Internet. RIP is based on distance-vector algorithms that measure the shortest path between two nodes on a network, based on the originating and destination devices. The shortest path is determined by the number of "hops" between those points.

RTT
Round-trip time. The total time required for a packet to traverse a network to its destination and back again.

S

SA Agent
The Service Assurance Agent (SA Agent) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. With this feature you can perform troubleshooting, problem notifications, and preventive analysis based on Service Assurance Agent statistics. The SA Agent router uses the Cisco Round Trip Time Monitor (RTTMON) MIB. You can use the Service Assurance Agent feature to troubleshoot problems by checking the time delays between devices (such as between two CEs in a VPN) and the time delays on the path from the source device to the destination device at the protocol level.

secondary edge device
A device that can be brought up automatically either for loadsharing or in the event that the primary edge device goes down.

secured interface
An edge device router must have a secured (encrypted) interface and a nonsecured (unencrypted) interface associated with the device. The secured interface faces the service provider network.
Security Associations (SAs)
A description of how two communicating edge device routers will use a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. SAs determine the IPsec protocol used for securing the packets, transforms, keys, and the duration for which keys are valid. IPsec applications, such as Cisco VPN Solutions Center, builds an SA database that maintains the SAs that the IPsec protocol use to secure packets. SAs are unidirectional (simplex) and protocol specific.

security level
A type of security algorithm performed on each SNMP packet. The three levels are: noauth, auth, and priv. noauth authenticates a packet by a string match of the user name. auth authenticates a packet by using either the HMAC MD5 or SHA algorithms. priv authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.

Security Parameter Index (SPI)
A 32-bit element that, with a destination IP address and security protocol, uniquely identifies a particular security association at the destination edge device. The destination edge device uses the SPI value to index into the receiving edge device’s SA database and fetch the SA.

Simple Network Management Protocol (SNMP)
A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. SNMPv2c supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

site
In VPN Solutions Center software, a site is a component of a VPN customer. A collection of one or more edge device routers (or CPEs). For two edge routers to be connected in a VPN, they must be in two different sites. A site is defined by VPN Solution software as an attribute of a VPN customer.

SNMP engine
A copy of SNMP that can either reside on the local or remote device.

SNMP group
A collection of SNMP users that belong to a common SNMP list. The SNMP list defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of the attributes defined by the group.

SNMP view
A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

static route
A route that is explicitly configured and entered into an edge device router’s routing table. Static routes take precedence over routes chosen by dynamic routing protocols (assuming default administrative distances for the protocols).

target
A single network device (usually a router) from which information can be collected and to which data can be sent. Targets are imported into VPN Solutions Center software by importing their corresponding router configuration files.

template configuration file
An IOS configuration file that stores the Cisco IOS commands created by the Template Manager. A template configuration file can be either a partial or complete configuration file. When you generate a template configuration file using a particular data file, the template configuration filename is the same as the data file’s name.
template data file: A text file that stores variable values to generate the template file. A valid data file contains name-value pairs for all the variables defined in a template. Each template file can be associated with multiple template data files; however, note that each data file can only be associated with a single template.

template file: A file created by the Template Manager that stores a VPN Solutions Center template definition.

terminal server: A communications processor that connects asynchronous devices such as terminals, printers, hosts, and modems to a LAN or WAN. In VPN Solutions Center 2.0, terminal servers provide a way to provision edge device routers from a workstation. In the VPN Solutions Center software, you first define a target as a terminal server, and then associate that terminal server device with a particular edge device router.

transform: A transform lists a security protocol (AH or ESP) with its corresponding algorithms. For example, one transform is the AH protocol with the HMAC-MD5 authentication algorithm.

transform set: An acceptable combination of security protocols, algorithms, and other settings to apply to IPsec protected traffic. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

tunnel: In IPsec, *tunnel* denotes a pair of security associations (SAs) that create a bidirectional connection between edge device routers. In IPsec tunnels, IP is tunneled through IP to provide data security and hide the internal structure of private networks.

tunnel endpoint: A virtual—not an actual—interface that is required by IPsec to define the endpoint of an IPsec tunnel. The tunnel endpoint interface can be either a loopback interface (with the IP address in the service provider’s address space) or an interface that is not a loopback.

tunnel mode: Encrypts both the payload and the header. IPsec in Tunnel mode is normally used when the ultimate destination of a packet is different than the security termination point. This mode is also used in cases when the security is provided by a device that did not originate packets, as in the case of VPNs.

**U**

UDP: User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.

unmanaged device: A network device that can only be configured by the Customer that owns that device. If an edge device in unmanaged, VPN Solutions Center is not responsible for configuring that device.

user model: The ability to authenticate a user at the point of system access by means of a user identity and password. Also refers to the ability to a) control users’ access to particular data, b) control users’ function on that data, and c) provide an audit trail of changes, which is linked to the user identity.

**V**

VCI: Virtual Channel Identifier. An ATM term that designates the address or label of a virtual channel (VC). The VCI is a unique numerical tag, defined by a 16-bit field in the ATM cell header. This number identifies a VC over which a stream of cells travels during the session between two devices.
| **VCL** | Virtual Channel Link. An ATM term that refers to unidirectional transport of ATM cells between the point where a VCI value is assigned and the point where that value is translated or removed as it exits the ATM network. |
| **VLAN** | Virtual LAN. A group of devices on a LAN that are configured so they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. |
| **VoIP** | Voice over IP protocol. |
| **VPN** | Virtual Private Network. A framework that provides private IP networking over a public infrastructure such as the Internet. In IPsec VPN Solution, a VPN is a set of customer sites that are configured to communicate through a VPN service. A VPN is a network in which two sites can communicate over the provider’s network in a private manner; that is, no one outside the VPN can intercept their packets or inject new packets. There is a physical connection from the provider edge network to the customer edge network. A VPN is a private network constructed within a public network infrastructure, such as the Internet. A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this communications medium provides services to the network on a nonexclusive basis. |

| **W** | A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group. |

| **X** | eXtensible Markup Language. A pared-down version of SGML, designed especially for Web documents. SML enables designers to create their own customized tags to provide functionality not available with HTML. |