Learning About the WSG

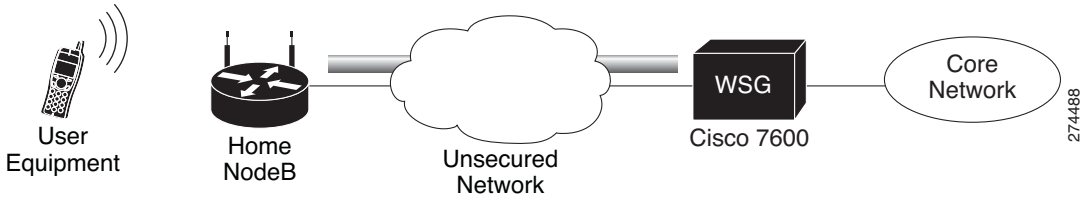
The following sections describe the WSG and Cisco Service and Application Module for IP (SAMI).

WSG Overview

The WSG is a high-density IP Security (IPSec) gateway for mobile wireless carrier networks. IPSec is an open standards set. IPSec provides confidentiality, integrity, and authentication for data between IP layer peers. The WSG uses an IPSec-protected tunnel to connect outside endpoints.

Figure 1-1 shows a WSG in a Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (UTRAN).

Figure 1-1 WSG Implementation in a UTRAN



Cisco Service and Application Module for IP (SAMI) Overview

The WSG application runs on the Cisco SAMI. The SAMI offers the following features:

- Takes up one slot in a Cisco 7600 router.
- Connects to the switch fabric in the Cisco 7600 router—SAMI does not have outside ports.
- Offers parallel architecture for Cisco applications—SAMI uses an IXP2800 network processor flow-distributor running at 1.4 GHz.
- Uses six PowerPCs (PPCs)—each PPC runs the same version of a Cisco application at 1.25 GHz.

Supervisor Engine

Using the Supervisor (SUP) Engine, virtual local area networks (VLANs) direct traffic from outside ports to each instance of the WSG on PPCs. A 10 Gigabit Ethernet port on the backplane connects the SAMI and the SUP.

From the SUP, start a session to each WSG instance. This allows you to do the following with the WSG:

- Set up
- Monitor
- Troubleshoot

For more information about the SAMI, see the *Cisco Service and Application Module for IP User Guide*.

WSG on a SAMI

This process shows how the WSG installs on a SAMI:

1. SAMI's SUP downloads the WSG application.
2. The SUP sends the WSG image to each of the SAMI's six PPCs.
3. The same WSG image installs on all of the PPCs.

After installing the WSG, individually set up each PPC. Use SAMI's remote console and logging (RCAL) to log into the SUP. This acts as a single connection to access the SAMI linecard control processor (LCP) and the PPCs. Using the SUP you can:

- Debug
- View **show** command output
- View logging output

WSG Features

WSG ships loaded on SAMI PPCs with fully-functional defaults that support the following features.

The following features are supported in WSG Release 4.4 and above:

- To increase the overall throughput of the WSG SAMI, the IXP Traffic distribution feature provides a method to divide the Clear traffic between 2 IXPs (IXP0 and IXP1) and enables both the IXPs to handle even distribution of traffic. The IXP1 will now handle more of the post encryption traffic which was originally handled by IXP0.
- Prior to Cisco 7600 WSG Release 4.4, WSG supported only TCP as the CMPv2 Transport Protocol. With Release 4.4 and above, WSG will support both transport protocols, TCP and HTTP. The HTTP based flows will be RFC 4210/4211/6712 compliant.

The following features are supported in WSG Release 4.3.2 and above:

- On request of IPsec client, WSG allocates the DNS server IP from a DHCP server or it can be locally configured on WSG card itself. As most WSG supports 3 DNS server IPs, wherein the DNS server IPs requested from DHCP server will have more precedence than the DNS IPs which are locally configured.

The following features are supported in WSG Release 4.3 and above:

- Allocation of IPv6 addresses from a DHCPv6 server to obtain an IPv6 address for IPSec tunnel setup.

Note DHCP is supported for RAS profiles and not for site-to-site profiles.

The following features are supported in WSG Release 4.2 and above:

- WSG performance and throughput indicators added to system to provide system wide throughput capacity characteristics of WSG. It also helps to identify the traffic load so that customer can plan for any future expansion of their system. The throughput capacity data is collected separately on each of the IXP. The packet and byte count are done on each packet in the lookup engine before Nitrox/PPC processing. Fragmented ESP packets are counted after reassembly. PPC CPU utilization should be monitored for fragmented packets. The overall throughput capacity is the sum of the throughputs on each IXP. The overall throughput utilization is limited by the limit on each IXP.
- IKE/IPSec Stats Collection and Timing Enhancements for SNMP:
  - Synchronized Statistics collection start times across all SAMI blades in a chassis using a NTP clock
  - Real time statistics collection for CLIs similar to previous releases
  - Auto adjustment of statistics collection interval based on the number of SAs
  - Configurable fixed statistics collection interval length
  - Persistent IKE/IPSec tunnel index for SNMP during a tunnel's lifetime
  - Alignment of IKE/IPSec global and per-tunnel statistics

The following features are supported in WSG Release 4.0 and above:

- Compared to policy-based routing, the IKEv2 redirect feature provides a more flexible scheme for load balancing between multiple WSG cards. The IKEv2 redirect feature is used in conjunction with the exchange director feature on the SUP. After the tunnel is set up, the packets flow directly to each WSG card.
- The Reverse Route Injection (RRI) feature now supports IPv6 routes. The IPv6 routes are inserted into the SUP or Route Switch Processor (RSP).
- High availability (HA) active-active redundancy mode (added in addition to active-standby mode). This feature supports active-active redundancy between two WSG cards for site-to-site tunnels. Compared to an active-standby redundant pair, the active-active mode allows full utilization of packet throughput of each redundant WSG card except during switch-over scenario.
- A global PMTU value can be configured to be used on all IPv4 and IPv6 tunnels. Path MTU (PMTU) discovery is a technique using ICMP to determine MTU size on the path between two hosts. PMTU is the effective MTU along the path and indicates the largest size to avoid fragmentation of IP packets. In IPSec tunneling, PMTU is utilized when performing pre-tunnel fragmentation to avoid the more expensive post-tunnel fragmentation.
- WSG now supports SSH user authentication using RADIUS server. When the RADIUS server is unreachable, the WSG will fallback to authenticating the SSH user locally.
- IPv6 VRF Support
- IPv6 DHCP Support
- Using reverse DNS lookup, WSG now displays both IP address and hostname for IKE peers.
- S2S Blacklisting

The following features are supported in WSG Release 3.1 and above:

- Prior to WSG Release 3.1, syslog messages display the CPU ID as the name of the source host where messages originated from. The enhancement in WSG Release 3.1 adds the configured hostname along with the CPU ID to the syslog in order to make management easier.
- Up to 5 multiple access-permit statements can be configured in a remote-access crypto profile.
- Multiple external logging servers with IPv4 addresses can be configured for syslog messages. Only a single logging server with an IPv6 address can be configured at a time.

The following features are supported in WSG Release 3.0 and above:

- IPv6 support was added in WSG Release 3.0. This feature allows users to configure interfaces with IPv6 addresses. IPv6 support is present for both the IKE SAs and IPSec SAs, enabling IPv6 IKE packet handling in the control path and IPv6 ESP packet handling in the datapath. WSG also supports the use of same or different IP protocol versions for the IKE SA and the IPSec SA, so an IPv4 IKE SA can be paired with an IPv6 IPSec SA and vice versa. This allows IPv6 clear packets to be secured inside an IPv4 tunnel or IPv4 clear packets to be secured inside an IPv6 tunnel
- Virtual Routing and Forwarding (VRF) allows the creation of multiple virtual networks within a single network entity. Each VRF comprises an IP routing table and a forwarding table, allowing the use of the same or overlapping IP addresses without conflicts. In a single network entity, multiple VRFs can be used to create isolation between virtual networks. VRFs allow encrypted/decrypted traffic separation, by having the encrypted traffic in one outside VRF and the decrypted traffic in one inside VRF.

  The typical case for this is an ISP that provides VPN service to multiple enterprise customers on the same box, the users and branches connect using internet for the encrypted traffic, but the decrypted traffic needs to go to the private network of each separate customer and this traffic cannot be mixed.
- Data Plane Routing

  Prior to WSG Release 3.0, all return traffic between the WSG and the SUP is carried over the same VLAN. It is not desirable for customers to have all their traffic converge onto the same VLAN at any point in the packet path. This feature supports true dual-arm implementation. Traffic on the clear and protected sides traverse different VLANs.

  A static routing table for IPv4/IPv6 is maintained on IXP for forwarding packets out to the correct VLAN. IPv4/IPv6 static routes are configured on the PPC. On the same PPC, two identical routes can be present in different VRFs. In case of more than one match in the routing table, the longest prefix approach is used. The maximum number of static routes per VRF per PPC is 10. The maximum number of static routes per WSG is 60. Dynamic routing is not supported in WSG Release 3.0.
- A SSH server is added in WSG Release 3.0. Open SSH is used to provide the SSH server while CLIs control and configure it. Since the main reason for SSH is to allow secure login on non-secure networks, the SSH server will respond to requests from all interfaces. Only SSHv2 and DSA are supported. DSA is similar to RSA but does not require an export license.

  There is no support for groups or privileges configuration. All users have the same privilege. Admin Group or role assignments are not supported. The number of users that can be configured are limited by the size of the configuration file. There is no timeout on the SSH sessions. The user cannot kill a session from the CLI.
- Per Peer IP Tunnel Debug

  WSG supports per peer debugging of tunnel setup and IKE protocol exchanges by allowing the peer IP address to be specified when turning on debugs.
- Reverse Route Injection (RRI)

Introduced in WSG Release 3.0, the RRI feature obviates the need to manually configure static routes on the SUP for clear traffic routing purposes in the reverse direction. RRI route entries are injected into the SUP when IPSec tunnels are created. These route entries are correspondingly withdrawn from the SUP when the IPSec tunnels are deleted. The BGP protocol is used to re-distribute the routes from WSG to the SUP. For WSG Release 3.0, the RRI feature supports only IPv4. Also, only site-to-site profiles are supported. The VRF feature on the WSG cannot be enabled when the RRI feature is already configured.

- WSG supports authentication of a peer through EAP-MD5, EAP-AKA and EAP-SIM protocols. These protocols are only supported with certificates for authenticating the WSG to the peer. Use of preshared keys to authenticate the WSG to the peer is not allowed by the standards, but might be required to support some legacy equipment. The EAP authentication is supported for IKEv2 only.
- RADIUS Accounting

  In some Femto networks, an Access Point (AP) sets up an IPSec tunnel with the WSG and sends an Iuh Register message via the tunnel to a Femto Gateway (FGW). The Iuh Register message is an IP packet which also contains the ID of the AP registering with the FGW. The ID used by the AP is the same as the IKE ID used by the AP during IPSec tunnel setup. The FGW needs to make sure that an authenticated AP is not presenting itself as another AP during registration. This can be achieved by the FGW by comparing the source IP address of the Iuh Register packet with the internal IP address assigned by the WSG for the same AP (ID is the lookup key). For this to work, the WSG needs to send the ID to internal IP address mapping to the FGW every time it assigns an IP to the AP. RADIUS Accounting messages are used to send the IKE ID to assigned IP address mapping from the WSG to the AAA server running in the FGW.
- Traffic-based Phase 2 rekey is introduced in WSG Release 3.0. This feature allows the user to specify security association lifetime in megabytes or seconds. Both formats of lifetime value can exist at the same time, and Phase 2 rekey is triggered by whichever occurs first.
- Blacklisting Remote Peer

  The blacklisting feature is a mechanism to prevent a remote peer from setting up a tunnel to the WSG. With the blacklisting feature, when a remote peer attempts to setup a tunnel with the WSG, the IKE ID of the remote peer is searched for in a blacklist file available to the WSG. If a match is found, the IKE AUTH request is failed and the remote peer is prevented from establishing a tunnel. The blacklisting feature provides a fast and simple mechanism to block a remote peer from setting up a tunnel to the WSG.
- Multiple IKE Proposals

  Remote peers can negotiate multiple proposals during IKE Phase 1. Each proposal contains one or more encryptions, integrity, prf and DH group algorithms. WSG accepts multiple proposals during IKE SA setup and rekey.
- Multiple DH groups, EAP authentication algorithms, and transform sets are supported in WSG Release 3.0.
- DHCP Address Allocation. See the "DHCP Address Allocation" section on page 2-61 for more information.
- High Availability

  WSG Release 2.0 and above supports inter-chassis stateful 1:1 redundancy. Redundancy works at the SAMI level. All 6 PPCs on a SAMI are in active or hot standby state. The PPC of the active WSG syncs its state to the corresponding PPC of the redundant WSG (for example, PPC3 (A) to PPC3 (S).

  The WSG redundancy feature works with all IPSec supported features including IKEv1, IKEv2, ESN, anti-replay, DPD, and NAT-traversal. WSG redundancy is applicable to both remote access and site-to-site tunnels.

If a primary card fails, traffic is switched to the newly active SAMI. The established tunnels stay up and continue to pass traffic after failover, and the IKE/IPSec internal state is synced between the active and redundant WSGs. Traffic outage is less than 1 second after the failure detection.

- Site-to-Site Scalability Improvements

  In previous releases, site-to-site traffic selector lookup was done by looking up an array of TS on the IXP. This linear search limited the performance of the site-to-site traffic selector lookup algorithm. For WSG Release 2.0 and above, the traffic selector lookup algorithm improves site-to-site performance. No change occurs for remote access traffic selector lookup; it is different from the lookup algorithm for site-to-site, and is already optimized.

  Up to 16666 S2S tunnels are supported per SAMI blade. S2S tunnels can only be configured on the director PPC.

  IKE protocol allows a peer to negotiate multiple TS for the same tunnel. However, in WSG Release 2.0 each tunnel can negotiate only one TS.

  All other features that are currently supported for site-to-site and remote access are maintained.

- Certificate Management Protocol

  WSG Release 2.0 introduced support for Certificate Management Protocol (CMPv2).

  The user manually requests the initial key or certificate from the CA server using the **crypto cmp initialize** command. The initial request is authenticated using the reference number and pre-shared key (PSK) from the CA server using an out-of-band mechanism. After receiving the initial certificate, the **crypto cmp enroll** command is used to enroll the certificate using the public key. Prior to the certificate expiration, the **crypto cmp update** command is used to update the certificate and private key. The WSG changes the name of the certificate and private key files during the update, so any WSG configuration commands which use the previous certificate file names must be replaced with commands using the new file names (configuration commands with **wsg-cert** or **current-wsg-cert** keywords). After the initialize, enroll, and update commands, the certificate and private key files are copied from the WSG to the SUPs in the Cisco 7600 chassis. The files must be manually copied to the SUP on other Cisco 7600 chassis.

  WSG Release 3.0 introduced an automatic certificate renewal mechanism. The **crypto cmp auto-update** configuration command may be used on a WSG to automatically update the certificate and private key and send them to its SUPs. The **crypto cert renewal retrieve** configuration command is used on other WSGs to retrieve the updated certificate from the Cisco 7600 SUPs. Both commands are global configuration commands, thus the configuration is saved. In a HA configuration, both commands update the standby WSG, which then updates their SUPs. If inter-chassis redundancy is configured, the certificate and private key will be propagated to redundant chassis. A WSG may be configured to automatically update some certificates and automatically retrieve others. The maximum number of certificates that may be configured for automatic renewal (update and retrieve) is 20.

  Syslog messages and two SNMP traps, **cert-expiry** and **cert-renewal**, were introduced for CMPv2 in WSG Release 3.0. The **crypto pki wsg-cert-trap expiry notification** configuration command may be used to configure a **cert-expiry** trap and syslog up to 30 days before a WSG certificate is about to expire (default is 24 hours). The **cert-renewal** trap and syslog will provide notifications for the automatic update or retrieve status, which may be configured to start 2 to 60 days before the certificate will expire. The SNMP traps are enabled using the **snmp-server enable traps ipsec** configuration command.

- Online Certificate Status Protocol

  In previous releases, the WSG used CRL (Certificate Revocation List) to obtain from the CRL server, a file containing the list of certificates that were revoked.

In WSG Release 2.0 the Online Certificate Status Protocol (OCSP) feature was introduced to address some of the limitations of CRL. OCSP works to achieve the same objective as the CRL mechanism; it determines if a certificate offered by a peer has been revoked. OCSP differs from CRL in that the revocation status is obtained on a per-certificate basis rather than a trust anchor basis. Since the revocation status is obtained when the certificate is first seen by the WSG, the status is up to date.

- IKEv1 and IKEv2 and Public Key Infrastructure (PKI)—IKE is a hybrid protocol that does the following for IPSec:
  - Authenticates peers
  - Negotiates IKE and security associations (SAs)
  - Sets up encryption algorithms keys

  IPSec SAs are secured links in one direction. IPSec endpoints must authenticate themselves to each other and set up Internet Security Association and Key Management Protocol (ISAKMP) shared keys.

  WSG uses the IKEv1 or IKEv2 protocols to communicate with the IPSec endpoint to set up an Encapsulating Security Payload (ESP)-encapsulated tunnel. This tunnel gives protected access to a private network. The WSG encapsulates, encrypts, and authenticates packets from private networks to IPSec endpoints. In the reverse direction, the WSG decapsulates, decrypts, and authenticates.
- Site-to-site tunnels are supported. This allows WSG to establish site-to-site tunnels with a peer (which can be another WSG, or any other implementation). The site-to-site tunnels between two peers are used to encrypt clear traffic originating from their protected networks. The WSG can be configured to either auto-initiate a site-to-site tunnel with a peer, or wait for incoming IKE requests to create a tunnel. The WSG supports both IKEv1 and IKEv2 for site-to-site tunnels.
- Both remote access and site-to-site type profiles can be used in combination on a SAMI. However, only one profile of type remote access is supported while multiple site-to-site profiles can be configured.
- DPD Initiation

  The DPD initiation feature allows the WSG to send DPD to peers at a regular interval. This allows WSG to detect and remove dead connections or peers. This feature is independent of existing functionality where the SAMI responds to DPD messages from its peer. The SAMI is able to both initiate DPD and respond to DPD at the same time.
- WSG Release 1.2 and above supports the extended form of traffic selectors. An additional extended syntax for the **access-permit** command is added in this release to configure the extended traffic selector used on established tunnels. The new form of traffic selectors can now include the following parameters, which are passed in the Traffic Selector payload during the IKE message exchange for establishing the tunnels:
  - Source IP address range
  - Source port range
  - Destination IP address range
  - Destination port range
  - IP protocol
- Multiple Child SA

  For a single IKE association with a peer, multiple child IPSec SAs can be created, each with its own traffic selector rule. We support one traffic selector per child IPSec SA.
- DNS to AP feature allows the WSG to pass the DNS server IP address to the remote peer.

- The WSG supports platform traps for PPC CPU congestion and memory exhaustion.
- OAM traffic routing feature allows the WSG to do static routes on the PPC to carry OAM traffic directly to a local network through a VLAN interface. Bearer traffic sent by IXP will go to the default gateway only. Additionally, this feature allows the WSG to create a separate VLAN interface on the PPC for carrying OAM traffic only.
- Single-entity configuration allows you to configure the SAMI from a single login interface rather than going to each of the 6 PPCs individually and configuring them. Parameters that are required to be different on each PPC (like address pool) still need to be configured multiple times (through the same session) on each PPC.
- All traps, syslog and SNMP stats are sent from a single PPC. For SNMP stats the external SNMP manager goes to the single PPC to retrieve stats for all the PPCs.
- The PPC Traffic Throttle feature throttles the number of IKE INIT messages sent to the PPC. This prioritizes the DPD traffic over new tunnel requests, and allows existing tunnels to remain intact. There is a specific bandwidth limit for each PPC which is slightly larger than the supported tunnel setup rate. Each PPC is throttled separately.
- WSG Release 1.2 and above supports debugs using the CLI.
- **Diffie-Hellman (DH)**

  In WSG Release 1.2 and above, DH Groups **14**, **15**, **16**, **17**, and **18** are added to **groups 1, 2 and 5**. DH is a public-key cryptography protocol. It allows two parties to set up a shared secret key used by encryption algorithms over an insecure communications channel. DH is used within IKE to set up session keys.
- WSG Release 1.2 and above adds Extended Sequence Number (ESN) support as longer lifetimes are expected in customer deployments. Additionally, higher traffic is expected in site-to-site setups. Extended Sequence Number (64 bit sequence number) implementation is required in such cases. In this release, the sequence number length cannot be negotiated by the peer with SAMI. The peer will have to match the setting on the SAMI (default is 32-bit sequence number). The 64 bit sequence number can be configured using the CLI.

The following features were introduced prior to WSG Release 1.2 and are still applicable:

- IPSec Security Association Lifetime

  The SA is kept by each peer until its lifetime expires. Because new SAs are negotiated before current SAs expire, they can be reused to save time. Shorter lifetimes mean more secure negotiations. Longer lifetimes mean SAs are more quickly set up.
- IKE Encryption

  WSG supports the following IKE secret encryption schemes:
  - Data Encryption Standard (DES)
  - Triple DES (3DES), also known as Triple Data Encryption Algorithm (3TDEA)
  - Advanced Encryption Standard (AES) (128, 192, 256)
- **N + 1 Redundancy** (load balancing with ACE module)
- **IPv4 traffic**
- **ESP transforms in IPSec Tunnel Mode**
- The WSG CLI is a line-oriented user interface that gives commands for customizing IPSec environment variables. This document describes only the features related to IPSec configuration. For a complete description of the features set up at the WSG CLI, see the *Cisco Service and Application Module for IP User Guide*.

- **NAT Traversal**

  The WSG supports IKE NAT traversal by encapsulating the ESP payload over UDP as in RFC 3948. The WSG listens for IKE messages on UDP ports 500 and 4500. When it receives an IKE request the WSG responds to the address and port from which the request is received. With NAT Detection Source/Destination IP notifications, if the WSG detects that the peer is behind a NAT device, it sets up an ESP tunnel to be UDP encapsulated.

- **X.509 Digital Certificate**

  The digital certificate is a package containing information such as the identity of a certificate bearer: his or her name or IP address, the certificate's serial number, the certificate's expiration date, and a copy of the certificate bearer's public key. The standard digital certificate format is defined in the X.509 specification.

- 100,000 Remote Access tunnels per SAMI.
- Site-to-site tunnels are supported.
- Pre-shared Keys—WSG and another network element agree ahead of time on a shared, secret key. The two use this preshared key during security negotiation.
- SNMP Version 2 Traps and MIBs—Each PPC runs an SNMP agent and generates its own SNMP traps. WSG supports SNMP statistics using Cisco Standard IPSec and IOS infrastructure MIBs.
- IPSec Anti-Replay—IPSec Anti-Replay is a security service on the WSG. Using IPSec Anti-Replay, the WSG rejects old or duplicate packets. This protects the WSG from replay attacks, the fraudulent resending of data.
- IPSec Perfect Forward Secrecy (PFS), Groups 1, 2 and 5—IPSec PFS ensures one IPSec SA key can not be used to build another. This prevents an attacker from breaking a key associated with a session, copying data, and compromising other IPSec SAs.
- Certificate Authority (CA) Certificate Chaining—A certificate chain is a sequence of certificates with dependent trust relationships. The first certificate is self-signed by the CA. Each subsequent certificate creates an association between a certificate owners, or CAs in the chain. This process creates a trust chain from trusted peer to a CA.
- Multiple CA Trust Anchors—A trust anchor is a third party the WSG trusts and to which it has a certification path. The trust anchor certifies the WSG. This certificate has information about prefixes that a WSG is allowed to use in router advertisements. Authorization delegation discovery enables a node to adopt a WSG as its default router.
- Hash Algorithms—Hash is a one-way algorithm. Hash takes an input message of arbitrary length and turns it into a fixed-length digest. Cisco uses Secure Hash Algorithm (SHA), Message Digest 5 (MD5), and AES-XCBC.

Feature Exclusions

- VRF feature on the WSG cannot be enabled when the RRI feature is already configured.

RFCs

For additional information, refer to these RFCs:

- RFC 822, *Standard for the Format of ARPA Internet Text Messages*

- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 2402, *IP Authentication Header*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*
- RFC 2407,*The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPSec*
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2869, *RADIUS Extensions*
- RFC 3022, *Traditional IP Network Address Translator*
- RFC 3027, *Protocol Complications with the IP Network Address Translator*
- RFC 3162, *RADIUS and IPv6*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE),* Group 2 only
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec, AES 128-CBC*
- RFC 3686, *Using AES Counter Mode With IPsec ESP*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- RFC 3947, *Negotiation of NAT-Traversal in the IKE*
- RFC 3948, *UDP Encapsulation of IPsec ESP Packets*
- RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*
- RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*
- RFC 4302, *IP Authentication Header*
- RFC 4303, *IP Encapsulating Security Payload (ESP)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 4308, *Cryptographic Suites for IPsec*
- RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*
- RFC 4634, *US Secure Hash Algorithms (SHA and HMAC-SHA)*
- RFC 4718, *IKEv2 Clarifications and Implementation Guidelines*
- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

- RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 6712, *Internet X.509 Public Key Infrastructure: HTTP Transfer for the Certificate Management Protocol (CMP)*