CHAPTER 2

Learning About the WSG

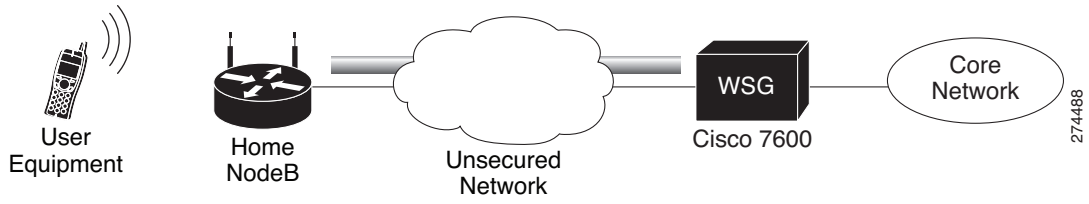
The following sections tell you about the WSG and the Cisco Service and Application Module for IP (SAMI).

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

Figure 1 WSG Implementation in a UTRAN



Cisco Service and Application Module for IP (SAMI) Overview

The WSG application runs on the Cisco Service Application for IP module (SAMI). 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 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 Supervisor Engine.

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

- Set up
- Monitor
- Troubleshoot

For information about 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 Supervisor Engine downloads the WSG application.
2. The Supervisor Engine sends the WSG image to each of SAMI's six PPCs.
3. The same WSG image installs on all PPCs.

After the WSG installs, separately set up each PPC. Use SAMI's remote console and logging (RCAL) to log in to the Supervisor Engine. This acts as a single connection to access the SAMI line card control processor (LCP) and the PPCs. Using the Supervisor Engine you can:

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

WSG Features

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

The following features are supported in WSG Release 2.0:

- High Availability

  Cisco 7600 Wireless Security Gateway Release 2.0 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 card. 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 Release 2.0, 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 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

  Release 2.0 introduces support for Certificate Management Protocol (CMPv2).

  WSG currently provides some support to generate its own certificate. Users generate a private key and a certificate request. The certificate request is transferred out to a CA server to generate a certificate, and the generated certificate needs to be transferred back into the 7600. The private key and the certificate will reside on the storage on the SUP of the 7600 chassis and other certificate configuration CLI will reference to these files. The root certificate of the CA also needs to be copied to the SUP storage.

  The operation of transferring files in and out of the 7600 chassis is cumbersome and error prone. Automatic certification enrollment protocols can be used to automate the process of generating the certificate from the WSG CLI itself. The private key and WSG certificate are written to the SUP storage automatically.

- 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 Release 2.0 the Online Certificate Status Protocol (OCSP) feature is 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 in this release. 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.
- 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.
- WSG supports authentication of a peer through EAP-MD5, EAP-AKA and EAP-SIM protocols. 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.
- 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 (D-H)—In WSG 1.2 and above, Diffie-Helman (DH) Groups **14**, **15**, **16**, **17**, and **18** are added to groups **1**, **2** and **5**. D-H 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. D-H is used within IKE to set up session keys.
- WSG 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
- CLI—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.
- 100k Remote Access tunnels per SAMI.
- Site-to-site tunnels are also 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.

Additional References

For additional information, see these:

- RFCs, page 2-6
- Finding Related Documentation, page 2-7

RFCs

For additional information, see these RFCs:

- RFC 822, *Standard for the Format of ARPA Internet Text Messages*
- 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 3022, *Traditional IP Network Address Translator*
- RFC 3027, *Protocol Complications with the IP Network Address Translator*
- 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 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)*

Finding Related Documentation

- *Release Notes for the Cisco 7600 Wireless Security Gateway Release 2.0*
- *Cisco Service and Application Module for IP Memory Upgrade Installation Note*
- *Cisco Service and Application Module for IP Guide to User Documents*
- *Cisco Service and Application Module for IP User Guide*
- Cisco 7600 series router platform
  - *Release Notes for Cisco IOS Release 12.2(33)SRC3 for the Cisco 7600 Series Routers*
  - *Cisco 7600 Series Router Installation Guide*
  - *Cisco 7600 Series Router Module Installation Guide*
  - *Cisco 7600 Series Router Cisco IOS Command Reference*
  - *Cisco 7600 Series Router Cisco IOS System Message Guide*
  - Application Control Engine Module Server Load-Balancing Configuration Guide (Software Version A2(1.0))
  - Configuring File Storage and the Remote Copy Protocol (RCP), see the *Cisco Service and Application Module for IP User Guide.*

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/slb/guide/slbgd.html
  - *Configuring Load Balancing, see ACE Configuration Guide*:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/slb/guide/slbgd.html
  - For information about MIBs, see:
    http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The documents are at

- Cisco 7600 series home page on Cisco.com at

  Products & Solutions > Products > Routers and Routing Systems > 7600 Series Routers

- Cisco 7600 series technical documentation on Cisco.com at

  Products & Solutions > Products > Routers and Routing Systems > 7600 Series Routers > in the Technical Documentation & Tools box on the right of the page, **Cisco 7600 Series Routers**