Security Gateway Overview

This chapter contains general overview information about the Security Gateway (SecGW) running on an ASR 9000 Virtualized Service Module (VSM) as a VPC-VSM instance.

The following topics are covered in this chapter:

Product Overview

The SecGW is a high-density IP Security (IPSec) gateway for mobile wireless carrier networks. It is typically used to secure backhaul traffic between the Radio Access Network (RAN) and the operator core network.

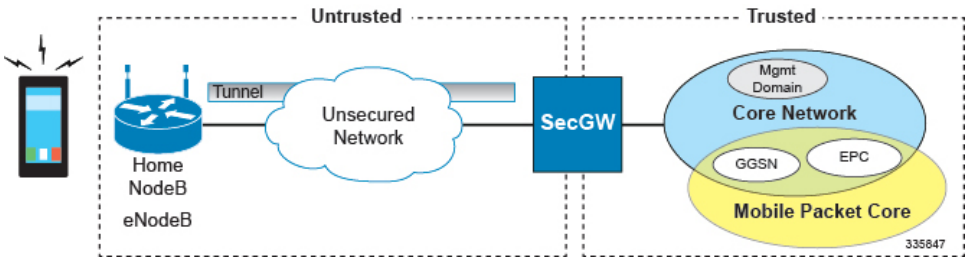
IPSec is an open standards set that provides confidentiality, integrity, and authentication for data between IP layer peers. The SecGW uses IPSec-protected tunnels to connect outside endpoints. SecGW implements the parts of IKE/IPSec required for its role in mobile networks.

The SecGW is enabled as a Wireless Security Gateway (WSG) service in a StarOS instance running in a virtual machine on a Virtualized Services Module (VSM) in an ASR 9000.

The following types of LTE traffic may be carried over encrypted IPSec tunnels in the Un-trusted access domain:

- S1-C and S1-U: Control and User Traffic between eNodeB and EPC
- X2-C and X2-U: Control and User Traffic between eNodeBs during Handoff
- SPs typically carry only Control Traffic, however there exists a case for carrying non-Internet User traffic over secured tunnels

Figure 1: SecGW Implementation



ASR 9000 VSM

SecGW is enabled via a StarOS image running in a virtualized environment supported on the ASR 9000 VSM. StarOS runs in four hypervisor-initiated virtual machines (one per CPU) on the VSM.

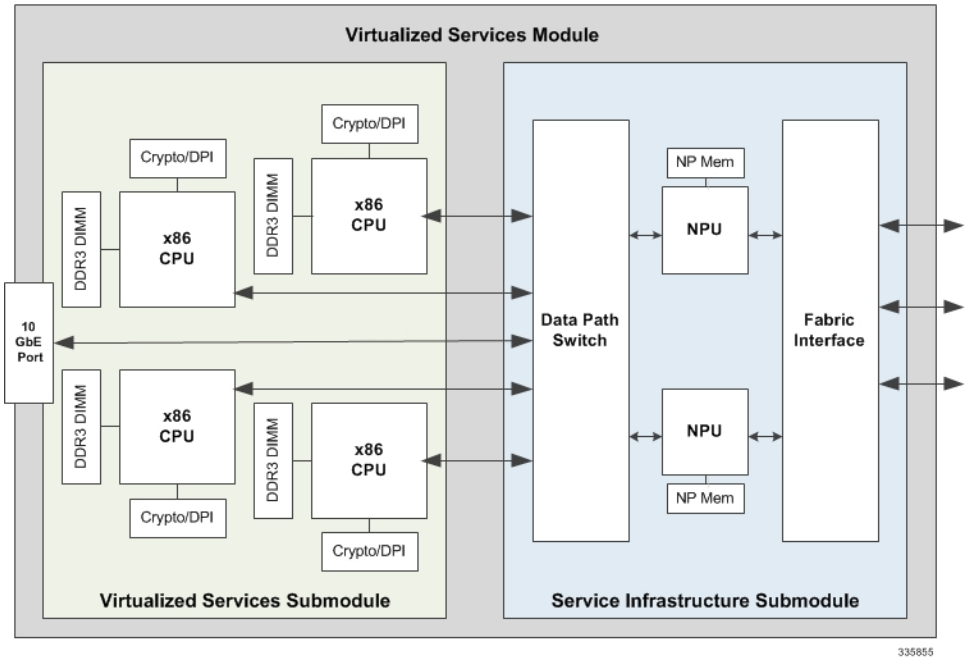
Also SecGW Suppors VPC-DI platform.

The VSM is a service blade for the ASR 9000 router that supports multiple services and applications running simultaneously on top of a virtualized hardware environment.

The VSM supports the following major hardware components:

- (4) CPUs [20 cores per socket]
- (4) hardware crypto devices
- (1) Data Path Switch supporting (12) 10 Gigabit Ethernet (GbE) devices
- (2) NPUs

Figure 2: VSM High Level Block Diagram



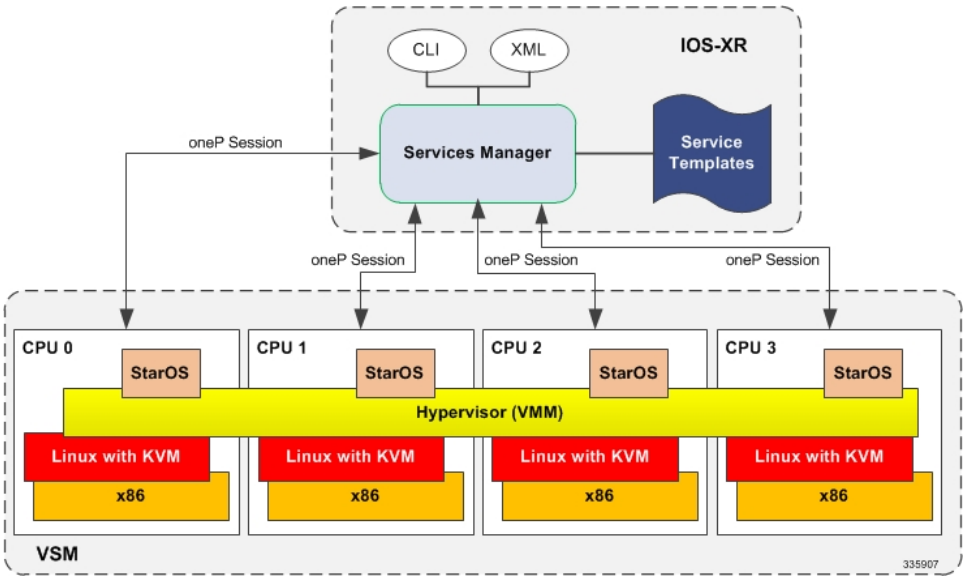
The ASR 9000 services architecture encompasses how the platform interfaces with the services independent of where the service is actually instantiated. It provides a common control plane, management plane and data plane infrastructure such that a consistent end user experience is provided whether the service is running on a service blade, on the RSP, on an attached appliance or server, or even running inline in the router.

The ASR 9000 platform supports the following functions:

- Enables services via IOS-XR
- Provides platform management via CLI and XML for:
  - Service parameter specification
  - Validation of service package including licenses
  - Service instantiation with associated parameters
  - Service health monitoring
  - Service termination, re-start and upgrades
- Decouples configuration of the WSG service from the service creation infrastructure
- Provides a set of templates for service parameters
- Interfaces with the hypervisor (Virtual Machine Manager client) to setup the StarOS WSG service on multiple virtual machines (VMs)

The figure below shows the relationship between IOS-XR running on the ASR 9000 and StarOS running on the VSM.

Figure 3: IOS-XR and VSM



The 10GE interfaces on the SecGW virtual machines are visible as 10GbE interfaces on the ASR 9000. The ASR 9000 line card forwards IP traffic to VSM 10GbE ports.

VSM Resource Mapping to VPC-VSM VMs

There are four CPU sockets on the VSM. Each CPU supports multiple cores. A VPC-VSM instance uses multiple virtual CPUs (vCPUs) consisting of available cores for its virtual machine.

Each CPU socket is associated with a Crypto engine. PCI Ports are also assigned to accept traffic from the ASR 9000 line cards.

The table below shows how resources are assigned among the four CPUs on the VSM.

Table 1: Resource Assignments for VSM CPUs

CPU	Available Cores	Crypto Device	PCI Port ID	VM	vCPUs
0	16 (2–9, 42–49)	04:00.0	00.0.0	VM1	16
			00.0.1		
1	18 (11–19, 51–59)	45.00.0	42.0.0		
			42.0.1	VM2	16
			48.0.0		
			48.0.1		
2	20 (20-29, 60-69)	85:00.0	82:0.0	VM3	20
			82:0.1		
			88:0.0		
			88:0.1	—	—
3	20 (30-39, 70-79)	C5:00.0	C2:0.0	VM4	20
			C2:0.1		
			C8:0.0		
			C8:0.1	—	—

Only twelve PCI ports can be mapped to ASR 9000 line card traffic. The table below shows how the interfaces are distributed.

Table 2: PCI Port Mapping

PCI Port ID	CPU	ASR 9000 TenG	VPC Slot/Port	VM	Application IF
00:0.0	0	TenGx/y/z/0	1/10	VM1	Uplink
00:0.1		TenGx/y/z/1	1/11		Downlink
42:0.0	1	TenGx/y/z/2	1/1		Management
42.0.1		TenGx/y/z/3	1/10	VM2	Uplink
48.0.0		TenGx/y/z/4	1/11		Downlink
48.0.1		TenGx/y/z/5	1/1		Management

PCI Port ID	CPU	ASR 9000 TenG	VPC Slot/Port	VM	Application IF
82:0.0	2	TenGx/y/z/6	1/10	VM3	Uplink
82:0.1		TenGx/y/z/7	1/11		Downlink
88:0.0		TenGx/y/z/8	1/1		Management
88:0.1		—	—	—	Unused
C2:0.0	3	TenGx/y/z/9	1/10	VM4	Uplink
C2:0.1		TenGx/y/z/10	1/11		Downlink
C8:0.0		TenGx/y/z/11	1/1		Management
C8:0.1		—	—	—	Unused

- For all VMs except VM1, the NICs are allocated from the corresponding socket. But in VM1, the third NIC (42:0.0) is picked from a different socket. To achieve maximum throughput, that NIC is used as the management port and the other two are used for the service.
- To make the interface-to-port mapping symmetric across all the VMs, the third NIC is always used as the management port.

VPC-VSM

Virtualized Packet Core for VSM (VPC-VSM) consists of the set virtualized mobility functions that implement mobility specific services and applications within the core of the network. VPC-VSM is essentially StarOS running within a Virtual Machine (VM).

VPC-VSM only interacts with supported hypervisors. It has little or no knowledge of physical devices.

Each VPC-VSM VM takes on the roles of an entire StarOS system. The only interfaces exposed outside the VM are those for external management and service traffic. Each VM is managed independently.

Each VPC-VSM VM performs the following StarOS functions:

- Controller tasks
- Out-of-band management for CLI and Logging
- Local context (management)
- NPU simulation via fastpath and slowpath
- Non-local context (subscriber traffic)
- Crypto processing (IPSec)

For a complete description of VPC-VSM functionality, refer to the *VPC-VSM System Administration Guide*.

Important Up to four instances of VPC-VSM can run on an ASR 9000 VSM. Each VSM CPU supports only one VPC-VSM instance. VSM resources are allocated to each SecGW VM; no other application VM is supported on any VSM CPU. vNICs must be passed to the SecGW VMs from RSP.

SecGW Application

The StarOS-based Security Gateway (SecGW) application is a solution for Remote-Access (RAS) and Site-to-Site (S2S) mobile network environments. It is implemented via StarOS as a WSG (Wireless Security Gateway) service that leverages the IPSec features supported by StarOS.

SecGW delivers the S2S IP Encryption capabilities required in UMTS/HSPA and LTE 3GPP LTE/SAE network architectures.

For complete descriptions of supported IPSec features, see the *IPSec Reference*.

Important 20.0.x is the last fully qualified build for ASR9k SecGW.

Important The SecGW is a licensed StarOS feature. A separate license is required for each VPC-VSM instance and SecGW. Contact your Cisco account representative for detailed information on specific licensing requirements.

Key Features

The following are key features of the SecGW product:

- Functions in a virtualized environment on one or more VSM blades in an ASR9000
- Supports IKEv2.
- Supports DES, 3DES, AES and NULL Encryption algorithms, and MD5, SHA1/2, HMAC-SHA2 and AES-XCBC Hash algorithms.
- Provides mechanisms for High Availability both within and outside of the ASR 9000 chassis.
- IPv6 support encompasses Inner-Outer pairs – v6-v6, v6-v4, v4-v6, v4-v4
- Allows dynamic provisioning of IPSec configuration for a new WSG service in the existing SecGW instance.

Each of the four SecGWs on a VSM must be configured separately.

Load balancing has not been implemented for the SecGWs; incoming calls will not be automatically distributed across the four SecGWs on a VSM. A workaround is to use VLANs for load balancing. The public side interface of each SecGW can be configured for a separate VLAN. Calls from multiple peers are routed to the same IP address via a different VLAN to distribute the traffic load.

IPSec Capabilities

The following IPSec features are supported by StarOS for implementation in an SecGW application:

- Anti Replay
- Multiple Child SA (MCSA)
- Certificate Management Protocol (CMPv2)
- Session Recovery/Interchassis Session Recovery for both RAS and S2S
- Support for IKE ID Type
- PSK support with up to 255 octets
- Online Certificate Status Protocol (OCSP)
- Reverse DNS Lookup for Peer IP in show Commands

- Blacklist/Whitelist by IDi
- Rekey Traffic Overlap
- CRL fetching with LDAPv3
- Sequence Number based Rekey
- IKE Call Admission Control (CAC)
- PSK Support for up to 1000 Remote Secrets
- Certificate Chaining
- RFC 5996 Compliance
- Duplicate Session Detection
- Extended Sequence Number
- Security Gateway as IKE Initiator
- Support to provide DNS server address to the Peer

Reverse Route Injection

SecGW also supports Reverse Route Injection (RRI). RRI injects routes in the reverse direction onto the ASR 9000 VSM so that clear traffic can be routed to the correct interface on the target VPC-VSM. For additional information, see the *Reverse Route Injection* chapter.

SecGW Management

Each SecGW instance is configured individually via its Management port. However, the Cisco Prime network management tool can be used to configure and manage individual SecGW instances.

A common or default configurations can be captured as "templates" in Cisco Prime which are then applied to each SecGW instance or all SecGW instances in the network.

For additional information on the Cisco Prime Mobility suite, contact your Cisco account representative.

Alternatively an operator can create a StarOS configuration file on the first gateway. The resulting configuration file can then be copied and edited offline with different parameters. The edited configuration file is then copied to the flash drive of the second SecGW. The process is repeated until all four SecGWs have been initially configured.

Subsequent changes made to the configuration of each SecGW must be saved to the local configuration file. For security and recovery the individual configuration files should then be saved off the VMS to a target network destination.

For additional information, see the *VPC-VSM System Administration Guide*.

oneP Communication

Each SecGW creates a oneP session with the ASR 9000 for route insertions, policy creation and flow creation. For additional information, refer to the *oneP Communication* chapter.

ASR 9000 VSM IPSec High Availability

This section briefly describes the IPSec High Availability (HA) capabilities for VSM service cards within an ASR 9000.

For this release the ASR 9000 supports the following levels of High Availability

• Process Recovery, on page 8

HA functions are triggered for the following events:

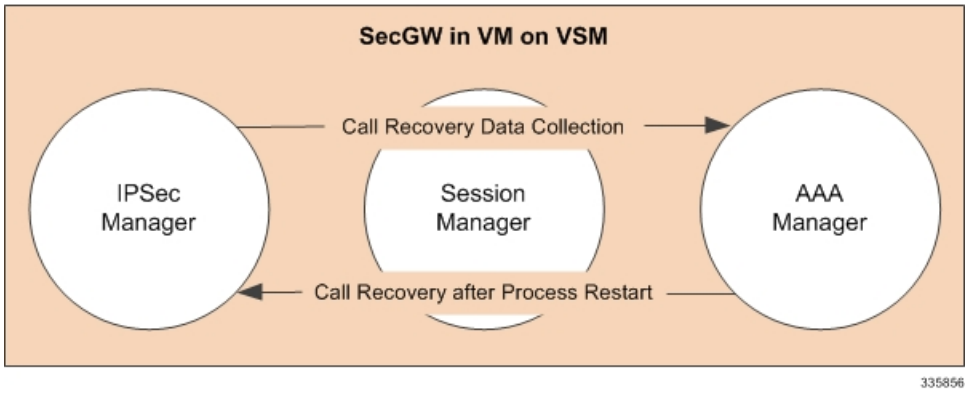
- Route Processor (RP) failure
- Virtual Machine (VM) failure
- VSM failure
- Link failure

Important The IPSec HA architecture is based on StarOS Interchassis Session Recovery (ICSR). For a complete description of ICSR and its configuration requirements, see the *VPC-VSM System Administration Guide*.

Process Recovery

The process recovery feature stores backup Security Association (SA) data in an AAA manager task. This manager runs on the SecGW where the recoverable tasks are located.

Figure 4: Process Recovery Diagram



VSM-to-VSM ICSR 1:1 Redundancy

In this redundancy scenario, Interchassis Session Recovery ICSR utilizes the Service Redundancy Protocol (SRP) implemented between VMs in a VSM running separate instances of VPC-VSM/SecGW in the same ASR 9000 chassis.

VSM card status data is exchanged between VPN managers on active and standby VSMs via SRP. SA data is also exchanged via SRP.

The *VPC-VSM System Administration Guide* fully describes ICSR configuration procedures.

Chassis-to-Chassis ICSR Redundancy

SecGW HA supports hot standby redundancy between VMs in a VSM in different ASR 9000 chassis. The Standby VSM is ready to become active once a switchover is triggered. SA re-negotiation is not required and traffic loss is minimal.

For additional information, see the *Reverse Route Injection (RRI)* chapter.

HA Configuration

HA involves configuration of both SRP and ConnectedApps (CA) for RRI to work.

HA employs ConnectedApps (CA) communication between the client running on the wsg-service VM and IOS-XR running on the ASR 9000.

StarOS **connectedapps** commands configure the CA client parameters, including those associated with HA mode. For additional information, refer to the *oneP Communication* chapter.

Network Deployment

SecGW supports the following network deployment scenarios:

- Remote Access Tunnels, on page 9
- Site-to-Site Tunnels, on page 9

Remote Access Tunnels

In a RAS scenario, a remote host negotiates a child SA with the SecGW and sends traffic inside the child SA that belongs to a single IP address inside the remote host. This is the inner IP address of the child SA. The outer IP address is the public IP address of the remote host. The addresses on the trusted network behind the SecGW to which the host talks could be a single IP or a network.

Figure 5: RAS Tunnel

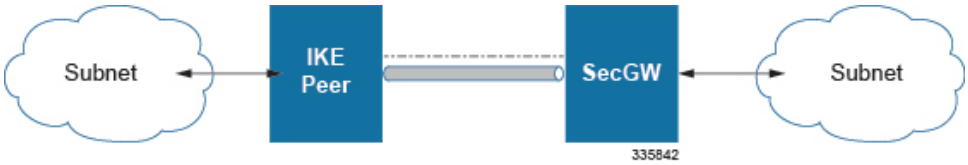
Site-to-Site Tunnels

In an S2S scenario, the remote peer sets up a child SA to the SecGW. The source of the traffic inside the child SA can be from multiple IP addresses on the remote peer's side. As in the remote access scenario, the addresses on the trusted network behind the SecGW can be a single IP or a network.

In this scenario also, the remote peer can setup multiple child SAs to the SecGW.

For S2S tunnels established using the WSG service, the TSi and TSr contain protocol as well as source and destination IP ranges.

Figure 6: S2S Tunnel



Packet Flow

The figures below indicate traffic packet flows to and from the SecGW.

Figure 7: SecGW Packet Flow – RAS

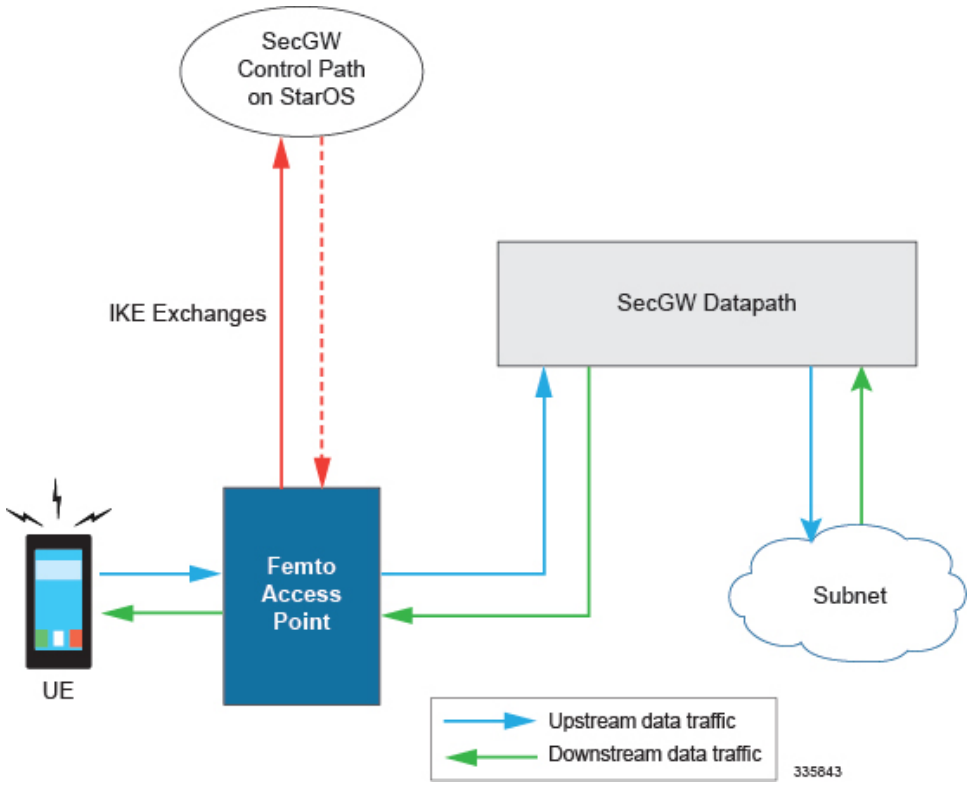
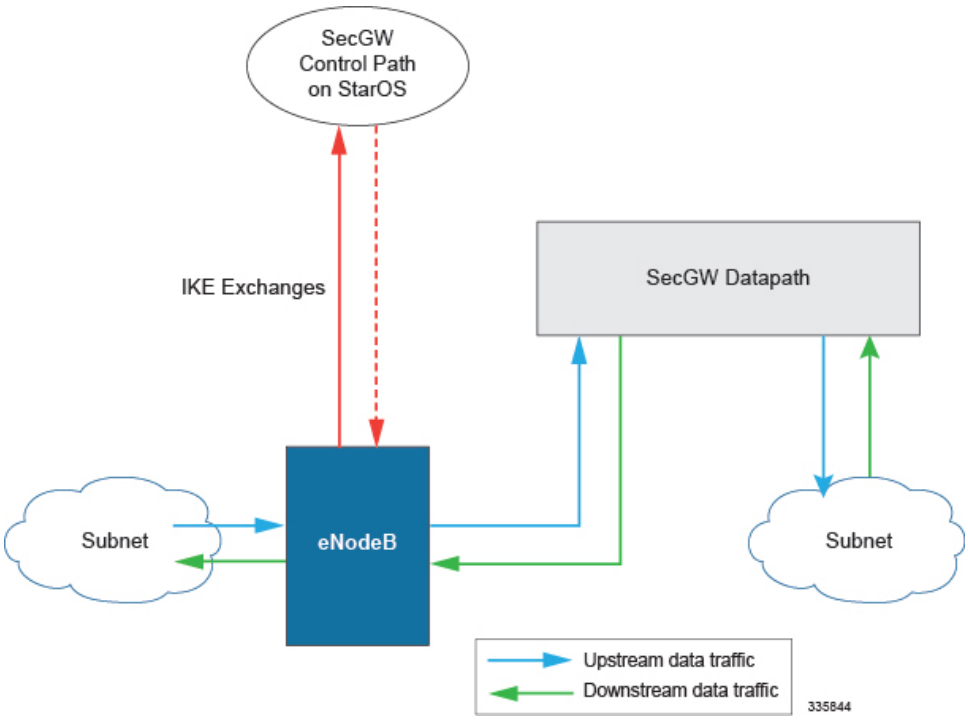


Figure 8: SecGW Packet Flow – S2S Scenario



Standards

Compliant

- RFC 1853 – IP in IP Tunneling
- RFC 2401 – Security Architecture for the Internet Protocol
- RFC 2402 – IP Authentication Header
- 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 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3554 – On the Use of Stream Control Transmission Protocol (SCTP) with IPsec [Partially compliant, ID_LIST is not supported.]
- RFC 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 4306 – Internet Key Exchange (IKEv2) Protocol
- RFC 4718 – IKEv2 Clarifications and Implementation Guidelines
- RFC 5996 – Internet Key Exchange Protocol Version 2 (IKEv2)
- Hashed Message Authentication Codes:
    - AES 96

- MD5
- SHA1/SHA2

- X.509 Certificate Support – maximum key size = 2048

Non-compliant

Standards

- RFC 3173 – IP Payload Compression Protocol (IPComp)
- RFC 5723 – Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption
- RFC 5840 – Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility
- RFC 5856 – Integration of Robust Header Compression over IPsec Security Associations

Hashed Message Authentication Codes

- HMAC AES 128 GMAC
- HMAC AES 192 GMAC
- HMAC AES 256 GMAC

Encryption Algorithms

- Diffie Hellman (DH) Group 17
- DH Group 18
- DH Group 19
- DH Group 20
- DH Group 21
- DH Group 24

Certificates

- Digital Signature Algorithm (DSA)
- xAuth