Cisco ASR 5000 Series Femto Network Gateway Administration Guide

Version 12.0

Last updated April 30, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24872-01

Cisco ASR 5000 Series Femto Network Gateway Administration Guide

CONTENTS

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
Femto Network Gateway Overview

This chapter contains general overview information about the Femto Network Gateway (FNG), including:

- Product Description
- Summary of FNG Features and Functions
- Product Specifications
- Network Deployment(s) and Interfaces
- Features and Functionality
- How the FNG Works
- Supported Standards

Product Description

The Cisco® ASR 5000 Chassis provides 3GPP mobile operators with a flexible solution that functions as a Femto Network Gateway (FNG) in CDMA2000 wireless voice and data networks. The FNG consists of new software for the ASR 5000.

The FNG enables mobile operators to provide 3G network services to subscribers with wireless handsets via Femtocell Access Points (FAPs). The FNG makes it possible for operators to provide secure access to the operator's 3G network from a non-secure network, extend wireless service coverage indoors, especially where access would otherwise be limited or unavailable, reduce the load on the macro wireless network, and make use of existing backhaul infrastructure to reduce the cost of carrying wireless calls.

The FNG functions as a security gateway that allows the FAPs in the access network to connect to circuit, packet, and IMS core networks. The FNG implements an IPSec interface to provide a secure, encrypted IPSec tunnel to each FAP in the access network as it connects to the operator's core network. In addition, the FNG provides a highly scalable femtocell solution by allowing a large number of FAPs to interoperate with legacy core network elements that are typically not designed to interface with such a large number of elements.

The FNG splits voice and data traffic flows into and out of the core network. It forwards all voice traffic to the operator's IMS core network and all data traffic to the PDSN/HA toward the packet data network. This network configuration fully isolates the traditional MSC from IP attacks, because all backhauled traffic is secure and offloaded to a convergence server in the IMS core network.

Summary of FNG Features and Functions

The FNG features and functions include:

- FNG service
- IKEv2 and IP Security (IPSec) encryption
- A12 aggregation
- X.509 certificate-based peer authentication
- RADIUS Support
- AAA server group selection
- FAP ID-based duplicate session detection
- Child SA rekey support
- Multiple Child SAs
- DoS protection cookie challenge
- IKEv2 keep-alive messages (dead peer detection)
- DSCP marking
- Custom DNS handling
- Session recovery support
- Congestion control
- Bulk statistics
- Threshold crossing alerts (TCAs)

Product Specifications

The following information is located in this section:

Licenses

The FNG is a licensed product. A session use license key must be acquired and installed to use the FNG service. For information about FNG licenses, contact your sales representative.

Hardware Requirements

Information in this section describes the hardware required to enable the FNG service.

Platforms

The FNG service operates on the ASR 5000.

Components

The following application and line cards are required to support FNG functionality on the ASR 5000:

- **System Management Cards (SMCs):** Provide full system control and management of all cards within the ASR 5000. Up to two SMCs can be installed; one active, one redundant.
- **Packet Services Cards (PSCs/PSC2s):** Provide high-speed, multi-threaded PDP context processing capabilities for 2.5G and 3G services. Up to 14 PSCs/PSC2s can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs):** Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management and for central office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Ethernet 10/100 and/or Ethernet 1000 Line Cards:** Installed directly behind PSCs/PSC2s, these cards provide the physical interfaces to elements in the operator's network. Up to 26 line cards can be installed for a fully

loaded system with 13 active PSCs/PSC2s, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs/PSC2s do not require line cards.

- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards and every PSC/PSC2 in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs/PSC2s.

Important: Additional information pertaining to each of the application and line cards required to support CDMA2000 wireless voice and data services is located in the "Hardware Platform Overview" chapter of the *Product Overview Guide*.

Operating System Requirements

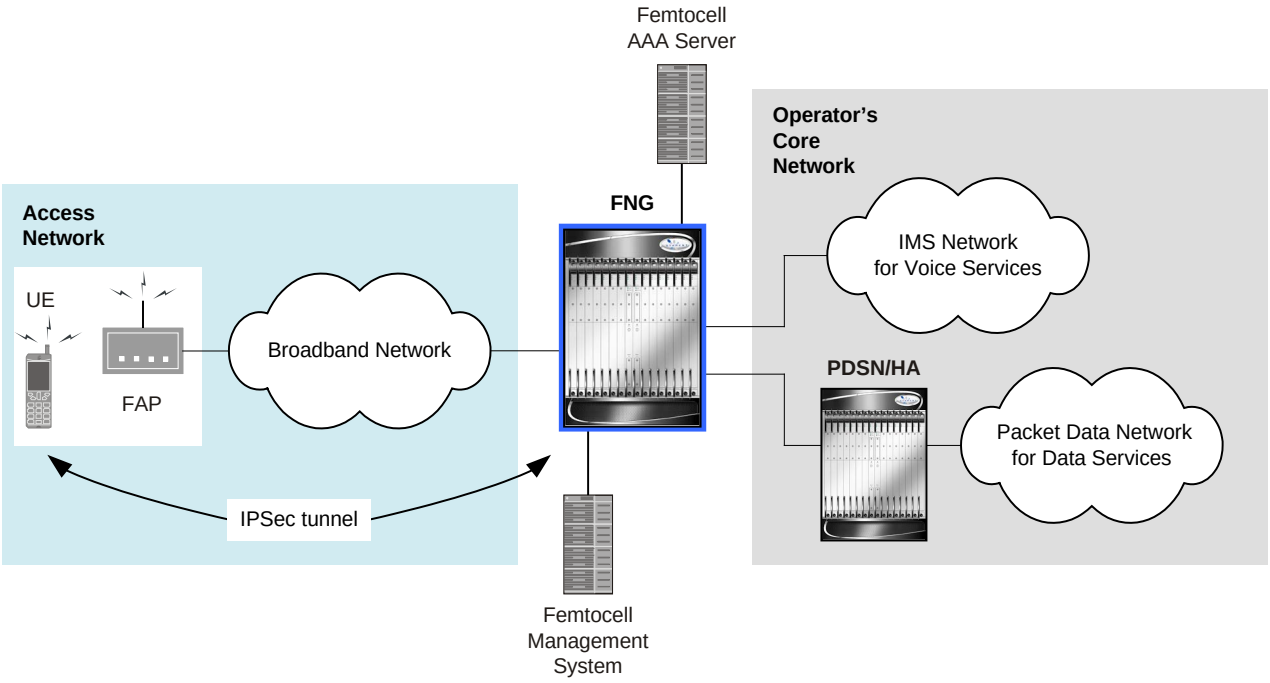
The FNG is available for the ASR 5000 running StarOS Release 10.0 or later.

Network Deployment(s) and Interfaces

This section describes the FNG as it functions in a CDMA2000 network.

The figure below shows how the FNG functions both as a security gateway and a femtocell gateway between the FAPs in the access network and the operator's IMS core network for voice services and the PDSN/HA and the packet data network for data services.

Figure 1. FNG Network Architecture



Network Elements

This section provides a description of the network elements in an FNG network.

Femtocell Access Point

The Femtocell Access Point (FAP) is a SIP-based CDMA2000 wireless access point that provides coverage in a small area, usually a private residence or small office, and connects the subscriber UEs to an operator's core network via a

broadband connection (e.g., DSL or cable). A FAP allows operators to extend wireless service coverage indoors, especially where access would otherwise be limited or unavailable.

Femtocell Management System

The Femtocell Management System (FMS) is a network element that resides in the operator's network and facilitates the provisioning, activation, and operational management of the FAPs in the network based on industry standards such as TR-069. The FMS helps to ensure the scalability of the FAP network to potentially millions of devices.

Femto Network Gateway

The Femto Network Gateway (FNG) is a network element that resides in the operator's network and functions as both a security gateway and a femtocell gateway. The security gateway functions provide secure access for the FAPs to access services within the operator's core network. The femtocell gateway functions provide aggregation and proxy capabilities for the FAPs. The FNG forwards all voice traffic to the operator's IMS core network and all data traffic to the PDSN/HA.

Femtocell AAA Server

The Femtocell AAA Server provides a FAP authorization function. It sends authorization policy information to the FNG.

IMS Core Network Elements

An operator's IMS core network may include the following elements to enable voice services:

- **P-CSCF:** The P-CSCF (Proxy Call/Session Control Function) is the entry point into the IMS domain and serves as the outbound proxy server for SIP messaging for the subscriber UEs. The UEs attach to the P-CSCF prior to performing IMS registrations and initiating SIP sessions. All SIP signaling traffic to and from the FAPs and the IMS core is handled by the P-CSCF. The P-CSCF provides message manipulation, breakout of emergency call services, QoS (Quality of Service) authorization, and signaling compression. Once the P-CSCF completes all of the functions for which it is responsible, it forwards the call to the I-CSCF.
- **I-CSCF:** The I-CSCF (Interrogating Call/Session Control Function) functions as a location server in the IMS core network. Its major functions are to select the appropriate registrar server for the subscriber UEs by consulting the HSS (Home Subscriber Server) and forwarding the request to the IMS registrar (the S-CSCF). The HSS returns a set of required S-CSCF capabilities for initial registration requests by the UE. Based on these capabilities, the I-CSCF selects the appropriate S-CSCF.
- **S-CSCF:** The S-CSCF (Serving Call/Session Control Function) provides session control and registration services for the subscriber UEs and FAPs in the network. It is responsible for all aspects of session control, handling all subscriber requests, which it relays to the appropriate application server. The S-CSCF routes mobile-terminating traffic to the P-CSCF and routes mobile-originating traffic to the convergence server based on iFC (initial Filter Criteria) downloaded from the HSS.

- **HSS:** The HSS (Home Subscriber Server), is the master user database that supports the IMS network entities that handle calls. It contains subscription-related information (subscriber profiles), performs authentication and authorization of the user, and provides information about the subscriber's location and IP information.
- **Femtocell Convergence Server:** The Femtocell Convergence Server (FCS) is an IMS application server that provides legacy Telephony Application Services (TAS) to 1x femtocell subscribers via SIP, including voice services and voice feature delivery. The femtocell convergence server also manages idle and active mode mobility for 1x subscribers as they move into and out of range of FAP coverage. It functions as an MFIF (MAP-Femtocell Interworking Function) and interfaces with the HLR for 1x subscriber authentication. It appears as an IMS application server to the S-CSCF and as a serving MSC to the HLR.
- **Media Gateway:** The Media Gateway terminates bearer channels from the circuit-switched network and media streams from the packet-switched network. It can support media conversion, bearer control, and payload processing (e.g., using codecs, echo cancellers, and conference bridges).

PDSN/HA

The PDSN/HA enables femtocell subscribers to receive packet data services in the mobile operator's core network. In most cases, these services are the same as those available via the mobile operator's macro network.

Basic Operation

When a FAP powers up, it uses DNS resolution to resolve its pre-configured FQDN of the FNG and obtain the FNG's IP address. It then initiates IPSec tunnel establishment over the broadband access network. The IPSec tunnel terminates at the FNG.

The FAP receives an IPv4 address known as the Tunnel Inner Address (TIA) from the FNG during the first IPSec tunnel establishment. The FNG assigns the TIA from its own IPv4 address pool. Once an IPSec tunnel is established, the FAP uses the TIA in all its SIP messages and to obtain configuration data from its FMS. The FNG is agnostic in regard to the protocol used between the FAP and its FMS, and simply forwards packets between the FAP and the FMS over the secure connection.

The 1x FAP performs P-CSCF discovery via a DHCP server per RFC 3319, or it may receive the IP address of the P-CSCF from the FMS. Once the FAP gets the P-CSCF address, it initiates SIP registration with the IMS core network. When a UE attaches to the FAP, it performs 1x registration with the IMS core network.

Network Interfaces

The following table provides descriptions of the network interfaces supported by the FNG in a CDMA2000 network.

Table 1. Network Interfaces in a CDMA2000 Network

Interface	Description

Interface	Description
FAP Interface	The secure interface to the FAPs in the network is an IPSec tunnel. The FNG uses IKEv2 for establishing the IPSec tunnel. Note that the FNG does not have a direct interface to the UEs in the network. The FNG receives all voice and data traffic from the UEs via secure IPSec tunnels between the FNG and the FAPs and sends the traffic to the operator's IMS core or PDSN/HA.
RADIUS Interface	The interface to the RADIUS server is used for FAP device authentication. The FAP can use one of the following authentication methods: • EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) authentication • PSK (Pre-Shared Key) authentication • X.509 certificate-based peer (client) authentication
Interface with the IMS Core	The FNG sends all SIP signaling and bearer traffic from the FAPs to the IMS core to access voice services.
Interface with the PDSN/HA	The FNG sends all signaling and bearer traffic from the FAPs to the PDSN/HA to access packet data services.

Features and Functionality

This section describes the features and functions supported by the FNG.

The following features are supported and described in this section:

- FNG Service
- IKEv2 and IP Security (IPSec) Encryption
- X.509 Certificate-based Peer Authentication
- A12 Aggregation
- RADIUS Support
- AAA Server Group Selection
- FAP ID-based Duplicate Session Detection
- Child SA Rekey Support
- Multiple Child SAs
- DoS Protection Cookie Challenge
- IKEv2 Keep-Alive Messages (Dead Peer Detection)
- DSCP Marking
- Custom DNS Handling
- Session Recovery Support
- Congestion Control
- Bulk Statistics
- Threshold Crossing Alerts

FNG Service

The FNG service and its associated processes enable the system to function as a femtocell gateway. The FNG service enables the FAPs in the network to connect to the core network elements via a secure IPSec interface. During configuration, you create the FNG service in an FNG context, which is a routing domain on the ASR 5000. FNG context and service configuration includes the following main steps:

- **Configure the IPv4 address for the service:** This is the IP address of the FNG to which the FAPs in the network attempt to connect, sending IKEv2 messages to this IP address to establish IPSec tunnels.
- **Configure the name of the crypto template for IKEv2/IPSec:** A crypto template is used to configure an IKEv2/IPSec policy. It includes most of the IKEv2 and IPSec parameters for keep-alive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per FNG service.

- **The name of the EAP profile:** This profile defines the EAP authentication method and associated parameters. If the PSK (Pre-Shared Key) authentication method is used, this configuration is not needed.
- **IKEv2 and IPSec transform sets:** Transform sets define the negotiable algorithms for IKE SAs and Child SAs to enable calls to connect to the FNG.
- **The setup timeout value:** This parameter specifies the session setup timeout timer value. The FNG terminates a connection attempt if the FAP does not establish a successful connection within the specified timeout period.
- **Max-sessions:** This parameter sets the maximum number of subscriber sessions allowed by this FNG service.
- **FNG supports a domain template for storing domain-related configuration:** The domain name is taken from the received Network Address Identifier (NAI) and searched in the domain template database.
- **Duplicate session detection parameters:** The FNG supports the FAP ID in the form of an NAI for duplicate session detection. This setting enables duplicate session detection for the FNG service.

When the FNG service is configured in the system with the IP address, crypto template, and so on, the FNG is ready to accept IKEv2 control packets for establishing IKEv2 sessions.

IKEv2 and IP Security (IPSec) Encryption

The FNG supports IKEv2 and IPSec encryption using IPv4 addressing. IKEv2 and IPSec encryption enables network domain security for all IP packet-switched networks in order to provide confidentiality, integrity, authentication, and anti-replay protection.

At the beginning of IKEv2 session setup, the FNG and the FAP exchange capabilities for authentication. IKEv2 and IPSec transform sets configured in the crypto template define the negotiable algorithms for IKE SA and Child SA setup to connect calls to the FNG by creating a single IPSec tunnel, called the Tunnel Inner Address (TIA), which is intended for user traffic coming from the FAP. There can be multiple UEs connecting to a single FAP at the same time, and the traffic from all of the connected UEs passes through the same IPSec tunnel. The FAP to which a UE is connected can request one of the following authentication methods:

- EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) authentication
- PSK (Pre-Shared Key) authentication
- X.509 certificate-based peer (client) authentication

The FNG partially supports the EAP MD5 (Extensible Authentication Protocol Message-Digest 5) authentication method.

X.509 Certificate-based Peer Authentication

In addition to the EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) and PSK (Pre-Shared Key) peer authentication methods, the FNG supports X.509 certificate-based peer authentication.

The FNG checks the network policy on whether a FAP is authorized to provide service. If the network policy states that all FAPs that pass device authentication are authorized to provide service, no further authorization check may be required. If the network policy requires that each FAP be individually authorized for service (in the case where the FEID is associated with a valid subscription), the FNG sends a RADIUS Access-Request message to the AAA server. If the AAA server sends a RADIUS Access-Accept message, the FNG proceeds with device authentication. Otherwise, the FNG terminates the IPSec tunnel setup by sending an IKEv2 Notification message indicating authentication failure.

For a detailed presentation of X.509 certificate-based peer authentication, see the section *How the FNG Works* later in this chapter.

A12 Aggregation

The Access Network AAA (AN-AAA) servers in 1x networks are not designed to handle a large numbers of FAPs attempting A12 authentication to access the network. The A12 aggregation feature reduces the number of source addresses in the A12 Access-Request messages sent to the AN-AAA servers by the FNG, which simplifies the configuration of the AN-AAA server's database.

A12 authentication is a CHAP-based authentication method used by CDMA2000 AN-AAA servers to provide High Rate Packet Data (HRPD) access authentication between the AN function in the FAPs and the AN-AAA servers in the network.

When the FNG receives an A12 Access-Request message from a FAP, it validates the source address of the FAP, then substitutes the source address (and, optionally, the NAS IP address/port number) in the Access-Request message with its own source address before sending the message to the AN-AAA server. When the FNG receives the Access-Accept message from the AN-AAA server, the FNG sends it back to the FAP. In this way, the number of AAA sessions required by the AN-AAA server is reduced.

RADIUS Support

RADIUS support on the FNG provides a mechanism for performing authentication, authorization, and accounting (AAA) for subscribers. The benefits of using AAA are:

- Higher flexibility for subscriber access control
- Better accounting, charging, and reporting options
- Industry standard RADIUS authentication

The Remote Authentication Dial-In User Service (RADIUS) protocol can be used to provide AAA functionality for subscribers. The AAA functionality on the FNG provides a wide range of configuration options via AAA server groups, which allow a number of RADIUS parameters to be configured in support of the FNG service.

Currently, two types of authentication load-balancing methods are supported: first-server and round-robin. The first-server method sends requests to the highest priority active server. A request will be sent to a different server only if the highest priority server is not reachable. With the round-robin method, requests are sent to all active servers in a round-robin fashion.

The FNG can detect the status of the AAA servers. Status checking is enabled by configuration in the AAA Server Group Configuration Mode of the system’s CLI. Once an AAA server is detected to be down, it is kept in the down state up to a configurable duration of time called the dead-time period. After the dead-time period expires, the AAA server is eligible to be retried. If a subsequent request is directed to that server and the server properly responds to the request, the system makes the server active again.

Important: For more information on RADIUS AAA configuration, refer to the *AAA Interface Administration and Reference.*

AAA Server Group Selection

This feature provides a maximum of 64 AAA groups on the ASR 5000. This could be spread across multiple contexts or all groups can be configured within a single context. A maximum of 320 RADIUS servers is allowed on the chassis, unless the **aaa-large-configuration** command is issued, and this number becomes a maximum of 800 AAA groups and 1600 RADIUS servers allowed to be configured per chassis.

FAP ID-based Duplicate Session Detection

When this feature is enabled and a FAP sets up a new session, the FNG automatically checks for any remnants of abandoned calls, and if found, clears them. Clearing the old session and establishing the new session in parallel optimizes FNG processing functions.

With every new session setup, the FNG verifies whether there are any old sessions that are bound to the Femtocell Access Point Identifiers (FAP IDs). For example, when a FAP reboots, it may initiate a new session with the FNG. After authentication, if the FNG detects an old session with the same FAP ID, the FNG clears the old IPSec tunnel and establishes a new IPSec tunnel with the FAP. This feature is designed with the assumption that not more than one call with duplicate FAP IDs is in the setup stage at any one time.

You enable FAP ID-based duplicate session detection in the FNG Service Configuration Mode of the system's CLI. This feature should be enabled in the boot-time configuration before any calls are established.

Tunnel Cleanup on FAP Reboot

The FNG supports initial contact handling in IKE_AUTH messages as per RFC 4306 and cleans up the original tunnel if a FAP initiates a new tunnel after a reboot. The CLI command for duplicate session detection is not needed to enable this detection. Initial contact notification asserts that this IKE_SA is the only IKE_SA currently active between the authenticated identities. It may be sent when an IKE_SA is established after a crash, and the recipient may use this information to delete any other IKE_SAs it has for the same authenticated identity without waiting for a timeout.

Child SA Rekey Support

Rekeying of an IKEv2 Child Security Association (SA) occurs for an already established Child SA whose lifetime (either time-based or data-based) is about to exceed a maximum limit. The FNG initiates rekeying to replace the existing Child SA. During rekeying, two Child SAs exist momentarily (500ms or less) to ensure that transient packets from the original Child SA are processed by the FNG and not dropped.

FNG-initiated Child SA rekeying is disabled by default, and rekey requests are ignored. You can enable this feature in the Crypto Configuration Payload Mode of the system's CLI.

Multiple Child SAs

The FNG supports the instantiation, termination, and rekeying of multiple simultaneous Child SAs derived from an IKE SA, as defined in RFC 4306.

As specified in the IKEv2 policy, which controls the behavior of encrypted tunnels, the first Child SA is instantiated during the IKE_AUTH exchange between the FAP and the FNG, and any additional Child SAs are instantiated during subsequent CREATE_CHILD_SA exchanges that may occur between the FAP and the FNG.

An IKEv2 policy may be terminated via operator intervention or be terminated when a service is terminated. In these scenarios, all objects derived from the IKEv2 policy, including the IKE SA and all Child SAs, are terminated.

The FNG maintains two maximum Child SA values per IKEv2 policy. The first is a system-enforced maximum value, which is four Child SAs per IKEv2 policy. The second is a configurable maximum value, which can be a value between one and four, and which is specified via the system's CLI in the Crypto Template Configuration Mode.

If the system maximum value or the configured maximum value is reached and the FNG receives a CREATE_CHILD_SA Request for an additional Child SA, the FNG returns a CREATE_CHILD_SA Response that contains a Notify payload of the type NO_ADDITIONAL_SAS. Note that the maximum value does not apply to interim Child SAs that may exist during transitional phases such as during Child SA rekeying. For example, if a maximum of two simultaneous Child SAs are specified, the FNG allows a burst of four during Child SA rekeying.

DoS Protection Cookie Challenge

There are several known types of Denial of Service (DoS) attacks associated with IKEv2. Through a configurable option in the Crypto Template Configuration Mode in the system's CLI, the FNG can implement the IKEv2 cookie challenge payload method per RFC 4306. This method is intended to protect against the FNG creating too many half-opened sessions or other similar mechanisms.

This feature is disabled by default. When enabled, and when the number of half-opened IPSec sessions exceeds the configured limit of any integer between 0 and 100,000 (or the trigger point with other detection mechanisms), the FNG invokes the cookie challenge payload mechanism to insure that only legitimate subscribers are initiating IKEv2 tunnel requests, as follows:

1. The FAP connects to the FNG and sends an IKE_SA_INIT Request message.
2. The FNG sends a Notify (cookie) payload to the FAP to request retransmission of the IKE_SA_INIT Request message with the received Notify (cookie) payload in the message.
3. Upon receipt of the retransmitted message, the FNG verifies the cookie payload and ensures that it is the same cookie payload as the one it had sent.
4. If the cookie challenge is met, setup continues as normal with the FNG sending an IKE_SA_INIT Response message.

IKEv2 Keep-Alive Messages (Dead Peer Detection)

The FNG supports IKEv2 keep-alive messages, also known as Dead Peer Detection (DPD), originating from both the FAPs and the FNG. You configure DPD per FNG service. You can also disable DPD, and the FNG will not initiate

DPD exchanges with the FAPs. However, the FNG always responds to DPD availability checks initiated by a FAP regardless of the FNG configuration.

DSCP Marking

If different classes of traffic are sent on the same SA and if the FAPs in the network and the FNG are employing the optional anti-replay feature in the Encapsulating Security Payload (ESP), this could result in inappropriate discarding of lower priority packets due to the windowing mechanism used by this feature. Therefore, it is recommended that multiple Child SAs are used to provide the appropriate QoS services. This handling can be applied to different types of traffic (voice and data) coming from the same UE behind a FAP, or from multiple UEs belonging to the same QoS class. The FNG will determine the traffic type and provide a QoS treatment based on configured rules.

Custom DNS Handling

The custom DNS feature provides a mechanism whereby the FNG sends the DNS address specified in the FNG configuration file to the FAP only if the FAP requests it. The FNG considers an address of 0.0.0.0 invalid and does not include it.

Session Recovery Support

The session recovery feature is a licensed feature on the FNG. It provides seamless failover and nearly instantaneous reconstruction of subscriber session information in the event of a hardware or software fault within the same chassis, preventing a fully-connected user session from being dropped. For information about the required software license for this feature, contact your sales representative.

Session recovery is performed by mirroring key software processes (the IPSec manager, session manager, and AAA manager, for example) on the FNG. These mirrored processes remain in an idle state (in standby mode), where they perform no processing until they may be needed in the case of a software failure (a session manager task aborts, for example). The system spawns new instances of standby mode sessions and AAA managers for each active control processor being used.

Additionally, other key system-level software tasks such as VPN manager are performed on a physically separate PSC/PSC2 to ensure that a double software fault (the session manager and the VPN manager fail at same time on same card, for example) cannot occur. The PSC/PSC2 used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

Important: For more information about session recovery support, refer to the *System Administration Guide*.

Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

The congestion control feature monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are resolved quickly. However, continuous or large numbers of these conditions within a specific time interval may have an impact on the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the *Thresholding Configuration Guide*. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated. A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.
- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
- **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

Important: For more information on congestion control, refer to the *System Administration Guide*.

Bulk Statistics

Bulk statistics allow operators to choose to view not only statistics that are of importance to them, but to also configure the format in which they are presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics and send them to a collection server called a receiver. Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. The following is a partial list of supported schemas:

- **System:** Provides system-level statistics.
- **Card:** Provides card-level statistics.
- **Port:** Provides port-level statistics.
- **FNG:** Provides FNG service statistics.

The system supports the configuration of up to four sets (primary/secondary) of receivers. Each set can be configured to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for headers and footers only), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics Server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

Important: For more information on bulk statistic configuration, refer to the "Configuring and Maintaining Bulk Statistics" chapter of the *System Administration Guide*.

Threshold Crossing Alerts

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outages. Typically, these conditions are temporary (i.e., high CPU utilization or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to avoid and/or minimize system downtime.

The system supports threshold crossing alerts for certain key resources such as CPU, memory, IP pool addresses, and so on. With this capability, the operator can configure a threshold on these resources whereby, should the resource depletion cross the configured threshold, an SNMP trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated, then generated and/or sent again at the end of the polling interval.
- **Alarm:** Both high and low thresholds are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated, then generated and/or sent again at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP Traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Generation of specific traps can be enabled or disabled on the chassis, ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a thresholding facility for which active and event logs can be generated. As with other system facilities, logs are generated messages pertaining to the condition of a monitored value are generated with a severity level of WARNING. Logs are supported in both Alert and Alarm modes.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered outstanding until a condition no longer exists or a condition clear alarm is generated. Outstanding alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

Important: For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide.*

How the FNG Works

This section describes the FNG functioning as a security gateway during IPSec tunnel establishment.

IPSec Tunnel Establishment

The figure below shows the message flow during IPSec tunnel establishment. The table that follows the figure describes each step in the message flow.

Figure 2. IPSec Tunnel Establishment

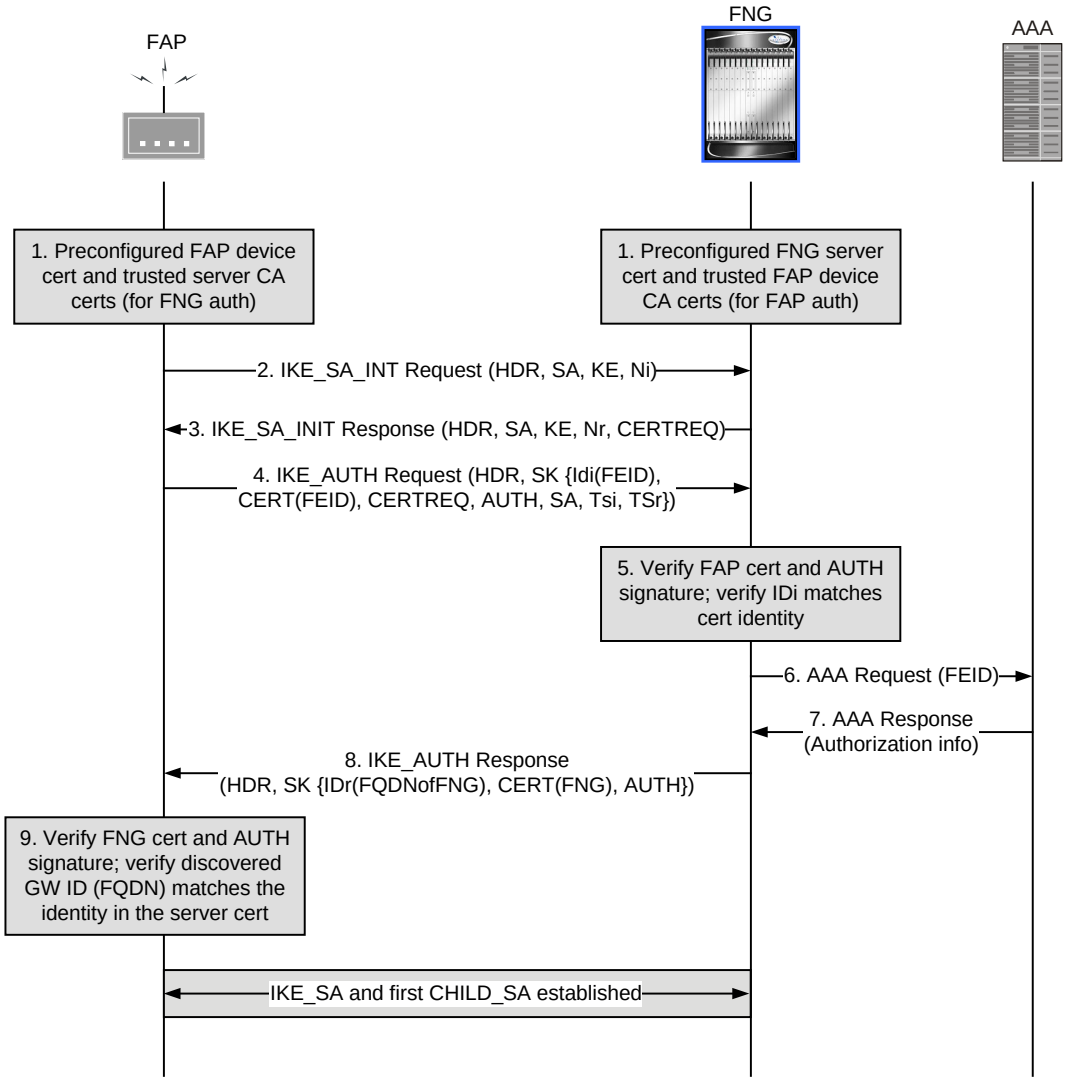


Table 2. IPSec Tunnel Establishment

Step	Description
1.	The FAP is assigned a device certificate during it's manufacturing. The private key for the certificate is stored securely at the FAP. Similarly, the FNG is assigned a server certificate. The FNG is also configured with a list of root CA certificates corresponding to the trusted device CA certificates.
2.	The FAP initiates an IKEv2 exchange with the FNG, known as the IKE_SA_INIT exchange, by issuing an IKE_SA_INIT Request to negotiate cryptographic algorithms, exchange nonces, and perform a Diffie-Hellman exchange with the FNG.
3.	The FNG responds with an IKE_SA_INIT Response by choosing a cryptographic suite from the initiator's offered choices, completing the Diffie-Hellman and nonce exchanges with the FAP. In addition, the FNG includes the list of FAP CA certificates that it will accept in its CERTREQ payload. For successful FAP authentication, the CERTREQ payload has to contain at least one CA certificate that is in the trust chain of the FAP device certificate. At this point in the negotiation, the IKE_SA_INIT exchange is complete and all but the headers of all the messages that follow are encrypted and integrity-protected.
4.	The FAP initiates an IKE_AUTH exchange with the FNG by setting the IDi payload to the FEID, the CERT payload set to the FAP device certificate corresponding to the FEID, and the AUTH payload containing the signature of the previous IKE_SA_INIT Request message (in step 2) generated using the private key of the FAP device certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload.
5.	Using the CA certificate corresponding to the FAP device certificate, the FNG first verifies that the FAP device certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to the identity in the FAP device certificate. If the verification is successful, using the public key of the FAP device certificate, the FNG generates the expected AUTH payload and compares it with the received AUTH payload. If they match, the authentication of the FAP is successful. Otherwise, the FNG sends an IKEv2 Notification message indicating authentication failure.
6.	If the network policy requires femtocell subscription authorization, the FNG contacts the AAA server to verify that the FAP identified by the FEID is authorized to provide service.
7.	The AAA server responds with the authorization result. If the authorization is not successful, the FNG sends an IKEv2 Notification message indicating authorization failure. Otherwise, the FNG proceeds with server authentication.
8.	The FNG responds with the IKE_AUTH Response by setting the IDr payload to the FQDN of the FNG, setting the CERT payload to the FNG server certificate corresponding to the FQDN, and including the AUTH payload containing the signature of the IKE_SA_INIT Response message (in step 3) generated using the private key of the FNG server certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload.
9.	Using the CA certificate corresponding to the FNG server certificate, the FAP first verifies that the FNG server certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to the identity in the server certificate and contains the expected FNG value as discovered during the FNG discovery procedures. If the verification is successful, using the public key of the FNG server certificate, the FAP generates the expected AUTH payload and compares it with the received AUTH payload. If they match, the FNG server authentication is successful. This completes the IKE_AUTH exchange. An IPSec SA with the first CHILD_SA pair is established between the FAP and the FNG.

IPSec Tunnel Establishment with EAP-AKA Authentication

The figure below shows the message flow during IPSec tunnel establishment with EAP-AKA authentication. The table that follows the figure describes each step in the message flow.

Figure 3. IPSec Tunnel Establishment with EAP-AKA Authentication

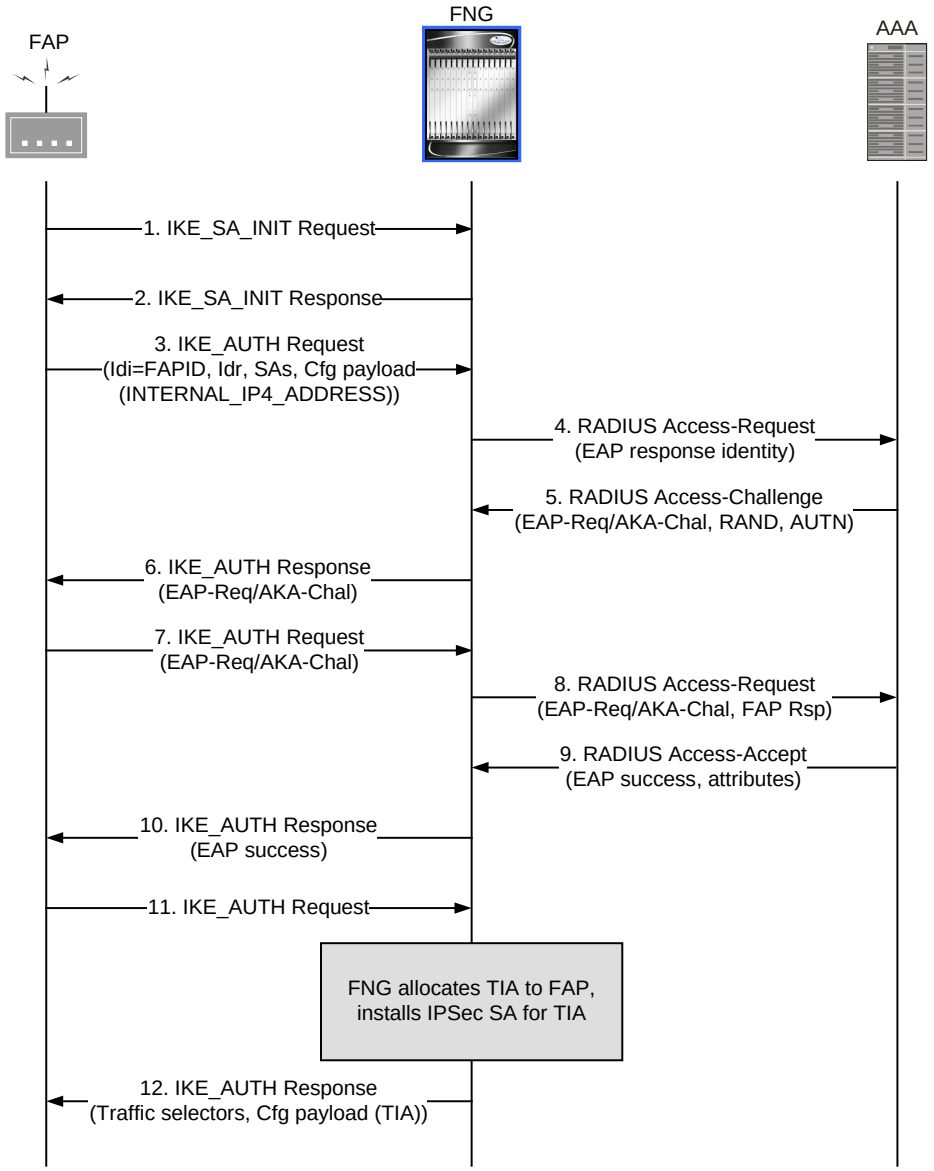


Table 3. IPSec Tunnel Establishment with EAP-AKA Authentication

Step	Description
1.	The FAP initiates an IKEv2 exchange with the FNG, known as the IKE_SA_INIT exchange, by issuing an IKE_SA_INIT Request to negotiate cryptographic algorithms, exchange nonces, establish NAT traversal, and perform a Diffie-Hellman exchange with the FNG.
2.	The FNG responds with an IKE_SA_INIT Response by choosing a cryptographic suite from the initiator's offered choices, completing the Diffie-Hellman and nonce exchanges with the FAP.

Step	Description
3.	The FAP initiates an IKE_AUTH exchange with the FNG. The FAP omits the AUTH payload, indicating that it wants to use an EAP exchange over IKEv2. The FAP includes its identity in the IDi payload of the IKE_AUTH Request. The IDi is set to the FAP ID. The FAP ID is a string in the format id@domain. The FAP also includes the IKEv2 CFG_REQUEST payload in the IKE_AUTH Request. The INTERNAL_IP4_ADDRESS attribute is included in the CFG_REQUEST payload with the length set to 0.
4.	The FNG receives the IKE_AUTH Request and sends the FAPID as the EAP Response identity to the AAA server using a RADIUS Access-Request message with an EAP-Message attribute.
5.	The AAA server verifies the FAP's identity and generates a random value RAND and AUTN based on the shared CHAP-key and a sequence number. The AAA server sends the EAP-Request/AKA-Challenge to the FNG via a RADIUS Access-Challenge message. The EAP-Request/AKA-Challenge contains the RAND and AUTN to protect the integrity of the EAP message.
6.	The FNG sends an IKE_AUTH Response to the FAP that contains the EAP-Request/AKA-Challenge message received from the AAA server.
7.	The FAP verifies the authentication parameters in the EAP-Request/AKA-Challenge message and if the verification is successful, it responds to the challenge with an IKE_AUTH Request message to the FNG.
8.	The FNG forwards the EAP-Response/AKA-Challenge message to the AAA server via a RADIUS Access-Request message.
9.	If the authentication is successful, the AAA server sends a RADIUS Access-Accept message with an EAP-Message attribute containing EAP Success. The AAA server sends the EAP Success and the MSK generated during the EAP-AKA authentication process to the FNG. In addition, the AAA server also sends other attributes that it normally sends to the PDSN for a simple IP session. These attributes include at a minimum the Framed-Pool (if required), so that the FNG can assign a TIA from the correct IP address pool, the Session-Timeout, and the Idle-Timeout.
10.	The FNG forwards the EAP Success message to the FAP in an IKE_AUTH Response message.
11.	The FAP calculates the MSK according to RFC 4187 and uses it as an input to generate the AUTH payload to authenticate the first IKE_SA_INIT message. The FAP sends the AUTH payload to the FNG in an IKE_AUTH Request message.
12.	The FNG uses the MSK to check the validity of the AUTH payload received from the FAP and calculates its own AUTH payload for the FAP to verify per RFC 4306. The FNG sends the AUTH payload to the FAP together with the configuration payload containing SAs and the rest of the IKEv2 parameters in an IKE_AUTH Response message. This completes the IKEv2 negotiation. The configuration payload contains the TIA. It is up to the FAP implementation to establish separate Child SAs for configuration management and VoIP traffic, or to use the same Child SA for all traffic types. The FNG supports both options. Once the IPSec tunnel is established, the FAP uses the TIA assigned by the FNG for each 1x UE (in the SIP headers or as the RTP IP address).

X.509 Certificate-based Peer Authentication

The figure below shows the message flow during X.509 certificate-based peer authentication. The table that follows the figure describes each step in the message flow.

Figure 4. X.509 Certificate-based Peer Authentication

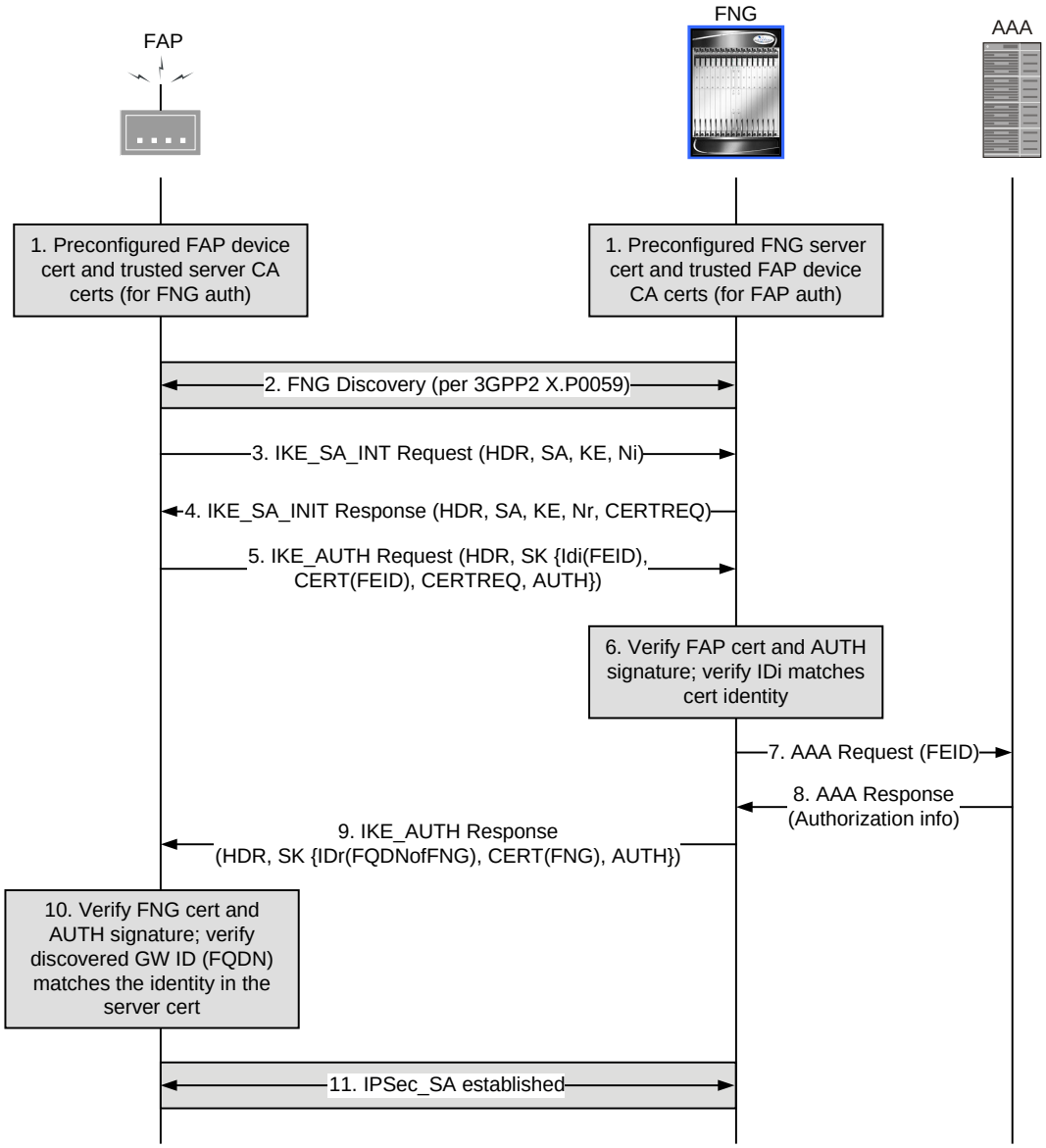


Table 4. X.509 Certificate-based Peer Authentication

Step	Description
1.	The FAP is assigned a device certificate during it's manufacturing. The FAP device certificate is signed by a Certificate Authority (device certificate CA) trusted by the operator. The private key for the certificate is stored securely at the FAP. Similarly, the FNG is assigned a server certificate. The private key of the FNG is stored securely at the FNG. In addition, the FNG is configured with a list of root CA certificates corresponding to the trusted device certificate CAs. The FAP is also configured with a list of root CA certificates corresponding to the server certificates that the FAP will accept from the FNG.

Step	Description
2.	Upon FAP power-up, using the FNG discovery procedures such as DNS discovery, the FAP determines the FQDN/IP address of the appropriate FNG.
3.	The FAP initiates an IKEv2 exchange with the FNG, known as the IKE_SA_INIT exchange, by issuing an IKE_SA_INIT Request to negotiate cryptographic algorithms, exchange nonces, and perform a Diffie-Hellman exchange with the FNG. In addition, using the NAT Traversal procedures, the FAP includes NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP payloads to negotiate support for UDP encapsulation.
4.	The FNG responds with an IKE_SA_INIT Response by choosing a cryptographic suite from the initiator's offered choices, completing the Diffie-Hellman and nonce exchanges with the FAP. In addition, the FNG includes the list of FAP CA certificates that it will accept in its CERTREQ payload. For successful FAP authentication, the CERTREQ payload must contain at least one CA certificate that is in the trust chain of the FAP device certificate. At this point in the negotiation, the IKE_SA_INIT exchange is complete and all but the headers of all the messages that follow are encrypted and integrity-protected.
5.	The FAP initiates an IKE_AUTH exchange with the FNG by setting the IDi payload to the FEID in FQDN format (from the subjectAltName extension of the FAP certificate), setting the CERT payload to the FAP device certificate corresponding to the FEID, and including the AUTH payload containing the signature of the previous IKE_SA_INIT Request message (in step 3) generated using the private key of the FAP device certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload. The FAP also includes the CERTREQ payload containing the list of SHA-1 hash algorithms for server authentication. For successful server authentication, the CERTREQ payload must contain at least one CA certificate that is in the trust chain of the FNG server certificate.
6.	Using the CA certificate corresponding to the FAP device certificate, the FNG first verifies that the FAP device certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to the identity in the FAP device certificate. If the verification is successful, using the public key of the FAP device certificate, the FNG generates the expected AUTH payload and compares it with the received AUTH payload. If they match, the authentication of the FAP is successful. Otherwise, the FNG sends an IKEv2 Notification message indicating authentication failure.
7.	If the network policy requires femtocell subscription authorization, the FNG contacts the AAA server to verify that the FAP identified by the FEID is authorized to provide service.
8.	The AAA server responds with the authorization result. If the authorization is not successful, the FNG sends an IKEv2 Notification message indicating authorization failure. Otherwise, the FNG proceeds with server authentication.
9.	The FNG responds with the IKE_AUTH Response by setting the IDr payload to the FQDN (or IP address) of the FNG, setting the CERT payload to the FNG server certificate corresponding to the FQDN (or IP address), and including the AUTH payload containing the signature of the IKE_SA_INIT Response message (in step 4) generated using the private key of the FNG server certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload.
10.	Using the CA certificate corresponding to the FNG server certificate, the FAP first verifies that the FNG server certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to the identity in the server certificate and contains the expected FNG value as discovered during the FNG discovery procedures. If the verification is successful, using the public key of the FNG server certificate, the FAP generates the expected AUTH payload and compares it with the received AUTH payload. If they match, FNG server authentication is successful. This completes the IKE_AUTH exchange.
11.	An IPSec SA is established between the FAP and the FNG. If more IPSec SAs are needed, either the FAP or the FNG can initiate the creation of additional Child SAs using a CREATE_CHILD_SA exchange.

Supported Standards

The FNG service complies with the following standards:

- 3GPP2 References
- IETF References

3GPP2 References

- 3GPP2 X.S0059-000-0 (V1.0): “cdma2000 Femtocell Network: Overview”.
- 3GPP2 X.S0059-100-0 (V1.0): “cdma2000 Femtocell Network: Packet Data Network Aspects”.
- 3GPP2 X.P0059-200-0_v0.C_1x_Femto_R&F.pdf

IETF References

- RFC 2401 (November 1998): “Security Architecture for the Internet Protocol”.
- RFC 2402 (November 1998): “IP Authentication Header”.
- RFC 2403 (November 1998): “The Use of HMAC-MD5-96 within ESP and AH”.
- RFC 2404 (November 1998): “The Use of HMAC-SHA1-96 within ESP and AH”.
- RFC 2405 (November 1998): “The ESP DES-CBC Cipher Algorithm With Explicit IV”.
- RFC 2406 (November 1998): “IP Encapsulating Security Payload (ESP)”.
- RFC 2410 (November 1998): “The NULL Encryption Algorithm and Its Use With IPsec”.
- RFC 3168 (September 2001): “The Addition of Explicit Congestion Notification (ECN) to IP”.
- RFC 3526 (May 2003): “More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)”.
- RFC 3602 (May 2003): “The AES-CBC Cipher Algorithm and Its Use with IPsec”.
- RFC 3706 (February 2004): “A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers”.
- RFC 3715 (March 2004): “IPsec-Network Address Translation (NAT) Compatibility Requirements”.
- RFC 3748 (June 2004): “Extensible Authentication Protocol (EAP)”.
- RFC 3947 (January 2005): “Negotiation of NAT-Traversal in the IKE”.
- RFC 3948 (January 2005): “UDP Encapsulation of IPsec ESP Packets”.
- RFC 4187 (January 2006): “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”.
- RFC 4306 (December 2005): “Internet Key Exchange (IKEv2) protocol”.

- RFC 4308 (December 2005): “Cryptographic Suites for IPsec”.
- RFC 4764 (January 2007): “The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method”.
- RFC 4894 (May 2007): “Use of Hash Algorithms in Internet Key Exchange (IKE)”.

Chapter 2
Femto Network Gateway Configuration

This chapter provides configuration information for the Femto Network Gateway (FNG).

Important: Information about the commands in this chapter can be found in the *Command Line Interface Reference.*

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational.

The following sections are included in this chapter:

Configuring the System to Perform as a Femto Network Gateway

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an FNG in a test environment. For a configuration example without the instructions, refer to Appendix A.

Information provided in this section includes the following:

Required Information

The following sections describe the minimum amount of information required to configure and make the FNG operational in the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context.

Table 5. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet mask	The IPv4 address assigned to the interface. Multiple addresses and subnet masks are needed if multiple interfaces will be configured.
Physical Ethernet port number	The physical Ethernet port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connectors on the card. For example, port 24/1 identifies connector number 1 on the card in slot 24. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.

Required Information	Description
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system, such as ftpd and/or telnetd.

Required FNG Context Configuration Information

The following table lists the information that is required to configure the FNG context.

Table 6. Required Information for FNG Context Configuration

Required Information	Description
FNG context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the FNG context is recognized by the system.
Configuration for the Secure Interface to the FAPs in the Network	
FNG interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the interface that carries the IPSec tunnels between the FAPs in the network and the FNG.
AAA interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the interface between the AAA server and the FNG.
Loopback interface	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the FNG loopback interface.
IP addresses and subnet masks	The IPv4 addresses assigned to the FNG, AAA, and loopback interfaces above.
Physical Ethernet port number	The physical Ethernet port to which the FNG interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	The gateway IP address for configuring the IP route from the FNG interface to the FAP network.
AAA configuration information	Identifies the IP address of the RADIUS AAA server.
EAP profile name (required for the EAP authentication method)	When the EAP method is used for FAP authentication, the name of the EAP profile to be used.

Required Information	Description
Encrypted PSK (required for the PSK authentication method)	When the Pre-Shared Key (PSK) method is used for FAP authentication, the encrypted PSK to be used.
IKEv2 transform set name(s)	The name(s) of the IKEv2 transform set(s) to be used.
IPSec transform set name(s)	The name(s) of the IPSec transform set(s) to be used.
Crypto template name(s)	The name(s) of the IKEv2 crypto template(s) to be used.

Required FNG Service Configuration Information

The following table lists the information that is required to configure the FNG service.

Table 7. Required Information for FNG Service Configuration

Required Information	Description
FNG service name	The name of the FNG service, which must be from 1 to 63 alpha and/or numeric characters. The FNG service name can be the same across all FNG services within the same context and across all contexts.
AAA group name	The name of the AAA group to be used for FAP authentication.
IP address of the FNG loopback interface	The IP address of the FNG loopback interface configured in the FNG context.
Crypto template name	The name of the crypto template to be used.

Required Egress Context Configuration Information

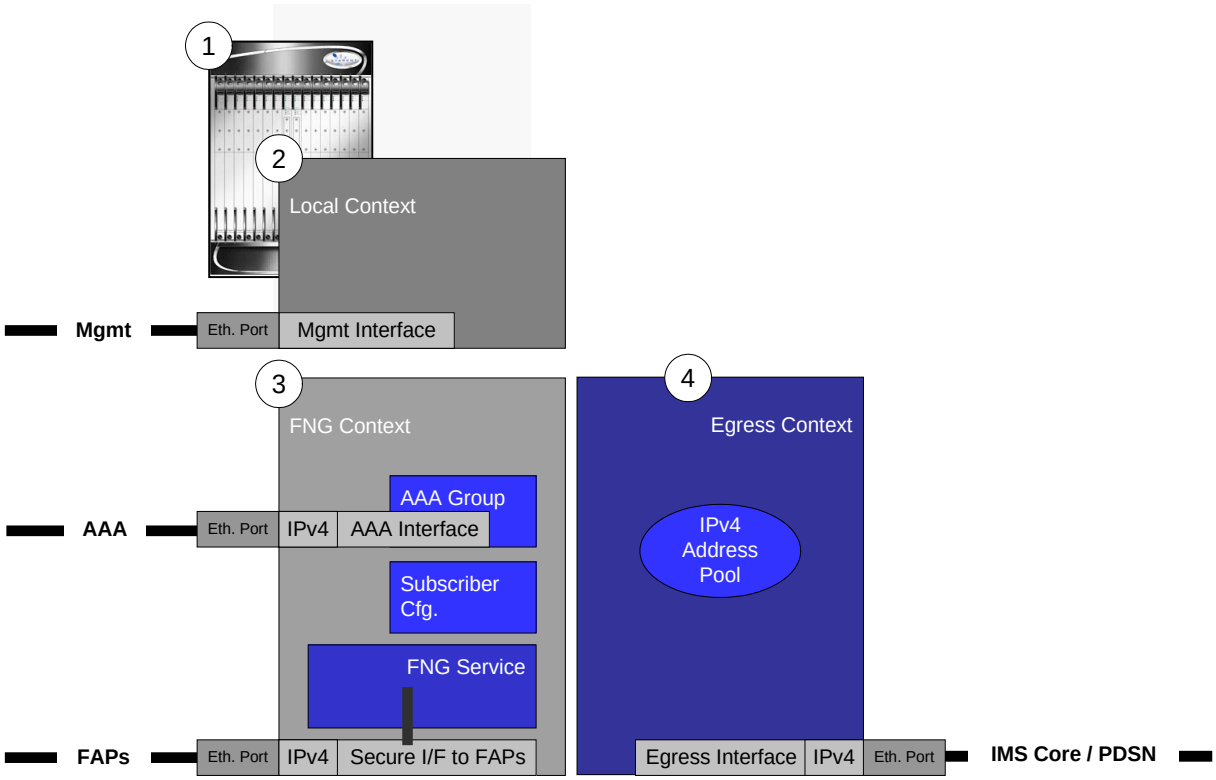
The following table lists the information that is required to configure the egress context.

Table 8. Required Information for Egress Context Configuration

Required Information	Description
Egress context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the egress context is recognized by the system.
IP pool	A logical name for the IPv4 address pool, which must be from 1 to 31 alpha and/or numeric characters.

Femto Network Gateway Configuration

The figure below shows the contexts in which FNG configuration occurs.



Step 1 Set system configuration parameters such as activating PSCs/PSC2s by applying the configuration examples in the *System Administration Guide.*

Step 2 Set initial configuration parameters by modifying the local context by applying the configuration example in the section Initial Configuration.

Step 3 Create the FNG context, FNG service, AAA group configuration, EAP profile configuration, IKEv2 and IPSec transform set configuration, and crypto template configuration by applying the configuration example in the section FNG Context Configuration.

Step 4 Create the egress context and IPv4 address pool by applying the configuration example in the section Egress Context Configuration.

Step 5 Log system activity by applying the configuration example in the section Logging Configuration.

Step 6 Save the configuration by following the steps in the *Verifying and Saving Your Configuration* chapter in this guide.

Initial Configuration

Set local system management parameters by applying the configuration example in the section Modifying the Local Context.

Modifying the Local Context

Use the following configuration example to create a management interface, configure remote access capability, and set the default subscriber in the local context:

```
configure
    context local
       interface <mgmt_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       server sshd
          subsystem sftpd
          exit
       server telnetd
          exit
       subscriber default
          exit
       administrator <name> encrypted password <password> ftp
       aaa group default
         exit
       gttp group default
          exit
       ip route 0.0.0.0 0.0.0.0 <gateway_ip_addr> <mgmt_interface_name>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
```

```
        bind interface <mgmt_interface_name> local
        exit
    end
```

The system automatically creates a default subscriber, default AAA group, and default GTTP group whenever a context is created. The **ip route** command in this example creates a default route for the management interface.

FNG Context Configuration

Step 1 Create the context in which the FNG service will reside by applying the configuration example in the section Creating the FNG Context.

Step 2 Create the AAA group by applying the configuration example in the section Creating the AAA Group.

Step 3 Create the EAP profile by applying the configuration example in the section Creating the EAP Profile.

Step 4 Create from one to six IKEv2 transform sets by applying the configuration example in the section Creating IKEv2 Transform Sets.

Step 5 Create from one to four IPSec transform sets by applying the configuration example in the section Creating IPSec Transform Sets.

Step 6 Create the crypto template for IKEv2 SA negotiation and specify the associated EAP profile by applying the configuration example in the section Creating the Crypto Template.

Step 7 Create the FNG service by applying the configuration example in the section Creating the FNG Service.

Creating the FNG Context

Use the following configuration example to create the FNG context and the interface between the FAPs in the network and the FNG, and to bind the interface to an Ethernet port:

```
configure
    context <fng_context_name>
        interface <fng_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        interface <fng_loopback_interface_name> loopback
            ip address <ip_address> <subnet_mask>
```

```
            exit
         ip route 0.0.0.0 0.0.0.0 <gateway_ip_address> <fng_interface_name>
         exit
      port ethernet <slot_number/port_number>
         no shutdown
         bind interface <fng_interface_name> <fng_context_name>
         end
```

The **ip route** command in this example creates a default route for the interface between the FAPs in the network and the FNG. This interface carries the IPSec tunnels between the FAPs and the FNG.

Creating the AAA Group

Use the following configuration example to create the AAA group configuration for FAP authentication and to bind the interface to an Ethernet port:

```
configure
    context <fng_context_name>
       interface <fng_aaa_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
          aaa group <group_name>
          radius algorithm round-robin
          radius accounting algorithm round-robin
          radius attribute nas-ip-address address <ip_address>
          radius strip-domain authentication-only
          radius dictionary <aaa_custom-dictionary>
          radius accounting interim interval <integer>
          radius server <ip_address> encrypted key <key> port <port_num>
          radius accounting server <ip_address> encrypted key <key> port
<port_num>
          exit
       exit
```

```
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <aaa_fng_interface_name> <fng_context_name>
       end
```

This example places the AAA group in the FNG context.

Creating the EAP Profile

Use the following configuration example to configure an EAP profile for FAP authentication:

```
configure
    context <fng_context_name>
       eap-profile <eap_profile_name>
          mode authenticator-pass-through
          end
```

In this example, the EAP method is used for FAP authentication. The **eap-profile** command creates the EAP profile to be used in the crypto template (configured below) for the FNG service.

The **mode authenticator-pass-through** command specifies that the FNG functions as an authenticator pass-through device, enabling an external EAP server to perform FAP authentication.

Creating IKEv2 Transform Sets

Use the following configuration example to create the required number of IKEv2 transform sets:

```
configure
    context <fng_context_name>
       ikev2-ikesa transform-set <ikev2_ikesa_tset1>
          encryption aes-cbc-128
          group 2
          hmac sha1-96
          prf sha1
          exit
```

This example shows default values.

Creating IPSec Transform Sets

Use the following configuration example to create the required number of IPSec transform sets:

```
configure
    context <fng_context_name>
       ipsec transform-set <ipsec_tset1>
       encryption aes-cbc-128
       group 2
       hmac sha1-96
       mode tunnel
          exit
```

This example shows default values.

Creating the Crypto Template

Use the following configuration example to create the crypto template used to define a cryptographic policy for the FNG service:

```
configure
    context <fng_context_name>
       crypto template <crypto_template_name> ikev2-subscriber
          certificate <name>
          natt
          authentication eap profile <eap_profile_name>
          ikev2-ikesa transform-set list <ikev2_ikesa_tset1>
          payload <payload_name_1> match childsa
             ip-address-allocation dynamic
             ipsec transform-set list <ipsec_tset1>
             exit
```

```
payload <payload_name_2> match childsa
   ipsec transform-set list <ipsec_tset1>
   exit
ikev2-ikesa keepalive-user-activity
ikev2-ikesa policy error-notification
   end
```

You must create one crypto template per FNG service. The **ikev2-subscriber** keyword in the **crypto template** command specifies that IKEv2 protocol is used for FAP authentication. The **certificate** command binds the specified X.509 trusted certificate to the crypto template. The **natt** command enables NAT traversal initiation for all security associations derived from the crypto template.

The **ikev2-ikesa keepalive-user-activity** command resets the user inactivity timer when keepalive messages are received from the peer. The **ikev2-ikesa policy error-notification** command enables the FNG to generate Error Notify messages for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT exchange.

In this FNG configuration example, the EAP method is used for FAP authentication. Alternately, the PSK (Pre-Shared Key) method can be used, as shown here:

```
configure
    context <fng_context_name>
       crypto template <crypto_template_name> ikev2-subscriber
          authentication pre-shared-key <value>
          end
```

If the PSK method is used for FAP authentication, *do not* create an EAP Profile as described in Creating the EAP Profile above.

Creating the FNG Service

Use the following configuration example to do the following:

- Create the FNG service.
- Specify that the FNG service uses the selected AAA group for FAP authentication.
- Bind the FNG service to the IP address of the FNG loopback interface.
- Bind a crypto template to the FNG service.

```
configure
    context <fng_context_name>
```

```
        fng-service <fng_service_name>

           aaa authentication context-name <fng_context_name> aaa group
<group_name>

           bind address <ip_address> crypto-template <crypto_template_name>

           end
```

The IP address that you bind to the FNG service above is used as the connection point for establishing the IKEv2 sessions between the FAPs in the network and the FNG.

Egress Context Configuration

Create the egress context by applying the configuration example in the following section.

Creating the Egress Context

Use the following configuration example to create the egress context, the interface to the IMS core/PDSN, and the IPv4 address pool for generating and assigning IPv4 addresses to the FAPs in the network:

```
configure

    context <egress_context_name> -noconfirm

       interface <egress_interface_name>

          ip address <ip_address> <subnet_mask>

          exit

       ip pool <name> < ip_address subnet_mask> public < priority>

       exit

    port ethernet <slot_number/port_number>

       no shutdown

       bind interface <egress_interface_name> < egress_context_name>

       end
```

Logging Configuration

Use the following configuration example to enable logging:

```
configure
    logging filter active facility sessmgr level <critical/error>
    logging filter active facility ipsec level <critical/error>
    logging filter active facility ikev2 level <critical/error>
    logging filter active facility fng level <critical/error>
    logging active
    end
```

Verifying and Saving the Configuration

To verify and save changes made to the FNG configuration, follow the steps in the *Verifying and Saving Your Configuration* chapter in this guide.

Configuring Optional Features

This section provides configuration examples for configuring optional features for the FNG in a test environment.

Information provided in this section includes the following:

- A12 Aggregation Configuration
- Multiple Child SAs and DSCP Marking Configuration
- FAP ID-based Duplicate Session Detection Configuration

A12 Aggregation Configuration

The A12 aggregation feature reduces the number of source addresses in the A12 Access-Request messages sent to the AN-AAA servers by the FNG, which simplifies the configuration of the AN-AAA server's database. Use the following configuration example to configure A12 aggregation:

```
configure
    context <fng_context_name>
       interface <fng_aaa_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
          aaa group <group_name>
          radius attribute nas-ip-address address <ip_address>
          radius dictionary <aaa_custom-dictionary>
          radius aggregation modify-nas-ip
          radius server <ip_address> encrypted key <key> port <port_num>
          exit
configure
    context <fng_context_name>
       fng-service <fng_service_name>
          aaa aggregation a12-group context-name <fng_context_name> aaa
group <group_name>
          aaa aggregation interface type a12
```

```
aaa aggregation a12-destination-address <ip_address_1>
aaa aggregation a12-destination-address <ip_address_2>
exit
```

In the example above, the **aaa aggregation interface type a12** command enables A12 aggregation for the FNG service. The **radius aggregation modify-nas-ip** command specifies that the FNG modifies the NAS IP address and port number to the local FNG bind address when forwarding A12 packets.

There are two **aaa aggregation a12-destination-address** commands in the example above. One destination address is the IP address of the AN-AAA server, the other is the IP address of the FNG service. When the FNG receives one of these destination addresses from a FAP, the FNG performs A12 aggregation.

Multiple Child SAs and DSCP Marking Configuration

It is recommended that multiple Child SAs are used on the FNG to provide the appropriate QoS services. This handling can be applied to different types of traffic (voice and data) coming from the same UE behind a FAP, or from multiple UEs belonging to the same QoS class. The FNG will determine the traffic type and provide a QoS treatment based on configured rules.

Use the following configuration example to configure multiple Child SAs and DSCP marking:

```
configure
    context <fng_context_name>
        class-map name <name> match-any
            match dst-ip-address <ip_address>
            exit
        policy-map name <name>
            class-map name <name>
            qos encaps-header dscp-marking <0x2e>
            child_sa_id <2>
            exit
        policy-group name <policygroup_out>
            policy <name> precedence <number>
            exit
        subscriber default
            policy-group <policygroup_out> direction <out>
            exit
```

```
            exit
```

In the example above, the traffic that matches the class rule destination IP address has DSCP marking 0x2e and uses the specified Child SA 2 for sending traffic. This example specifies that this is applied to downlink traffic only.

If the specified Child SA 2 does not exist or does not match any class rule, the FNG uses the default Child SA 1.

FAP ID-based Duplicate Session Detection Configuration

When this feature is enabled and a FAP sets up a new session, the FNG automatically checks for any remnants of abandoned calls, and if found, clears them. Clearing the old session and establishing the new session in parallel optimizes FNG processing functions. Use the following configuration example to configure FAP ID-based duplicate session detection:

```
configure
    context <fng_context_name>
       fng-service <fng_service_name>
          duplicate-session-detection fapid-based
          end
```

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save your system configuration.

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

Feature Configuration

In many configurations, you have to set and verify specific features. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##############################################################################

Displaying Global
AAA-configuration errors
##############################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SMC's CompactFlash or on an installed PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

save configuration *url* **[-redundant] [-noconfirm] [showsecrets] [verbose]**

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name* [*:port#*] } [*/directory*] */file_name* • **ftp://**[*username* [*:pwd*] *@*] { *ipaddress*|*host_name* } [*:port#*] [*/directory*] */file_name* • **sftp://**[*username* [:*pwd*] *@*] { *ipaddress*|*host_name* } [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the /pcmcia1 device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).

Keyword/Variable	Description
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.

Important: The **-redundant** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs, using an FTP server with an IP address of 192.168.34.156, on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

save configuration *tftp://config_server/init_config.cfg*

Chapter 4
Monitoring the FNG Service

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the *Command Line Interface Reference*.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Output descriptions for most of the commands are located in the *Statistics and Counters Reference.*

Table 9. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View FNG Service Information and Statistics	
View FNG service information and statistics	**show fng-service { all [counters] | name** *service_name* **| statistics }**
View FNG service session information	**show fng-service session [all | callid** *call_id* **| counters | full [all | callid** *call_id* **| ip-address** *ip-address* **| peer-address** *ip_address* **| username** *name* **] | ip-address** *ip-address* **| peer-address** *ip-address* **| summary [all | callid** *call_id* **| ip-address** *ip-address* **| peer-address** *ip-address* **| username** *name* **] | username** *name*]
View additional session statistics	**show session [disconnect-reasons | duration | progress | setuptime | subsystem]**
View FNG service bulk statistics	**show bulkstats variables fng**
View IPSec and IKEv2 Information	
View IPSec security associations	**show crypto ipsec security-associations**
View IKEv2 security associations	**show crypto ikev2 security-associations**
View crypto map configuration information	**show crypto map map-type ipsec-ikev2-subscriber**
View IPSec session recovery status	**show ipsec session recovery status**
View IKEv2 statistics	**show crypto statistics ikev2**
View Congestion Control Information	
View congestion control statistics for FNG	**show congestion-control statistics ipsecmgr**
View Subscriber Information	
Display Session Resource Status	
View session resource status	**show resources session**
Display Subscriber Configuration Information	

To do this:	Enter this command:
View locally configured subscriber profile settings (must be in the context where the subscriber resides)	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings	**show subscribers aaa-configuration username** *subscriber_name*
View Subscribers Currently Accessing the System	
View a list of subscribers currently accessing the system	**show subscribers all**
View a list of FNG subscribers currently accessing the system	**show subscribers fng-only**
View Session Subsystem and Task Information	
Display Session Subsystem and Task Statistics *Important:* Refer to the *System Software Task and Subsystem Descriptions* appendix in the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View Session Manager statistics	**show session subsystem facility sessmgr all**
View Session Recovery Information	
View session recovery status	**show session recovery status [verbose]**
View Session Disconnect Reasons	
View session disconnect reasons	**show session disconnect-reasons**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping.

Statistics and counters can be cleared using the CLI **`clear`** command. Refer to the *Command Line Interface Reference* for detailed information on using this command.

Appendix A
Sample Femto Network Gateway Configuration File

This appendix contains a sample Femto Network Gateway (FNG) configuration file. The following configuration is supported:

Sample FNG Configuration

In the following configuration example, commented lines are labeled with the number symbol (#) and variables are identified using italics within brackets (<*variable*>).

Sample FNG Configuration

This section contains the following sample FNG configuration file.

```
# Modify the local context for local system management
configure
    context local
       interface <mgmt_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       server sshd
          subsystem sftpd
          exit
       server telnetd
          exit
       subscriber default
          exit
       administrator <name> encrypted password <password> ftp
       aaa group default
         exit
       gttp group default
          exit
       ip route 0.0.0.0 0.0.0.0 <gateway_ip_addr> <mgmt_interface_name>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <mgmt_interface_name> local
       exit
    end
```

```
# Configure the FNG context
configure
    context <fng_context_name>
       interface <fng_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       interface <fng_loopback_interface_name> loopback
          ip address <ip_address> <subnet_mask>
          exit
       ip route 0.0.0.0 0.0.0.0 <gateway_ip_address> <fng_interface_name>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <fng_interface_name> <fng_context_name>
       end
# Configure the AAA group
configure
    context <fng_context_name>
       interface <fng_aaa_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       aaa group <group_name>
          radius algorithm round-robin
          radius accounting algorithm round-robin
          radius attribute nas-ip-address address <ip_address>
          radius strip-domain authentication-only
          radius dictionary <aaa_custom-dictionary>
          radius accounting interim interval <integer>
          radius server <ip_address> encrypted key <key> port <port_num>
```

```
            radius accounting server <ip_address> encrypted key <key> port
<port_num>
            exit
         exit
      port ethernet <slot_number/port_number>
         no shutdown
         bind interface <aaa_fng_interface_name> <fng_context_name>
         end
# Create the EAP profile
configure
      context <fng_context_name>
         eap-profile <eap_profile_name>
            mode authenticator-pass-through
            end
# Create the IKEv2 transform sets
configure
      context <fng_context_name>
         ikev2-ikesa transform-set <ikev2_ikesa_tset1>
            encryption aes-cbc-128
            group 2
            hmac sha1-96
            prf sha1
            exit
# Create the IPSec transform sets
      context <fng_context_name>
         ipsec transform-set <ipsec_tset1>
         encryption aes-cbc-128
         group 2
         hmac sha1-96
```

```
        mode tunnel
           exit
# Create the crypto template
configure
    context <fng_context_name>
        crypto template <crypto_template_name> ikev2-subscriber
           certificate <name>
           natt
           authentication eap profile <eap_profile_name>
           ikev2-ikesa transform-set list <ikev2_ikesa_tset1>
           payload <payload_name_1> match childsa
              ip-address-allocation dynamic
              ipsec transform-set list <ipsec_tset1>
              exit
           payload <payload_name_2> match childsa
              ipsec transform-set list <ipsec_tset1>
              exit
           ikev2-ikesa keepalive-user-activity
           ikev2-ikesa policy error-notification
              end
# Create the FNG service
configure
    context <fng_context_name>
        fng-service <fng_service_name>
           aaa authentication context-name <fng_context_name> aaa group
default
           bind address <ip_address> crypto-template
<crypto_template_name>
           end
# Create the Egress context
```

```
configure
    context <egress_context_name> -noconfirm
       interface <egress_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       ip pool <name> < ip_address subnet_mask> public < priority>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <egress_interface_name> < egress_context_name>
       end
# Enable logging
configure
    logging filter active facility sessmgr level <critical/error>
    logging filter active facility ipsec level <critical/error>
    logging filter active facility ikev2 level <critical/error>
    logging filter active facility fng level <critical/error>
    logging active
    end
```

Appendix B
Femto Network Gateway Engineering Rules

This appendix provides Femto Network Gateway (FNG) engineering rules or guidelines that must be considered prior to configuring the ASR 5000 for your network deployment. General and network-specific rules are located in the appendix of the *System Administration and Configuration Guide* for the specific network type.

The following rules are covered in this appendix:

IKEv2/IPSec Restrictions

The following is a list of known restrictions for IKEv2 and IPSec:

- Each FNG service must specify one crypto template.
- The FNG supports traffic selectors with IPv4 address values only. IPv6 address values are not supported.
- The FNG supports IKEv2 only between the FAP and the FNG.
- IKEv2 does not support Perfect Forward Secrecy (PFS) of individual Child SAs. While the PFS for FAP-initiated IKE SA rekeying will be implemented, the rate for rekeying (with PFS enabled) shall not exceed the rate of the IKEv2 call setup rate. This is because PFS would require performing a new D-H exchange each time a rekey is negotiated, and a performance impact is expected. Also, note that the call setup rate and the rekeying rate are mutually exclusive.
- All IKEv2 packets are sent over IPv4.
- Per RFC 4306 and RFC 4718, the following known restrictions apply with respect to the payload and its order. Violations result in INVALID_SYNTAX being returned which is being enabled or disabled through a configurable parameter, except when the processing is noted below.
- While RFC 4306 Section 2.19 specifies “CP payload MUST be inserted before the SA payload,” the FNG does not force strict ordering of this. The FNG processes these payloads as long as the FAP sends a Configuration Payload (CP) anywhere inside the encrypted data.
- While RFC 4306 Section 2.23 specifies “The location of the payloads (Notify payloads of type NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP) in the IKE_SA_INIT packets are just after the Ni and Nr payloads (before the optional CERTREQ payload),” The FNG does not force strict ordering of this and still can process these NOTIFY payloads.
- The FNG supports transform selector payloads with only one traffic selector. The TS field must be set to “1”.
- Traffic selector payloads from the FAP support only traffic selectors by IP address range. In other words, the IP protocol ID must be 0. The start port must be 0 and the end port must be 65535.
- The CP is specified in RFC 4306, Section 2.19 (Requesting an Internal Address on a Remote Network) for the situation where dynamic IP address assignment is required. Since the FNG does not support INTERNAL_IP6_ADDRESS, the CP must include at least the attribute INTERNAL_IP4_ADDRESS.
- As described above, when the FNG receives IKEv2 messages, the FNG does not enforce the payloads to be in order. However, when the FNG sends the response or generates any IKEv2 messages, the FNG will ensure that payloads are ordered according to RFC 4306.
- Only IKE and ESP protocol IDs are supported. AH is not supported since AH is deprecated in RFC 4306.
- The IKE Protocol ID specification may not use the NONE algorithm for authentication or the ENCR_NULL algorithm for encryption as specified in Section 5 (Security Considerations) of RFC 4306.
- In ESP, ENCR_NULL encryption and NONE authentication cannot be simultaneously used.
- Only one single proposal number can be used. Because RFC 4306 states that the first proposal must be numbered 1, this implies that only proposals with the proposal number value of 1 are supported. The FAP must send a list of transforms within this single proposal number.
- No more than 16 transform types may be present in a single IKE_SA_INIT or IKE_AUTH Request message. If a deviation from this format is used in the proposal format, the FNG returns an error of INVALID_SYNTAX.