FNG Service Configuration Mode Commands

Command Modes

The FNG Service Configuration Mode is used to configure the properties required for the Femto Network Gateway (FNG) to interface with the Femto Access Points (FAPs) in the network.

Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aaa aggregation

Sets the system attributes for A12 aggregation for the FNG service.

Product

FNG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

Syntax Description

```
aaa aggregation { interface type a12| destination address ipv4_address |
a12-group { context name [ aaa-group name ] | aaa-group name [ context name ]
 } }
no aaa aggregation interface type a12
no a12 destination address ipv4_address
no aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group
 name [ context name ] }
```

aaa aggregation interface type *a12*

Enables A12 aggregation functionality for the FNG service.

aaa aggregation interface a12 destination address *ipv4_address*

Adds a destination address for an AN-AAA server for A12 aggregation. A maximum of ten destination addresses can be configured.

aaa aggregation a12-group { context *name* [aaa-group *name*] | aaa-group [context *name*] }

Defines the AAA context and AAA group to be used for A12 aggregation.

If the context name and AAA group are not specified, the FNG defaults to the FNG service context and the default AAA group in that context. If the AAA group is specified but the context is not specified, the FNG uses the FNG service context and the AAA group in that context. If the AAA group is not specified and the context is specified, the FNG uses the default AAA group in that context.

no aaa aggregation interface type *a12*

Disables A12 aggregation functionality for the FNG service.

no aaa aggregation a12-destination address *ipv4_address*

Deletes the specified destination address for an AN-AAA server.

no aaa aggregation a12-group { context *name* [aaa-group *name*] | aaa-group [context *name*] }

Deletes the specified AAA context and AAA group to be used for A12 aggregation.

Usage Guidelines

Sets the system attributes for AAA aggregation in the FNG service.

Example

The following command enables the A12 functionality for the FNG service:

```
aggregation interface type a12
```

aaa authentication

Specifies the AAA group to use for FAP authentication.

Product FNG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

Syntax Description

aaa authentication { context-name *name* **aaa-group** *name* **| context-name** *name* **aaa-group** *name* **}**
no aaa authentication

no aaa authentication

Removes any existing authentication configuration.

context-name *name* aaa-group *name*

Specifies the context name and the AAA group name configured in the context for FAP authentication.

context-name *name*: Specifies the context where the AAA server group is defined as an alphanumeric string of 1 through 79 characters.

aaa-group *name*: Specifies the name of the AAA group to be used for authentication as an alphanumeric string of 1 through 63 characters.

Usage Guidelines Use this command to specify that during IPSec session establishment using IKEv2 setup, the FNG will use Radius AAA for FAP authentication.

Example

Use the following to configure device authentication for an AAA group named *aaa-10* in the FNG context named *fng1*:

```
aaa authentication context-name fng1 aaa-group aaa-10
```

bind

Binds the FNG service IP address to a crypto template and specifies the maximum number of sessions the FNG service supports.

Product FNG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

Syntax Description

bind address *ipv4_address* **{ crypto-template** *string* **}[max-sessions** *number* **]**
no bind

no bind

Removes a previously configured binding.

address *ipv4_address*

Specifies the IPv4 address of the FNG service.

crypto-template *string*

Specifies the name of the crypto template to be bound to the FNG service.

string is any value from 0 - 127 alpha and/or numeric characters.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the FNG service as an integer from 0 through 1000000. Default: 1000000

If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage Guidelines

Binds the IP address used as the connection point for establishing the IKEv2 sessions to a crypto template. It can also define the maximum number of sessions the FNG can support.

Example

The following command binds an FNG service with an IP address of *10.2.3.4* to the crypto template named *T1* and sets the maximum number of sessions to *500000*:

```
bind address 10.2.3.4 crypto-template T1 max-sessions 500000
```

default

Sets or restores the default condition for the selected parameter.

Product

FNG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

Syntax Description

default { { aaa attribute 3gpp2-service-option } | duplicate-session-detection | ip source-violation { drop-limit | period } | setup-timeout | subscriber *name* **}**

aaa attribute 3gpp2-service-option

Sets or restores the default value of 4095.

duplicate-session-detection

Sets or restores the default option for duplicate session detection to be fapid-based.

ip source-violation (drop-limit | period }

Sets or restores the IP source violation detection defaults, as follows:

drop-limit: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.

period: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

setup-timeout

Sets or restores the maximum time allowed for session setup to the default value of 60 seconds.

subscriber *name*

Sets or restores the name of the default subscriber.

name is a string of 1-127 characters.

username mac-address-stripping

The default behavior is to disable stripping the MAC address from the username.

Usage Guidelines

Configures the default settings for a given parameter.

Example

Use the following command to set the maximum time allowed for session setup to the default value of 60 seconds:

```
default setup-timeout
```

duplicate-session-detection

Configures the FNG to detect duplicate call sessions based on Femtocell Access Point (FAP) ID and to clear old call information.

This feature is disabled by default.

Product

FNG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-fng-service)#`

Syntax Description

```
duplicate-session-detection { fapid-based }
no duplicate-session-detection
default duplicate-session-detection
```

fapid-based

Sets the FNG to detect duplicate call sessions based on the FAP ID.

no duplicate-session-detection

Disables duplicate session detection.

default duplicate-session-detection

Sets or restores the default option for duplicate session detection to be fapid-based.

Usage Guidelines By default, duplicate session detection is disabled.Use this command to enable this feature. It applies only to calls established after the feature has been enabled.

The following command enables duplicate session detection based on FAP ID:

```
duplicate-session-detection fapid-based
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `exit`

Usage Guidelines Use this command to return to the parent configuration mode.

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product FNG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-fng-service)#`

Syntax Description

`ip source-violation { clear-on-valid-packet | drop-limit` *`num`* **`| period`** *`secs`* **`}`**
`no ip source-violation clear-on-valid-packet`

clear-on-valid-packet

Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

drop-limit *num*

Sets the maximum number of allowed IP source violations within the detection period before dropping a call as an integer from 1 through 1000000. Default: 10

period *secs*

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. Default: 120

Usage Guidelines This function allows the operator to configure the network to prevent problems such as when a user gets handed back and forth between two gateways a number of times during a handoff scenario.

When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment.

For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example

The following command sets the drop limit to *15* and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```

setup-timeout

Specifies the maximum time allowed to set up a session in seconds.

Product

FNG

Privilege

Security-Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context *context_name* **> fng-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

Syntax Description

setup-timeout *integer*
default setup-timeout

setup-timeout *integer*

Sets the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

default

Sets or restores the default session setup timer value to 60 seconds.

Usage Guidelines

The FNG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

Example

The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```