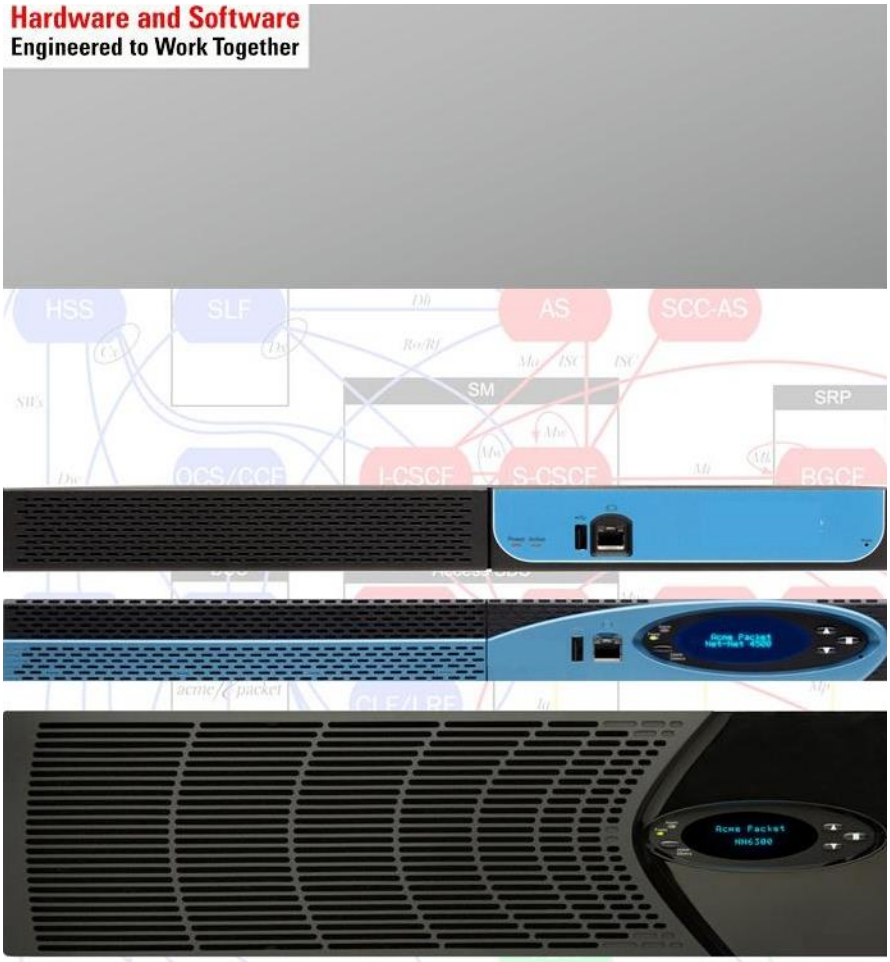


Oracle Communications Security Gateway MCX300– IP.access nano3G AP561.2.0 technical Application Note

Technical Application Note

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Intended Audience

This document is intended for use by Oracle Sales Consultants, Engineers, third party Systems Integrators, and end users of the Oracle Communications Security Gateway product. It assumes that the reader is familiar with basic operations of the Oracle Communications Acme Packet 4500 platform.

Document Overview

This technical application note documents the Oracle Communications Security Gateway (OCSG) and IP.access nano3G Integration and interoperability testing. It should be noted that while this application note focuses on the optimal configuration between Oracle Communications Security Gateway and the ip.access nano3G UTRAN system, production environments in different customer networks will have additional configuration parameters that are specific to other applications.

Introduction

IP.access – Oracle Communications Partnership

Ip.access integrates and supports the Oracle Communications Security Gateway as part of its complete nano3G femtocell and picocell solution. The OCSG fulfills the security gateway functional requirements defined in 3GPP, providing authentication and IPsec tunnel management between nano3G Access Points and the Access Controller.

Ip.access nano3G small cells generate high-quality 3G signals indoors and use broadband IP backhaul for rapid deployment, low-cost operation while offloading macro traffic. The combined solution delivers on all the benefits of small cells–improved customer experience and reduced macro network costs–with security, manageability and reliability.

Oracle Communications Security Gateway

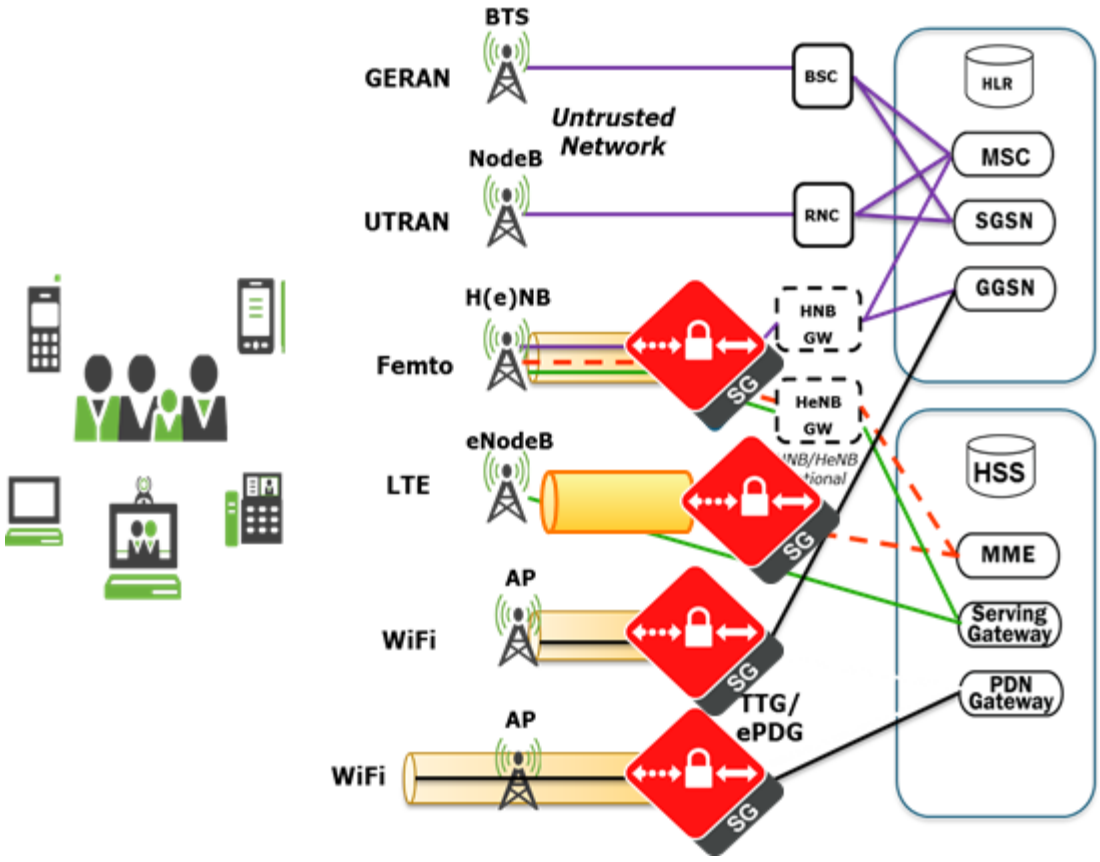
Oracle Communications Security Gateway is a high performance tunneling gateway for heterogeneous networks, enabling fixed mobile convergence and offload macro Radio Access network traffic. It secures the core networks of service providers from untrusted internet access to local femtocells, evolved Home Node Bs (LTE femtocells) and Wi-fi devices. Oracle Communications Security Gateway is supported on the Acme Packet 4500 platform. It leverages the industry leading Acme Packet OS software platform to offer security gateway capabilities – large scale IPsec tunnel termination from femtocells and Wi-Fi devices into mobile operator core.

The security gatewayis typically deployed in operator's Core network and is based on industry standards and fulfills the following functional elements defined by Third Generation Partnership Project (3GPP) and

Third Generation Partnership Project Two (3GPP2):

- Interworking-Wireless Local Area Network (I-WLAN) Tunnel Terminating Gateway (TTG)
- Home NodeB (HNB) Security Gateway
- Femtocell Security Gateway
- Evolved Packet Data Gateway (ePDG)

Role of the Security Gateway in Mobile Networks



Application Overview

Security gateway provides secure integration from RAN to Mobile Core. The role of Security Gateway can be elaborated:

Integrated Small Cell and WiFi with Mobile Core

- EAP authentication
- Seamless hand-overs

Secure RAN to Mobile Core

- Integrate with Oracle PCRF, SBC, IMS solutions

Enforce QoS

- Low latency, PCRF integration

Comprehensive security

- IPsec tunnels with rich authentication suite and encryption models
- DOS/DDOS protection

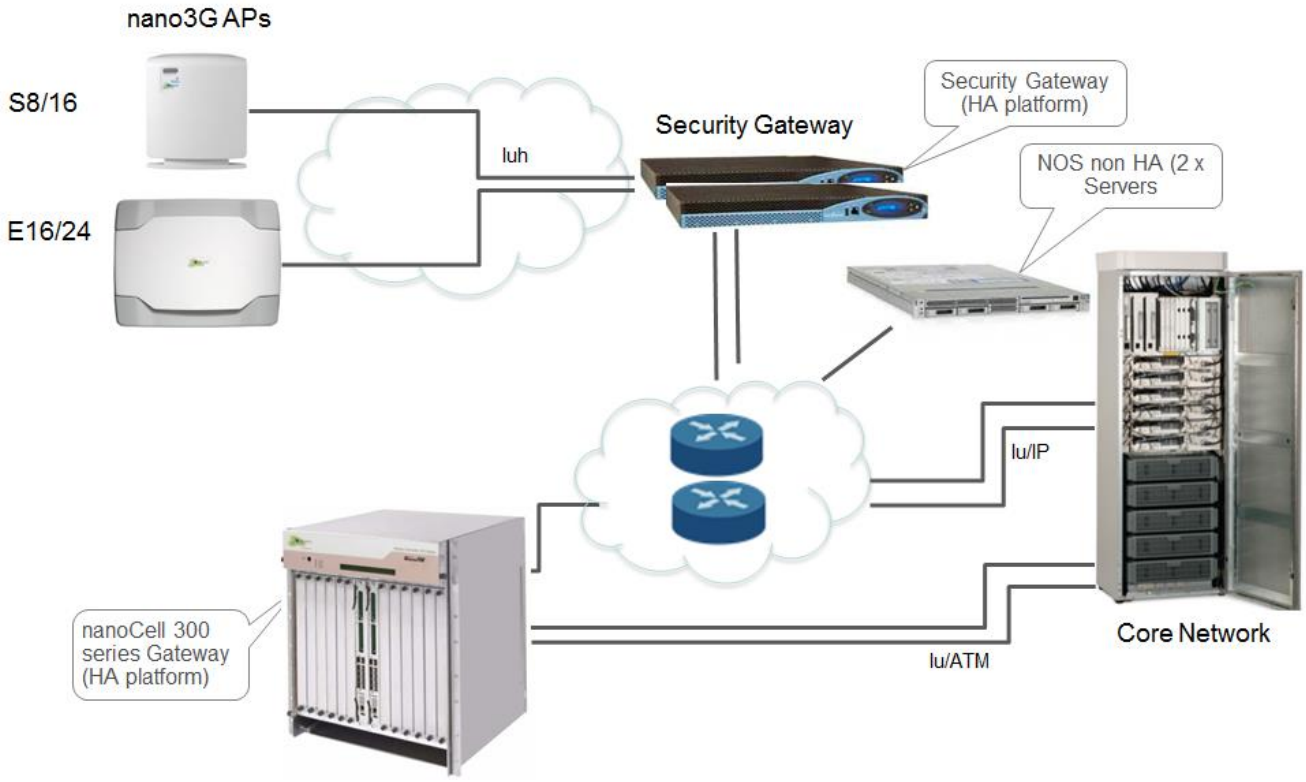
Simplified integration and service flexibility

- Support different topologies and 3GPP functional elements (WAG, ePDG, SeGW), can be deployed close to cell sites/access points to improve radio efficiency by limiting packet loss and retransmissions
- Local Break-out of traffic, Integration with AAA, Mobile Core
- Support IPv6 and v6 address families, routing protocols, tunneling technology

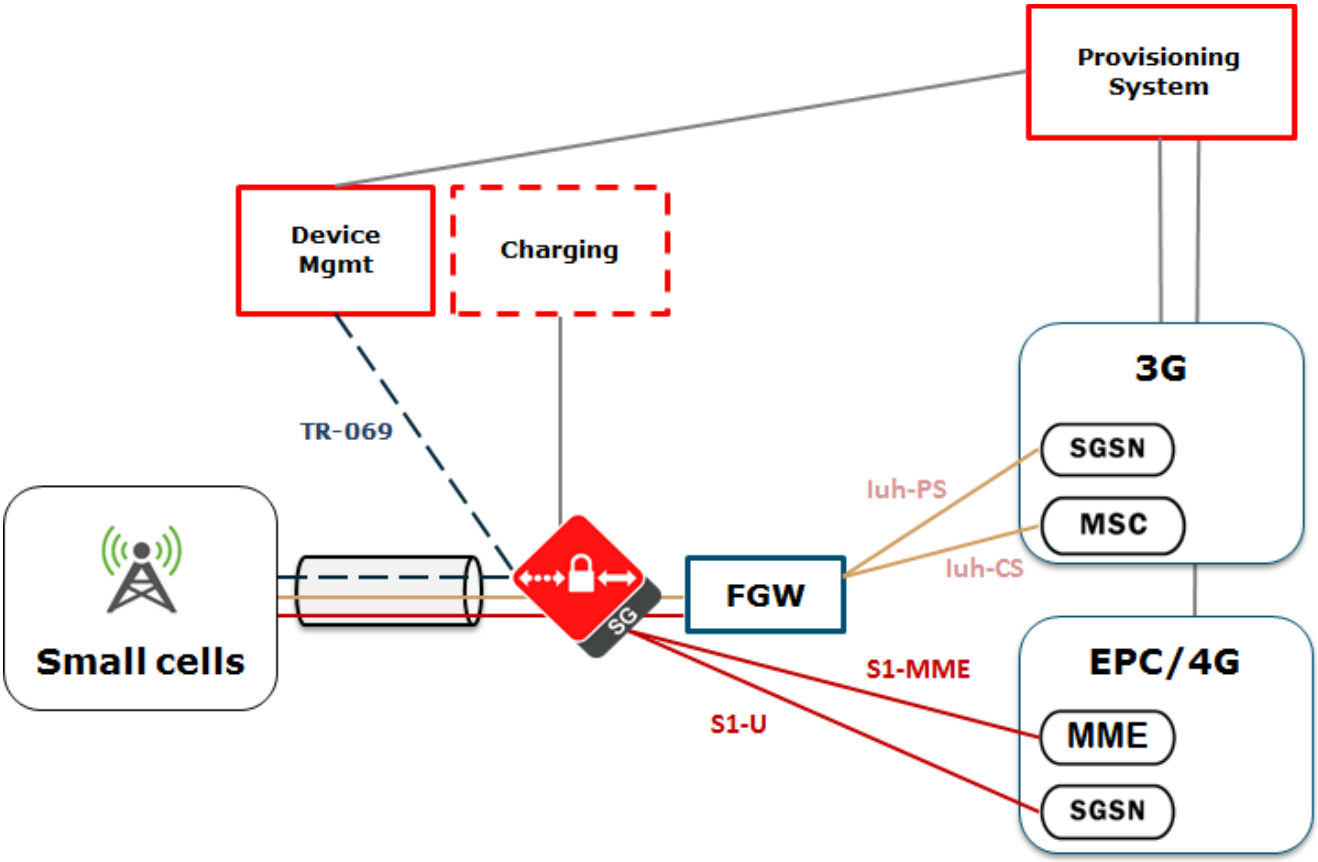
Compact and powerful

- High tunnel processing (10K's -100K's per 1RU)
- Non-blocking data path for low latency (VoLTE, gaming, real-time 2-way video)
- High availability for service continuity

Ip.access NC300 Architecture



Small Cell Architecture



Functional Overview of OCSG features and configuration in ip.acccess Small Cell solution

Authentication

The OCSG supports device authentication under the IKEv2 framework. Device authentication is initiated by the endpoints or AP towards the user-facing IKE interface of the OCSG. There are many different modes of authentication in the IKEv2 framework and

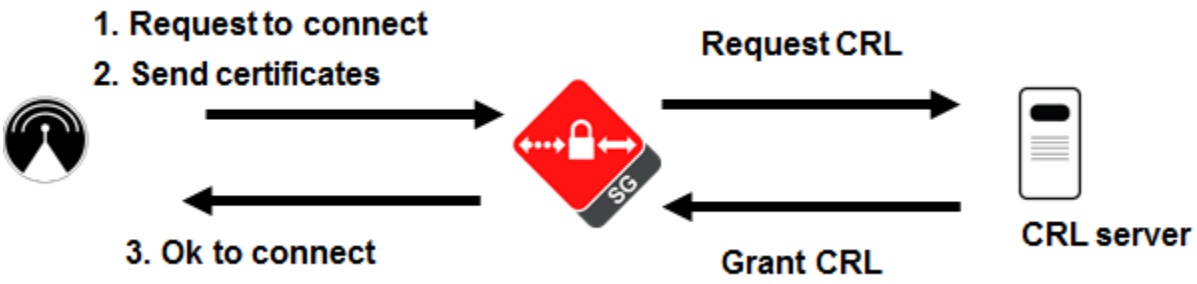
ip.access solution utilizes the Certificate based authentication mode with X.509v3 certificates. An overview of the mechanism is provided below:

Certificate authentication (mutual)

With X.509v3 certificate mutual authentication, the endpoint and security gateway authenticate each other. The OCSG offers a certificate to the endpoint that has been signed by the CA (Certificate Authority) so that the endpoint/AP can verify the identity of the OCSG. The endpoint then utilizes the root certificate of the CA to validate the OCSG's certificate. This operation ensures endpoint that it is connecting to a valid OCSG.Now to verify whether the AP/endpoint is genuine or not, the endpoint/AP offers a certificate signed by the CA and the OCSG validates the endpoint with the OCSG's root certificate of the CA. Sample configuration is provided in Appendix A of this document. (certificate-record and ike-certificate-profile and ike-certificate-profile-id-list in ike-interface)

Certificate Revocation List

An alternative to utilizing Online Certificate Status Protocol (OCSP) to verify the endpoint certificate validity when performing mutual certificate authentication, is to utilize CRL (RFC 3280) to validate the public key certificate of an endpoint. With CRL support, the OCSG loads a list that contains the certificates of the revoked endpoints. When the endpoint offers its certificate for validation to the OCSG, the OCSG checks the certificate against the list in the CRL, and if there is a match, the endpoint is not allowed to establish an IPsec tunnel towards the OCSG. If there is no match against the CRL, then the OCSG allows the IPsec tunnel establishment to succeed. Ip.access deployments use this feature of the security gateway. A diagram of the exchange process in CRL is given below:



Sample configuration is below:

```
cert-status-profile
       name                              IPAoemCRL
       ip-address                        10.m.n.p
```

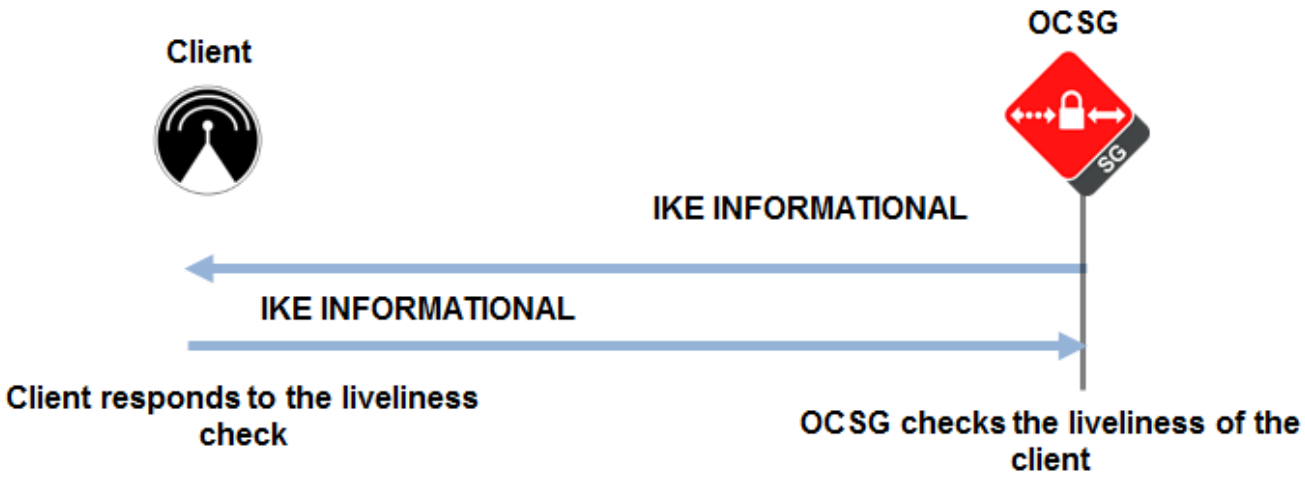
```
       hostname
       port                            80
       type                            CRL
       trans-proto                     HTTP
       requestor-cert
       responder-cert                  IPAoemCert
       realm-id                        Core1
       retry-count                     3
       dead-time                       0
       crl-update-interval             86400
       crl-list
/crl/crl.ipaccess.com/ipaccessltd_oemca_101_100.crl

ike-interface
       address                         e.f.g.h0
       realm-id                        Access1
       ike-mode                        responder
       local-address-pool-id-list      LocalPool1
       dpd-params-name                 DpdParams1
       v2-ike-life-secs                259200
       v2-ipsec-life-secs              43200
       v2-rekey                        enabled
       multiple-authentication         disabled
       multiple-child-sa-mode          none
       shared-password
       eap-protocol
       addr-assignment                 local
       sd-authentication-method        certificate
       certificate-profile-id-list     <fqdn>
       threshold-crossing-alert-group-name
       cert-status-check               disabled
       cert-status-profile-list        IPAoemCRL
       access-control-name
       accounting-param-name
       traffic-selectors               10.0.0.0/8
       ip-subnets
       authorization                   disabled
```

Dead Peer Detection

Dead Peer Detection (DPD) enables the detection of endpoints that have stale, or unused, IPsec tunnels. The OCSG acts as both a DPD responder, as well as a DPD initiator. As a DPD responder, the IPsec endpoint sends the INFORMATIONAL request (defined in RFC 4306) with no payloads (other than the empty Encrypted payload required by the syntax) to the OCSG to check liveness of the OCSG. The OCSG replies to these messages. As a DPD initiator, the OCSG sends the INFORMATIONAL request

with no payloads (other than the empty Encrypted payload required by the syntax) to check the liveness of the endpoint. A diagram of the DPD message exchange is provided below:



Sample configuration is below:

```
dpd-params
        name                            DpdParams1
        max-loop                        100
        max-endpoints                   25
        max-cpu-limit                   60
        load-max-loop                   40
        load-max-endpoints              5
        max-attempts                    1
        max-retrans                     0
```

Lab Configuration and Software/Hardware Tools

The test environment consisted of the following components:

- Oracle Communications Security Gateway
- Ip.access Nano3G Small cell Access point and Controller

The following tables provide the software hardware versions used for the elements:

Oracle Communications Security Gateway System Specifications

Hardware	Acme Packet 4500 platform with ETC2 10G NIU
Software Release	nnMCX300m2p1.tar
Software modules enabled	Security gateway, IKE tunnels (200000 tunnels)

Ip.access Nano3G Small cell Access Point and Controller System Specifications

Hardware	Nano-16 3G AP (NodeB)
Software Release	N3G_2.0.5 (AP561.2.0)
Access Controller Hardware	nano3G AC (RNC) Version - N3G_2.0.5(SR2.0.0-138.0)
3G MSC/ SGSN	NG40

Test Cases

The purpose of this testing was to verify the correct implementation of interface between ip.access nano3G UTRAN and ACME Security Gateway.

The following main areas were covered during IOT:

- IPsec & Traffic/data pass through
- Standalone
- Redundancy

This section gives a one-line description of each test case. For each test case the appropriate Result is given as defined below.

Passed (P): All parties agree that the test case has met all the requirements defined in the test case description.

Conditionally Passed (P*) : All parties agree that the test case has met the requirements defined in the test case description, however; a comment is included to clarify the behavior witnessed during the test.

Failed (F): All parties agree that the test case has not met the criteria specified in the test case description.

Not Possible (NP): The test case was not performed

Not Triggered (NT): The test case could not be triggered

Under test (UT): The test case couldn't be concluded in the current session

Total number of test cases: 20

Test cases

IPsec & Traffic

Test ID	IPsec & Traffic	Result	Comments
ACME_AP_01	Demonstrate that the AP can connect through the Security Gateway to the AC and that UEs can make CS calls and PS calls	**P**	
ACME_AP_02	Set up an IPsec tunnel between an AP and the Security Gateway using “Real” Certificates in both the AP and the Security Gateway.	**P**	
ACME_AP_03	Set up an IPsec tunnel between an AP and Security Gateway using Test Certificates in both the AP and the Security Gateway.	**P**	
ACME_AP_04	Demonstrate that the Security Gateway works with its certificate containing an FQDN.	**P**	
ACME_AP_05	Demonstrate that the Security Gateway works with its certificate containing an IP address.	**P**	
ACME_AP_06	Demonstrate that the IPsec tunnel conforms to the IPsec profile (e.g. uses AES-128 encryption, DH 2, etc see profile). Initial IKE_INIT_SA using UDP port 500 and subsequently using UDP port 4500 (NAT support required).	**P**	

Test ID	Cell Broadcast	Result	Comments
ACME_AP_07	Demonstrate that the AP is given an in-tunnel IP address from the pool provided.	**P**	

ACME_AP_08	Demonstrate that if there is a mismatch in Trust Anchors that the AP will not connect to a Security Gateway that it does not trust. This test is to check that the Security Gateway copes properly with the AP refusing to proceed with the connection due to the mismatch.	**P**	
ACME_AP_09	Demonstrate that if there is a mismatch in Trust Anchors that the Security Gateway will not accept an AP connection that it does not trust.	**P**	
ACME_AP_10	Demonstrate that the Security Gateway refuses IPsec connection from an AP that has an out-of-date certificate. (Use a Test Certificate on the AP).	**P**	
ACME_AP_11	Demonstrate that the IKE SA may be rekeyed repeatedly with the AP tunnel and the tunnels of other APs continuing to work. Demonstrate that rekey is successful while a UE has a speech call up, without any degradation of the voice quality.	**P**	
ACME_AP_12	Demonstrate that the CHILD SA may be rekeyed repeatedly with the AP tunnel and the tunnels of other APs continuing to work. Demonstrate that rekey is successful while a UE has a speech call up, without any degradation of the voice quality.	**P**	
ACME_AP_14	Demonstrate that the AP copes when the tunnel from Security Gateway killed.	**P**	
ACME_AP_15	Demonstrate that the AP sends new request to establish new tunnel when IPsec disabled and enabled in AP.	**P**	
ACME_AP_20	Demonstrate that the Security Gateway refuses connection from an AP that has a revoked certificate.	**P**	
ACME_AP_21	Establish tunnel from Femto side. Reboot client and ensure Dead Peer Detection clears tunnel on gateway side	**P**	

ACME_AP_22	Verify that the received IKE_AUTH message has TSr of 0.0.0.0/0 and the traffic-selector parameter that is defined in the MSG is included in the TSr of MSG's auth message (single traffic selector)	**P**	
ACME_AP_23	Verify that when there is no intersection between the received proposed TSr and the configured traffic-selectors, the MSG rejects the IKE_AUTH message with an TS_UNACCEPTABLE message.	**P**	
ACME_AP_24	Verify that the MSG correctly performs the intersection of a single received proposed TSr address with the configured traffic-selectors in determining the TSr listed in the MSG's AUTH message.	**P**	
ACME_AP_25	Verify that the MSG correctly performs the intersection of multiple received proposed TSr address with the configured traffic-selectors in determining the TSr listed in the MSG's AUTH message TSr payloads.	**P**	
ACME_AP_26	Support for multiple DNS servers in IKE negotiation	**P**	

Total: 22

Standalone

Test ID	Standalone	Result	Comments
ACME_AP_13	Demonstrate that the Security Gateway copes successfully when it is rebooted with several APs that have tunnels active. The APs must be able to set up new tunnels: the Security Gateway must not keep alive old tunnels for which it has lost state information.	**P**	

Total: 1

Redundancy

Test ID	Redundancy	Result	Comments
ACME_AP_16	Demonstrate that when the active Security Gateway is powered off that the passive Security Gateway takes control within one second and that AP tunnels in use remain up and operational.	**P**	
ACME_AP_17	Demonstrate that IPsec tunnels can continue to be set up and taken down on the active unit following a fail-over. Verify that the tunnels can be used for CS and PS calls from a UE through to the 3GAC.	**P**	
ACME_AP_18	Demonstrate that disconnecting the failover synchronisation cables for a period during which existing tunnels remain in effect and also new tunnels are created, and old tunnels are removed, that when the cables are reconnected that the system is still capable of correct fail-over, carrying all working IPsec tunnels with it ok.	**P**	
ACME_AP_19	Demonstrate that following multiple fail-overs the Security Gateway continues to work, with ability to create new IPsec tunnels and remove old tunnels, and maintain existing tunnels. Also that rekey will occur ok for both IKE and CHILD SAs for existing and new tunnels.	**P**	

Summary

This section provides a statistical summary of the testing.

Section	Total no. of tests	P	F	NP	NT	P*	UT
IPsec & Traffic	22						
Standalone	1						
Redundancy	4						
Total	27		0	0	0	0	0

Conclusions and Recommendations

The integration and interoperability between ip.access nano3G UTRAN N3G_2.0.5 and Oracle Communications Security Gateway has been completed successfully. No open issues reported.

References

1. Ip.access nano3G UTRAN and Oracle Communications Secuity Gateway test report
2. Oracle Communications Security Gateway Essentials Guide

Appendix – A: Sample Configuration (PKI Certificate based authentication)

```
certificate-record
        name                            MSGcert2013
        country                         <C>
        state                           <PLACE>
        locality                        <PLACE>
        organization                    ip.access Ltd
        unit                            3GAS Server
        common-name                     <FQDN>
        key-size                        1024
        alternate-name
        trusted                         enabled
        key-usage-list
                                        digitalSignature
                                        keyEncipherment
        extended-key-usage-list
                                        serverAuth
        options
certificate-record
        name                            CAcert
        country                         GB
        state                           Cambs
        locality                        Cambourne
        organization                    ip.access Ltd
        unit                            Root CA
        common-name                     100
        key-size                        1024
        alternate-name
        trusted                         enabled
        key-usage-list
                                        digitalSignature
                                        keyEncipherment
        extended-key-usage-list
                                        serverAuth
        options
certificate-record
        name                            OEMcert
        country                         GB
        state                           Cambs
        locality                        Cambourne
        organization                    ip.access Ltd
        unit                            OEM CA
        common-name                     101
        key-size                        1024
        alternate-name
        trusted                         enabled
        key-usage-list
                                        digitalSignature
                                        keyEncipherment
```

```
        extended-key-usage-list
                                        serverAuth
        options
data-flow
        name                            DataFlow1
        realm-id                        Core1
        group-size                      256
        upstream-rate                   0
        downstream-rate                 0
dpd-params
        name                            DpdParams1
        max-loop                        100
        max-endpoints                   25
        max-cpu-limit                   60
        load-max-loop                   40
        load-max-endpoints              5
        max-attempts                    5
        max-retrans                     3
host-routes
        dest-network                    10.x.y.0
        netmask                         255.255.255.0
        gateway                         10.x.0.1
        description                     NTP route
host-routes
        dest-network                    10.x.Z.0
        netmask                         255.255.255.0
        gateway                         10.X.Y.1
        description                     SCP/OMCR network
host-routes
        dest-network                    10.X.Y.0
        netmask                         255.255.255.0
        gateway                         10.Y.Z.1
        description                     AC Card1
host-routes
        dest-network                    10.X.Y.0
        netmask                         255.255.255.0
        gateway                         10.Y.Z.1
        description                     AC Card2
ike-certificate-profile
        identity                        <FQDN>
        end-entity-certificate          MSGcert
        trusted-ca-certificates
                                        OEMcert
        verify-depth                    3
ike-config
        state                           enabled
        ike-version                     2
        log-level                       DEBUG
        udp-port                        500
        negotiation-timeout             15
```

```
        event-timeout                   60
        phase1-mode                     main
        phase1-dh-mode                  dh-group2
        v2-ike-life-secs                28800
        v2-ipsec-life-secs              25200
        v2-rekey                        disabled
        anti-replay                     enabled
        phase1-life-seconds             3600
        phase1-life-secs-max            86400
        phase2-life-seconds             28800
        phase2-life-secs-max            86400
        phase2-exchange-mode            no-forward-secrecy
        shared-password
        eap-protocol                    eap-radius-passthru
        eap-bypass-identity             disabled
        addr-assignment                 local
        dpd-time-interval               60
        overload-threshold              100
        overload-interval               1
        overload-action                 none
        overload-critical-threshold     100
        overload-critical-interval      1
        red-port                        1995
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        sd-authentication-method        certificate
        certificate-profile-id
        id-auth-type                    idi
        account-group-list
ike-interface
        address                         <IP ADDRESS>
        realm-id                        Access1
        ike-mode                        responder
        local-address-pool-id-list      LocalPool1
        dpd-params-name                 DpdParams1
        v2-ike-life-secs                259200
        v2-ipsec-life-secs              43200
        v2-rekey                        enabled
        multiple-authentication         disabled
        multiple-child-sa-mode          none
        shared-password
        eap-protocol
        addr-assignment                 local
        sd-authentication-method        certificate
        certificate-profile-id-list     <FQDN>
        threshold-crossing-alert-group-name
        cert-status-check               disabled
        cert-status-profile-list
        access-control-name
```

```
        accounting-param-name
        traffic-selectors
        authorization                   disabled
ike-sainfo
        name                            sainfo1
        security-protocol               esp-auth
        auth-algo                       sha1
        encryption-algo                 aes
        ipsec-mode                      tunnel
        tunnel-local-addr               <ip Address>
        tunnel-remote-addr              *
ipsec-global-config
        red-ipsec-port                  1994
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
local-address-pool
        name                            LocalPool1
        address-range
                network-address                 10.X.0.0
                subnet-mask                     255.255.0.0
        dns-realm-id
        data-flow                       DataFlow1
network-interface
        name                            M00
        sub-port-id                     0
        description                     Public
        hostname
        ip-address                      <IP1>
        pri-utility-addr                <ip2>
        sec-utility-addr                <IP3>
        netmask                         255.255.255.224
        gateway                         <ipg>
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     <IP>
        ftp-address
        icmp-address                    <ip>
        snmp-address
        telnet-address
```

```
network-interface
        name                            M10
        sub-port-id                     0
        description                     Private
        hostname
        ip-address                      10.X.Y.z0
        pri-utility-addr                10.X.Y.z1
        sec-utility-addr                10.X.Y.z2
        netmask                         255.255.255.0
        gateway                         10.X.Y.z
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   1
                health-score                    25
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     10.X.Y.z0
        ftp-address
        icmp-address                    10.X.Y.z0
        snmp-address
        telnet-address
network-interface
        name                            wancom1
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                169.254.1.1
        sec-utility-addr                169.254.1.2
        netmask                         255.255.255.252
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list
```

```
        ftp-address
        icmp-address
        snmp-address
        telnet-address
network-interface
        name                            wancom2
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                169.254.2.1
        sec-utility-addr                169.254.2.2
        netmask                         255.255.255.252
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list
        ftp-address
        icmp-address
        snmp-address
        telnet-address
ntp-config
        server                          10.X.Y.2
        server                          10.X.Y.6
        server                          10.X.Y.10
        server                          10.X.Y.14
phy-interface
        name                            M00
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           1000
phy-interface
        name                            M10
        operation-type                  Media
        port                            0
```

```
        slot                            1
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           1000
phy-interface
        name                            wancom1
        operation-type                  Control
        port                            1
        slot                            0
        virtual-mac
        wancom-health-score             8
phy-interface
        name                            wancom2
        operation-type                  Control
        port                            2
        slot                            0
        virtual-mac
        wancom-health-score             9
realm-config
        identifier                      Access1
        description                     Access Side
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M00:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        class-profile
        average-rate-limit              0
```

```
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint

realm-config
        identifier                     Core1
        description                    Core Side
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M10:0
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
```

```
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        fallback-bandwidth             0
        max-priority-bandwidth         0
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
```

```
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint

redundancy-config
        state                           enabled
        log-level                       INFO
        health-threshold                75
        emergency-threshold             50
        port                            9090
        advertisement-time              500
        percent-drift                   210
        initial-time                    1250
        becoming-standby-time           180000
        becoming-active-time            100
        cfg-port                        1987
        cfg-max-trans                   10000
        cfg-sync-start-time             5000
        cfg-sync-comp-time              1000
        gateway-heartbeat-interval      0
        gateway-heartbeat-retry         0
        gateway-heartbeat-timeout       1
        gateway-heartbeat-health        0
        media-if-peercheck-time         0
        peer
                name                            ACMESeGw1
                state                           enabled
                type                            Primary
                destination
                        address                         169.254.2.1:9090
                        network-interface               wancom2:0
                destination
                        address                         169.254.1.1:9090
                        network-interface               wancom1:0
        peer
                name                            ACMESeGw2
                state                           enabled
                type                            Secondary
                destination
                        address                         169.254.2.2:9090
                        network-interface               wancom2:0
                destination
                        address                         169.254.1.2:9090
                        network-interface               wancom1:0
security-policy
        name                            ikepol1
        network-interface               M00:0
        priority                        10
```

```
        local-ip-addr-match             <IP>
        remote-ip-addr-match            0.0.0.0
        local-port-match                500
        remote-port-match               0
        trans-protocol-match            ALL
        direction                       both
        local-ip-mask                   255.255.255.255
        remote-ip-mask                  0.0.0.0
        action                          allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                   255.255.255.255
                remote-ip-mask                  255.255.255.255
                local-port-mask                 0
                remote-port-mask                0
                trans-protocol-mask             0
                valid                           enabled
                vlan-mask                       0xFFF
security-policy
        name                            ikepol4500
        network-interface               M00:0
        priority                        2
        local-ip-addr-match             <IP>
        remote-ip-addr-match            0.0.0.0
        local-port-match                4500
        remote-port-match               0
        trans-protocol-match            ALL
        direction                       both
        local-ip-mask                   255.255.255.255
        remote-ip-mask                  0.0.0.0
        action                          allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                   255.255.255.255
                remote-ip-mask                  255.255.255.255
                local-port-mask                 0
                remote-port-mask                0
                trans-protocol-mask             0
                valid                           enabled
                vlan-mask                       0xFFF
security-policy
        name                            access-ipsec-1
        network-interface               M00:0
        priority                        100
        local-ip-addr-match             0.0.0.0
        remote-ip-addr-match            10.X.0.0
        local-port-match                0
        remote-port-match               0
        trans-protocol-match            ALL
        direction                       both
```

```
        local-ip-mask                   0.0.0.0
        remote-ip-mask                  255.255.0.0
        action                          ipsec
        ike-sainfo-name                 sainfo1
        outbound-sa-fine-grained-mask
                local-ip-mask                   0.0.0.0
                remote-ip-mask                  255.255.255.255
                local-port-mask                 0
                remote-port-mask                0
                trans-protocol-mask             0
                valid                           enabled
                vlan-mask                       0xFFF
system-config
        hostname                        ACMESeGw1
        description
        location
        mib-system-contact              Acmecontact
        mib-system-name                 AcmeMSG
        mib-system-location             <PLACE>
        snmp-enabled                    enabled
        enable-snmp-auth-traps          enabled
        enable-snmp-syslog-notify       enabled
        enable-snmp-monitor-traps       enabled
        enable-env-monitor-traps        enabled
        snmp-syslog-his-table-length    1
        snmp-syslog-level               WARNING
        system-log-level                WARNING
        process-log-level               NOTICE
        process-log-ip-address          0.0.0.0
        process-log-port                0
        collect
                sample-interval                 5
                push-interval                   15
                boot-state                      disabled
                start-time                      now
                end-time                        never
                red-collect-state               disabled
                red-max-trans                   1000
                red-sync-start-time             5000
                red-sync-comp-time              1000
                push-success-trap-state         disabled
        call-trace                      disabled
        internal-trace                  disabled
        log-filter                      all
        default-gateway                 <IP>
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
```

```
        cli-audit-trail                 enabled
        link-redundancy-state           disabled
        source-routing                  enabled
        cli-more                        disabled
        terminal-height                 24
        debug-timeout                   0
        trap-event-lifetime             1
        cleanup-time-of-day             00:00
```

Appendix B – Oracle Communications Security Gateway SW 3.0 highlights

This section highlights some of the important additions and feature inclusions in Oracle Communications Security Gateway SW 3.0 and the hardware requisite. (For detailed features and description, please review the Oracle Communications Security Gateway MC-X 3.0 Essentials Guide – February 2014)

Acme Packet 4500 platform support

10G 2 port ETC2 NIU with Cavium (SW 2.0 requires 4x1G HiFN based NIU)

IPv6 support (configuration and new show commands)

- IPv6 IKE interface, IPv6 peer support
- IPv6 local address pool
- IPv6 tunnels (local address assignment as well as via external Radius server)
- IPv6 contents in IDi, IDr, Traffic selector, CFG_REQUEST and CFG_REPLY payloads

Certicate related changes (SHA-256 support, subject alternative name extension support, Key Usage extension)

Authentication/Authorization server per ike-interface

Persistent tunnel addressing (resume previously assigned tunnel local address in case of UE reboot)

Configure multiple traffic selectors

For upgrading an exsiting Oracle Communications Security gateway Acme Packet 4500 platform which is installed and running with 4x1G NIU and SW 2.0 to SW 3.0m2p1, please peruse and follow instructions specified in document – **"Oracle Communications Security Gateway – MOP for Installation of 10G ETC2 NIU and upgrade existing 4500 system to SW 3.0m2p2"**

Appendix C – Reference configuration (Use of CRL)

```
cert-status-profile
       name                              IPAoemCRL
       ip-address                        10.m.n.p
       hostname
       port                              80
       type                              CRL
       trans-proto                       HTTP
       requestor-cert
       responder-cert                    IPAoemCert
       realm-id                          Core1
       retry-count                       3
       dead-time                         0
       crl-update-interval               86400
       crl-list
/crl/crl.ipaccess.com/ipaccessltd_oemca_101_100.crl

certificate-record
       name                              IPArootCert
       country                           GB
       state                             Cambs
       locality                          Cambourne
       organization                      ip.access Ltd
       unit                              Root CA
       common-name                       100
       key-size                          2048
       alternate-name
       trusted                           enabled
       key-usage-list
                                         digitalSignature
                                         keyEncipherment
       extended-key-usage-list
                                         serverAuth
       options

certificate-record
       name                              IPAoemCert
       country                           GB
       state                             Cambs
       locality                          Cambourne
       organization                      ip.access Ltd
       unit                              OEM CA
       common-name                       101
       key-size                          2048
       alternate-name
       trusted                           enabled
       key-usage-list
                                         digitalSignature
                                         keyEncipherment
```

```
       extended-key-usage-list
                                    serverAuth
       options

certificate-record
       name                         fqdnCert
       country                      <C>
       state                        <State>
       locality                     <Loc>
       organization                 ip.access Ltd
       unit                         3GAS Server
       common-name                  <FQDN>
       key-size                     2048
       alternate-name
       trusted                      enabled
       key-usage-list
                                    digitalSignature
                                    keyEncipherment
       extended-key-usage-list
                                    serverAuth
       options

certificate-record
       name                         Cust2014
       country                      <C>
       state                        <state>
       locality                     <loc>
       organization                 ip.access Ltd
       unit                         3GAS Server
       common-name                  <fqdn>
       key-size                     1024
       alternate-name
       trusted                      enabled
       key-usage-list
                                    digitalSignature
                                    keyEncipherment
       extended-key-usage-list
                                    serverAuth
       options

data-flow
       name                         DataFlow1
       realm-id                     Core1
       group-size                   256
       upstream-rate                0
       downstream-rate              0

dpd-params
       name                         DpdParams1
       max-loop                     100
```

```
       max-endpoints                   25
       max-cpu-limit                   60
       load-max-loop                   40
       load-max-endpoints              5
       max-attempts                    5
       max-retrans                     3

host-routes
       dest-network                    10.m.n.64
       netmask                         255.255.255.192
       gateway                         10.m.n.225
       description

host-routes
       dest-network                    10.b.c.28
       netmask                         255.255.255.255
       gateway                         10.m.n.225
       description                     Internal DNS

host-routes
       dest-network                    10.b.c.d
       netmask                         255.255.255.255
       gateway                         10.m.n.225
       description                     Internal DNS

host-routes
       dest-network                    10.b.c.d1
       netmask                         255.255.255.255
       gateway                         10.m.n.225
       description                     Internal DNS

ike-certificate-profile
       identity                        <fqdn>
       end-entity-certificate          Cust2014
       trusted-ca-certificates
                                       IPAoemCert
       verify-depth                    0
ike-config
       state                           enabled
       ike-version                     2
       log-level                       INFO
       udp-port                        500
       negotiation-timeout             15
       event-timeout                   60
       phase1-mode                     main
       phase1-dh-mode                  dh-group2
       v2-ike-life-secs                28800
       v2-ipsec-life-secs              25200
       v2-rekey                        disabled
       anti-replay                     enabled
```

```
       phase1-life-seconds             3600
       phase1-life-secs-max            86400
       phase2-life-seconds             28800
       phase2-life-secs-max            86400
       phase2-exchange-mode            no-forward-secrecy
       shared-password
       eap-protocol                    eap-radius-passthru
       eap-bypass-identity             disabled
       addr-assignment                 local
       dpd-time-interval               60
       overload-threshold              100
       overload-interval               1
       overload-action                 none
       overload-critical-threshold     100
       overload-critical-interval      1
       red-port                        1995
       red-max-trans                   10000
       red-sync-start-time             5000
       red-sync-comp-time              1000
       sd-authentication-method        certificate
       certificate-profile-id
       id-auth-type                    idi
       options                         assume-initial-contact
       account-group-list
ike-interface
       address                         e.f.g.h0
       realm-id                        Access1
       ike-mode                        responder
       local-address-pool-id-list      LocalPool1
       dpd-params-name                 DpdParams1
       v2-ike-life-secs                259200
       v2-ipsec-life-secs              43200
       v2-rekey                        enabled
       multiple-authentication         disabled
       multiple-child-sa-mode          none
       shared-password
       eap-protocol
       addr-assignment                 local
       sd-authentication-method        certificate
       certificate-profile-id-list     <fqdn>
       threshold-crossing-alert-group-name
       cert-status-check               disabled
       cert-status-profile-list        IPAoemCRL
       access-control-name
       accounting-param-name
       traffic-selectors               10.0.0.0/8
       ip-subnets
       authorization                   disabled
ike-sainfo
       name                            sainfo1
```

```
        security-protocol               esp-auth
        auth-algo                       sha1
        encryption-algo                 aes
        ipsec-mode                      tunnel
        tunnel-local-addr               e.f.g.h0
        tunnel-remote-addr              *
ipsec-global-config
        red-ipsec-port                  1994
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
local-address-pool
        name                            LocalPool1
        address-range
                network-address                 10.g.h.0
                subnet-mask                     255.255.248.0
        dns-assignment
        dns-realm-id                    Core1
        data-flow                       DataFlow1
network-interface
        name                            wancom1
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                169.254.1.1
        sec-utility-addr                169.254.1.2
        netmask                         255.255.255.252
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list
        ftp-address
         icmp-address
        snmp-address
        telnet-address
         neighbor-list
network-interface
        name                            wancom2
        sub-port-id                     0
```

```
       description
       hostname
       ip-address
       pri-utility-addr              169.254.2.1
       sec-utility-addr              169.254.2.2
       netmask                       255.255.255.252
       gateway
       sec-gateway
       gw-heartbeat
              state                         disabled
              heartbeat                     0
              retry-count                   0
              retry-timeout                 1
              health-score                  0
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                   11
        hip-ip-list
       ftp-address
        icmp-address
       snmp-address
       telnet-address
        neighbor-list
network-interface
       name                          M00
       sub-port-id                   0
       description                   Public Access Side
       hostname
       ip-address                    e.f.g.h0
       pri-utility-addr              e.f.g.h1
       sec-utility-addr              e.f.g.h2
       netmask                       255.255.255.0
       gateway                       e.f.g.h
       sec-gateway
       gw-heartbeat
              state                         disabled
              heartbeat                     0
              retry-count                   0
              retry-timeout                 1
              health-score                  0
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                   11
        hip-ip-list                   e.f.g.h0
       ftp-address
        icmp-address                  e.f.g.h0
```

```
       snmp-address
       telnet-address
        neighbor-list
network-interface
       name                            M10
       sub-port-id                     0
       description                     Private
       hostname
       ip-address                      x.y.z.b0
       pri-utility-addr                x.y.z.b1
       sec-utility-addr                x.y.z.b2
       netmask                         255.255.255.240
       gateway                         x.y.z.225
       sec-gateway
       gw-heartbeat
              state                           disabled
              heartbeat                       0
              retry-count                     0
              retry-timeout                   1
              health-score                    0
       dns-ip-primary                  10.a.b.c1
       dns-ip-backup1                  10.a.b.c2
       dns-ip-backup2                  10.a.b.c3
       dns-domain                      <fqdn>
       dns-timeout                     11
        hip-ip-list                     x.y.z.b0
       ftp-address
        icmp-address                    x.y.z.b0
       snmp-address
       telnet-address
        neighbor-list
ntp-config
       server                          10.n.p.q1
       server                          10.n.p.q2
       server                          10.n.p.q3
       server                          10.n.p.q4
phy-interface
       name                            wancom1
       operation-type                  Control
       port                            1
       slot                            0
       virtual-mac
       wancom-health-score             8
phy-interface
       name                            wancom2
       operation-type                  Control
       port                            2
       slot                            0
       virtual-mac
       wancom-health-score             9
```

```
phy-interface
       name                            M00
       operation-type                  Media
       port                            0
       slot                            0
       virtual-mac                     <MAC>
       admin-state                     enabled
       auto-negotiation                enabled
       duplex-mode                     FULL
       speed                           100
phy-interface
       name                            M10
       operation-type                  Media
       port                            0
       slot                            1
       virtual-mac                     <MAC>
       admin-state                     enabled
       auto-negotiation                enabled
       duplex-mode                     FULL
       speed                           100
realm-config
       identifier                      Core1
       description                     Core
       addr-prefix                     0.0.0.0
       network-interfaces
                                       M10:0
       mm-in-realm                     disabled
       mm-in-network                   enabled
       mm-same-ip                      enabled
       mm-in-system                    enabled
       bw-cac-non-mm                   disabled
       msm-release                     disabled
       generate-UDP-checksum           disabled
       max-bandwidth                   0
       fallback-bandwidth              0
       max-priority-bandwidth          0
       max-latency                     0
       max-jitter                      0
       max-packet-loss                 0
       observ-window-size              0
       parent-realm
       dns-realm
       media-policy
       in-translationid
       out-translationid
       in-manipulationid
       out-manipulationid
       manipulation-string
       class-profile
       average-rate-limit              0
```

```
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
realm-config
        identifier                     Access1
        description                    Access
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M00:0
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        generate-UDP-checksum          disabled
```

```
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
```

```
       stun-changed-ip                 0.0.0.0
       stun-changed-port               3479
       match-media-profiles
       qos-constraint
redundancy-config
       state                           enabled
       log-level                       INFO
       health-threshold                75
       emergency-threshold             50
       port                            9090
       advertisement-time              500
       percent-drift                   210
       initial-time                    1250
       becoming-standby-time           180000
       becoming-active-time            100
       cfg-port                        1987
       cfg-max-trans                   10000
       cfg-sync-start-time             5000
       cfg-sync-comp-time              1000
       gateway-heartbeat-interval      0
       gateway-heartbeat-retry         0
       gateway-heartbeat-timeout       1
       gateway-heartbeat-health        0
       media-if-peercheck-time         500
       peer
              name                             femtosegw1
              state                            enabled
              type                             Primary
              destination
                     address                          169.254.1.1:9090
                     network-interface                wancom1:0
              destination
                     address                          169.254.2.1:9090
                     network-interface                wancom2:0
       peer
              name                             femtosegw2
              state                            enabled
              type                             Secondary
              destination
                     address                          169.254.2.2:9090
                     network-interface                wancom2:0
              destination
                     address                          169.254.1.2:9090
                     network-interface                wancom1:0
security-policy
       name                            ike500pol1
       network-interface               M00:0
       priority                        10
       local-ip-addr-match             x.y.z.a
       remote-ip-addr-match            0.0.0.0
```

```
        local-port-match                500
        remote-port-match               0
        trans-protocol-match            ALL
        direction                       both
        local-ip-mask                   255.255.255.255
        remote-ip-mask                  0.0.0.0
        action                          allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                   255.255.255.255
                remote-ip-mask                  255.255.255.255
                local-port-mask                 0
                remote-port-mask                0
                trans-protocol-mask             0
                valid                           enabled
                vlan-mask                       0xFFF
security-policy
        name                            ike4500pol1
        network-interface               M00:0
        priority                        1
        local-ip-addr-match             a.b.c.d
        remote-ip-addr-match            0.0.0.0
        local-port-match                4500
        remote-port-match               0
        trans-protocol-match            ALL
        direction                       both
        local-ip-mask                   255.255.255.255
        remote-ip-mask                  0.0.0.0
        action                          allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                   255.255.255.255
                remote-ip-mask                  255.255.255.255
                local-port-mask                 0
                remote-port-mask                0
                trans-protocol-mask             0
                valid                           enabled
                vlan-mask                       0xFFF
security-policy
        name                            access-ipsec-1
        network-interface               M00:0
        priority                        100
        local-ip-addr-match             0.0.0.0
        remote-ip-addr-match            10.5.32.0
        local-port-match                0
        remote-port-match               0
        trans-protocol-match            ALL
        direction                       both
        local-ip-mask                   0.0.0.0
        remote-ip-mask                  255.255.248.0
```

```
       action                          ipsec
       ike-sainfo-name                 sainfo1
       outbound-sa-fine-grained-mask
              local-ip-mask                   0.0.0.0
              remote-ip-mask                  255.255.255.255
              local-port-mask                 0
              remote-port-mask                0
              trans-protocol-mask             0
              valid                           enabled
              vlan-mask                       0xFFF
snmp-community
       community-name                  public
       access-mode                     READ-ONLY
       ip-addresses
                                       10.x.y.z1
                                       10.x.y.z1
                                       10.x.y.z2
system-config
       hostname                        CustSeGW
       description
       location
       mib-system-contact              Acmecontact
       mib-system-name                 AcmeMSG
       mib-system-location             <C>
       snmp-enabled                    enabled
       enable-snmp-auth-traps          enabled
       enable-snmp-syslog-notify       enabled
       enable-snmp-monitor-traps       enabled
       enable-env-monitor-traps        enabled
       snmp-syslog-his-table-length    1
       snmp-syslog-level               WARNING
       system-log-level                WARNING
       process-log-level               NOTICE
       process-log-ip-address          0.0.0.0
       process-log-port                0
       collect
              sample-interval                 5
              push-interval                   15
              boot-state                      disabled
              start-time                      now
              end-time                        never
              red-collect-state               disabled
              red-max-trans                   1000
              red-sync-start-time             5000
              red-sync-comp-time              1000
              push-success-trap-state         disabled
       call-trace                      disabled
       internal-trace                  disabled
       log-filter                      all
       default-gateway                 e.f.g.h
```

```
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
        cli-audit-trail                 enabled
        link-redundancy-state           disabled
        source-routing                  enabled
        cli-more                        disabled
        terminal-height                 24
        debug-timeout                   0
        trap-event-lifetime             0
        cleanup-time-of-day             00:00
```

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together