Best Current Practice
OCSBC – 9.2 to 9.3 IPsec upgrade
Category: Informational
March 2025, Version 1.00

Revision History

Version	Author	Description of Changes	Date Revision Completed
0.00	Matej Maric	Initial version	11.3.2025
1.00	Matej Maric	Ikev2 and responder role tested	29.4.2025

Abstract

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.
The configurations provided in this document SHOULD NOT be treated as RECOMMENDED. The information is intended to provide guidance as to the OCSBC behavior when configurations listed in this document are applied.
This document is intended to provide the reader with information regarding configuration of an OCSBC to provide user authentication via several RADIUS servers.

Applicability

The details provided are relevant to physical & virtual Oracle Communications Session Border Controller (OCSBC) instances before upgrade to 9.3. Document will detail the best approach to migrate to 9.3 for customers having multiple IPsec tunnels in prior versions, negotiated with 9.3 deprecated ciphers. Instructions are valid for ikev1 and ikev2 with PSK in use.

Table of content

Contents

Changes introduced with 9.3 impacting IPsec functionality

The S-Cz9.3.0 SBC release includes a Mocana version upgrade that generates important changes to the ciphers you should use with the SBC. The latest Mocana 7.0 software code disables weak ciphers/algorithms used by IKE-based IPsec tunnels. Removal of these weak ciphers is mandated by Oracle Security standards. If in use, you should consider replacing deprecated ciphers in your configuration. Changes introduced have impact on both, IKE secure exchange protocol method and IPsec SA authentication and encryption algorithms.

- Concerning IKE exchange, dh-group2(mod1024) is removed from the supported list of DH groups

- Concerning IPsec SA authentication, sha1 and md5 are removed from auth-alg list
- Concerning IPsec SA encryption, 3des and null are removed from encryption-alg list

IPsec generic introduction

IPsec (Internet Protocol Security) is a suite of protocols used to secure network communications by authenticating and encrypting IP packets. It relies on the **IKE (Internet Key Exchange)** protocol to establish security associations (SAs) between peers.

IPsec IKEv1 vs IKEv2 Comparison

Feature	IKEv1	IKEv2
Introduced	1998 (RFC 2409)	2005 (RFC 4306, updated in RFC 7296)
Phases	Two phases: Phase 1 (Main/Aggressive Mode) and Phase 2 (Quick Mode)	Single phase, simplifying the exchange process
Performance	More overhead, slower negotiation	Faster, more efficient
Reliability	Limited support for NAT traversal, less efficient failure handling	Built-in NAT traversal, better resilience and failover
Mobility	No built-in support for mobility	Supports MOBIKE for better mobile client support
Flexibility	More complex, less adaptable	More robust and adaptable to modern networks
Security	More vulnerable to DoS attacks, lacks built-in anti-replay protection	Stronger security, includes anti-replay protection and improved authentication

Conclusion:
IKEv2 is a significant improvement over IKEv1 in terms of security, performance, and efficiency. It is the preferred choice for modern IPsec VPN implementations.

IKEv1 Message Exchange

IKEv1 Phase 1 (Main Mode)

Initiator	Message	Responder
Initiator	SA Proposal -->	
	<-- SA Proposal Accepted	Responder
Initiator	Key Exchange -->	
	<-- Key Exchange	Responder
Initiator	Authentication -->	
	<-- Authentication	Responder
	(Secure tunnel established for Phase 2)	

IKEv1 Phase 2 (Quick Mode)

Initiator	Message	Responder
Initiator	SA Negotiation -->	
	<-- SA Negotiation Response	Responder
Initiator	Key Exchange -->	
	<-- Key Exchange	Responder
Initiator	Authentication -->	
	<-- Authentication	Responder
	(IPsec tunnel established)	

Phase 1: Establishes a secure, authenticated channel between peers (ISAKMP SA).
Phase 2: Negotiates IPsec SAs for encrypting traffic.

IKEv2 Message Exchange

Initiator	Message	Responder	Description
Initiator	IKE_SA_INIT Request -->		Initiator proposes cryptographic algorithms and sends key material
	<-- IKE_SA_INIT Response	Responder	Responder agrees on algorithms and responds with key material
Initiator	IKE_AUTH Request -->		Initiator authenticates and sends identity information
	<-- IKE_AUTH Response	Responder	Responder authenticates and sends identity information
	(IKE SA established)		Secure tunnel established for child SA setup
Initiator	CREATE_CHILD_SA Request -->		Negotiation of additional child SA parameters
	<-- CREATE_CHILD_SA Response	Responder	Agreement on child SA parameters
	(IPsec tunnel established)		Secure IPsec tunnel setup

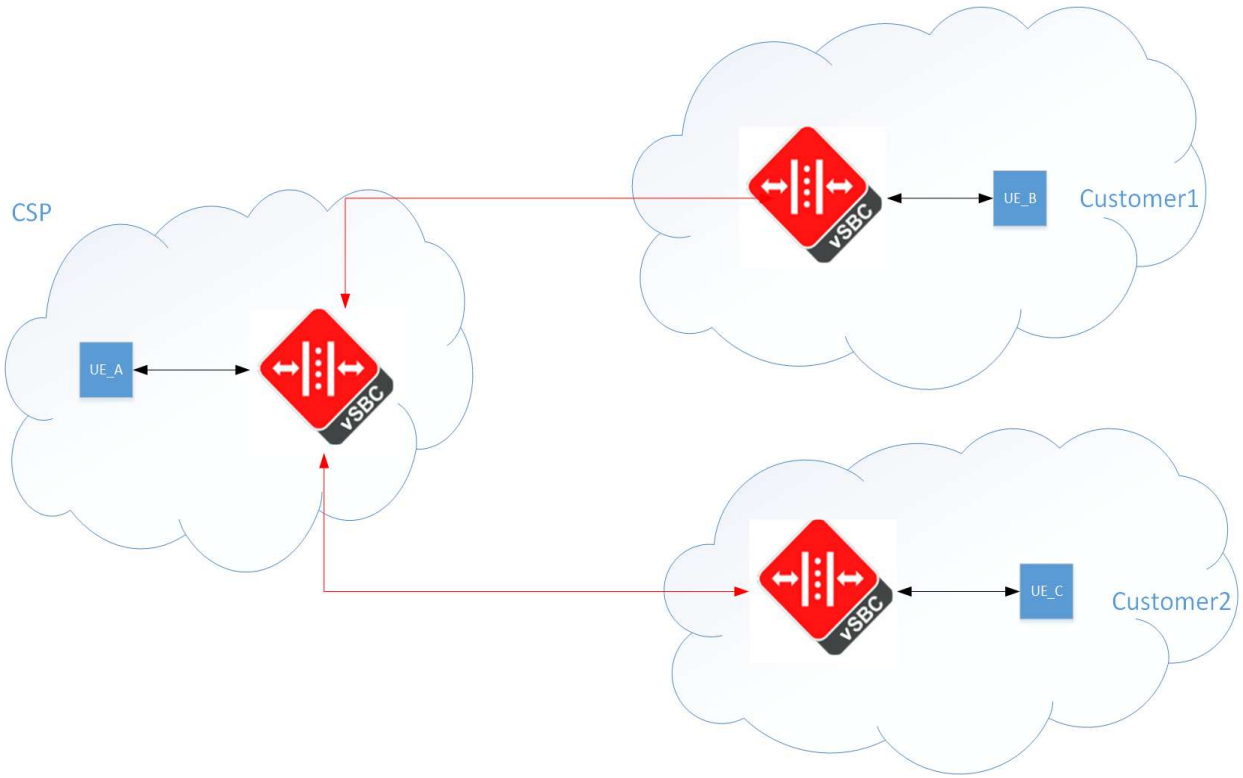
Software

Software SBC - SCZ920.p6
Software OCOM – 6.0

Problem statement and challenges

Focus of this BCP is on how to prepare SBC running in version lower than 9.3 for as less affecting 9.3 upgrade with minimal service disruption. SBC handling multiple tunnels that were set up at point of time and need sudden reconfiguration are a challenge for several reasons, main being one that customer cannot manage some global SBC changes without affecting all the tunnels and gathering different group of people responsible for remote tunnel end becomes mission impossible. This BCP should provide guidance on best steps to take for this migration but outcome also gives an idea of what SBC blueprint configuration might be that may make future maintenance easier.

LAB IPsec testing topology



Disclaimer on test coverage

Testing scope of this BCP includes ONLY DH groups and authentication and encryption algorithms outlined in this document. Any other combination should be thoroughly tested in lab premises following same procedure before any live activities.

SBC IPSec configuration objects

SBC in SP infrastructure

This is the SBC that needs to move to 9.3 and has both remote tunnels negotiated using 9.3 deprecated IKE DH phase1 group mod1024 (dh-group2). In addition, one remote peer has fixated but 9.3 deprecated IPsec SA encryption and authentication algorithm. Let us list the relevant configuration parts

```
SP_SBC# sho configuration ike-config
ike-config
      state                         enabled
      ike-version                     1
      log-level                     INFO
      udp-port                      500
      negotiation-timeout             15
      event-timeout                 60
      phase1-mode                    main
      phase1-dh-mode                 dh-group2
      phase2-exchange-mode           dh-group2
      v2-ike-life-secs              86400
      v2-ipsec-life-secs            28800
      v2-rekey                    enabled
      anti-replay                 enabled
      phase1-life-seconds             3600
      phase1-life-secs-max            86400
      phase2-life-seconds             28800
      phase2-life-secs-max            86400
      shared-password               ********
      eap-protocol                eap-radius-passthru
      eap-bypass-identity             disabled
      red-port                    0
      red-max-trans                 10000
```

```
        red-sync-start-time                5000
        red-sync-comp-time                 1000
        dpd-time-interval                  0
        overload-threshold                 100
        overload-interval                  1
        overload-action                    none
        overload-critical-threshold        100
        overload-critical-interval         1
        sd-authentication-method           shared-password
        certificate-profile-id
        id-auth-type                       idi
        options
        last-modified-by                   admin@10.0.15.149
        last-modified-date                 2025-03-11 08:56:00
    ikev2-ipsec-wancom0-params

SP_SBC# sho configuration ike-interface
ike-interface
        state                      enabled
        ike-version                1
        address                    10.0.17.40
        realm-id                   Core
        ike-mode                   initiator
        dpd-params-name
        v2-ike-life-secs           86400
        v2-ipsec-life-secs         28800
        v2-rekey                   none
        v1-ike-life-secs           3600
        v1-ipsec-life-secs         28800
        esnSupport                 disabled
        shared-password            ********
        eap-protocol
        sd-authentication-method   shared-password
        certificate-profile-id-list
        cert-status-check          disabled
        cert-status-profile-list
        access-control-name
        tunnel-orig-name-list
        options
        last-modified-by           admin@10.0.15.149
        last-modified-date         2025-03-10 13:27:19
ike-interface
        state                      enabled
```

```
        ike-version                     1
        address                         10.0.17.41
        realm-id                        Core1
        ike-mode                        initiator
        dpd-params-name
        v2-ike-life-secs                86400
        v2-ipsec-life-secs              28800
        v2-rekey                        none
        v1-ike-life-secs                3600
        v1-ipsec-life-secs              28800
        esnSupport                      disabled
        shared-password                 ********
        eap-protocol
        sd-authentication-method        shared-password
        certificate-profile-id-list
        cert-status-check               disabled
        cert-status-profile-list
        access-control-name
        tunnel-orig-name-list
        options
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-11 08:45:47
SP_SBC# sho configuration ike-sainfo
ike-sainfo
        name                            customer2
        security-protocol               esp-auth
        auth-algo                       sha1
        encryption-algo                 3des
        ipsec-mode                      tunnel
        tunnel-local-addr               10.0.17.41
        tunnel-remote-addr              10.0.17.19
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-11 08:44:25
ike-sainfo
        name                            ipsec
        security-protocol               esp-auth
        auth-algo                       sha2-512
        encryption-algo                 aes-ctr
        ipsec-mode                      tunnel
        tunnel-local-addr               10.0.17.40
        tunnel-remote-addr              10.0.17.19
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-10 21:04:47
```

```
SP_SBC# sho configuration security-policy short
security-policy
        name                    pol1
        network-interface               S1P0:0.4
        local-ip-addr-match             10.0.17.40
        remote-ip-addr-match                10.0.17.19
        local-port-match                500
        local-port-match-max                4500
        remote-port-match               500
        remote-port-match-max               4500
        action                  allow
security-policy
        name                    pol2
        network-interface               S1P0:0.4
        priority                2
        local-ip-addr-match             10.0.17.40
        remote-ip-addr-match                10.0.17.19
        ike-sainfo-name                 ipsec
security-policy
        name                    pol33
        network-interface               S1P0:0.4
        priority                1
        local-ip-addr-match             10.0.17.41
        remote-ip-addr-match                10.0.17.19
        local-port-match                500
        local-port-match-max                4500
        remote-port-match               500
        remote-port-match-max               4500
        action                  allow
security-policy
        name                    pol35
        network-interface               S1P0:0.4
        priority                5
        local-ip-addr-match             10.0.17.41
        remote-ip-addr-match                10.0.17.19
        ike-sainfo-name                 customer2
```

Note down the relevant parts bolded and highlighted yellow! All these are deprecated in 9.3 and blind upgrade would lead to all IPsec tunnels down!

Remote SBC in customer1 infrastructure

```
ike-config
        state                         enabled
        ike-version                     1
        log-level                     INFO
        udp-port                      500
        negotiation-timeout             15
        event-timeout                 60
        phase1-mode                    main
        phase1-dh-mode                 dh-group2
        phase2-exchange-mode           dh-group2
        v2-ike-life-secs              86400
        v2-ipsec-life-secs             28800
        v2-rekey                      enabled
        anti-replay                   enabled
        phase1-life-seconds             3600
        phase1-life-secs-max            86400
        phase2-life-seconds             28800
        phase2-life-secs-max            86400
        shared-password               ********
        eap-protocol                  eap-radius-passthru
        eap-bypass-identity             disabled
        red-port                      0
        red-max-trans                 10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        dpd-time-interval              0
        overload-threshold              100
        overload-interval              1
        overload-action                none
        overload-critical-threshold       100
        overload-critical-interval        1
        sd-authentication-method          shared-password
        certificate-profile-id
        id-auth-type                  idi
        options
        last-modified-by              admin@10.0.15.149
        last-modified-date             2025-03-10 20:33:50
customer1# sho configuration ike-interface
ike-interface
        state                         enabled
```

```
        ike-version                     1
        address                         10.0.17.19
        realm-id                        CoreAS
        ike-mode                        responder
        dpd-params-name
        v2-ike-life-secs                86400
        v2-ipsec-life-secs              28800
        v2-rekey                        none
        v1-ike-life-secs                3600
        v1-ipsec-life-secs              28800
        esnSupport                      disabled
        shared-password                 ********
        eap-protocol
        sd-authentication-method        shared-password
        certificate-profile-id-list
        cert-status-check               disabled
        cert-status-profile-list
        access-control-name
        tunnel-orig-name-list
        options
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-10 13:24:11
customer1# sho configuration ike-sainfo
ike-sainfo
        name                            customer1
        security-protocol               esp-auth
        auth-algo                       sha2-512
        encryption-algo                 aes-ctr
        ipsec-mode                      tunnel
        tunnel-local-addr               10.0.17.19
        tunnel-remote-addr              10.0.17.40
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-10 21:05:52
customer1# sho configuration security-policy short
security-policy
        name                            pol1
        network-interface               S1P0:0.4
        local-ip-addr-match             10.0.17.19
        remote-ip-addr-match            10.0.17.40
        local-port-match                500
        local-port-match-max            4500
        remote-port-match               500
        remote-port-match-max           4500
```

```
        action                  allow
security-policy
        name                    pol2
        network-interface               S1P0:0.4
        priority                2
        local-ip-addr-match             10.0.17.19
        remote-ip-addr-match                10.0.17.40
        ike-sainfo-name                 customer1
```

To be noted here what is bolded and highlighted yellow at remote peer, in same time deprecated in 9.3 release. At this remote peer, only problematic part is IKE phase1 DH group selection.

Remote SBC in customer2 infrastructure

```
ike-config
        state                   enabled
        ike-version               1
        log-level               INFO
        udp-port                500
        negotiation-timeout             15
        event-timeout             60
        phase1-mode               main
        phase1-dh-mode                  dh-group2
        phase2-exchange-mode                dh-group2
        v2-ike-life-secs            86400
        v2-ipsec-life-secs            28800
        v2-rekey                enabled
        anti-replay             enabled
        phase1-life-seconds             3600
        phase1-life-secs-max              86400
        phase2-life-seconds             28800
        phase2-life-secs-max              86400
        shared-password                 ********
        eap-protocol              eap-radius-passthru
```

```
        eap-bypass-identity             disabled
        red-port                        0
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        dpd-time-interval               0
        overload-threshold              100
        overload-interval               1
        overload-action                 none
        overload-critical-threshold     100
        overload-critical-interval      1
        sd-authentication-method        shared-password
        certificate-profile-id
        id-auth-type                    idi
        options
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-10 20:33:50
customer2# sho configuration ike-interface
ike-interface
        state                           enabled
        ike-version                     1
        address                         10.0.17.19
        realm-id                        CoreAS
        ike-mode                        responder
        dpd-params-name
        v2-ike-life-secs                86400
        v2-ipsec-life-secs              28800
        v2-rekey                        none
        v1-ike-life-secs                3600
        v1-ipsec-life-secs              28800
        esnSupport                      disabled
        shared-password                 ********
        eap-protocol
        sd-authentication-method        shared-password
        certificate-profile-id-list
        cert-status-check               disabled
        cert-status-profile-list
        access-control-name
        tunnel-orig-name-list
        options
        last-modified-by                admin@10.0.15.149
        last-modified-date              2025-03-10 13:24:11
customer2# sho configuration ike-sainfo
```

```
ike-sainfo
        name                    customer2
        security-protocol       esp-auth
        auth-algo               sha1
        encryption-algo         3des
        ipsec-mode              tunnel
        tunnel-local-addr       10.0.17.19
        tunnel-remote-addr      10.0.17.41
        last-modified-by        admin@10.0.15.149
        last-modified-date      2025-03-11 08:36:27
customer2# sho configuration security-policy short
security-policy
        name                    pol23
        network-interface       S1P0:0.4
        priority                1
        local-ip-addr-match     10.0.17.19
        remote-ip-addr-match    10.0.17.41
        local-port-match        500
        local-port-match-max    4500
        remote-port-match-max   4500
        action                  allow
security-policy
        name                    pol34
        network-interface       S1P0:0.4
        priority                5
        local-ip-addr-match     10.0.17.19
        remote-ip-addr-match    10.0.17.41
        ike-sainfo-name         customer2
```

To be noted what is highlighted yellow and bolded, in same time deprecated in SBC release 9.3. At customer2, we have problem with IKE phase1 dh-group selection, but also encryption and authentication IPSEC SA algorithms.

Remote SBC in customerN infrastructure

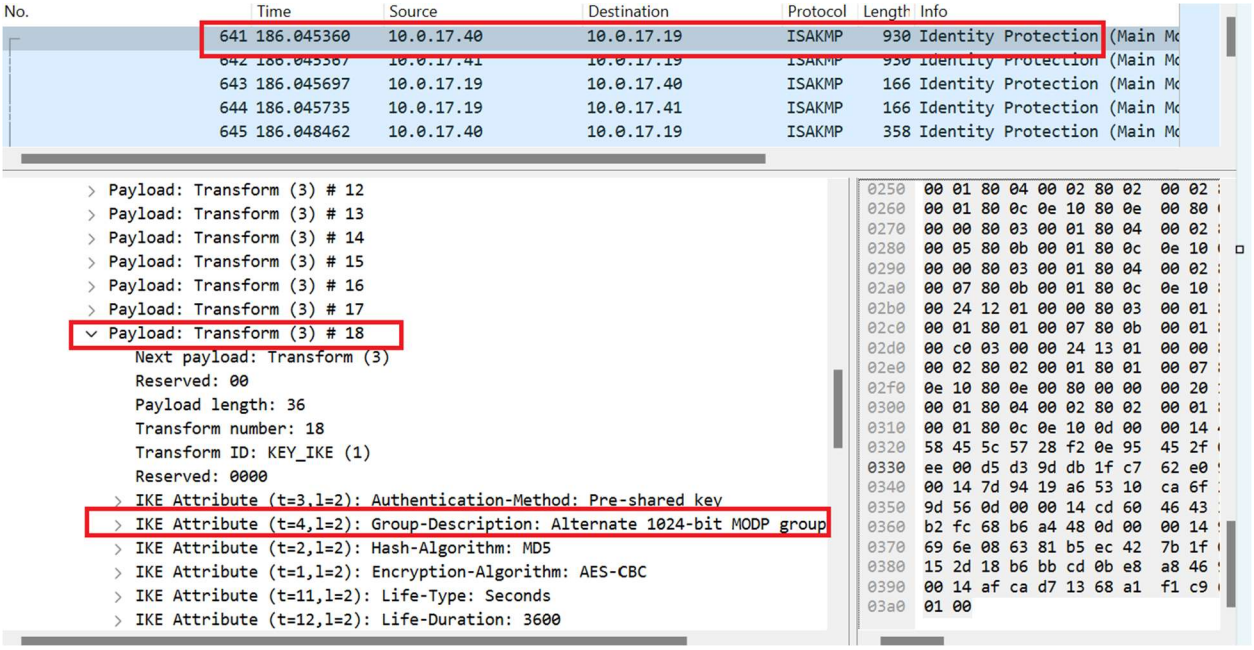
In certain cases SP SBC may act as IP sec tunnel responder for a tunnel in which case same steps up to now apply.

Guidance to tackle the problem

What should be clearly outlined here is that we should get every tunnel in 9.2 up and running with dh-group and IPsec SA ciphers supported in 9.3. Upgrade should be attempted only and only then if we aim for minimal service disruption. We will follow here how to get there in couple of iterations.

DH group selection

Idea in step 1 is to get the most flexible SBC configuration in place when it comes to IKE dh-group selection. As we have seen, this selection will be specified in global element ike-config and current SP settings are fixating dh-group2 for phase1 and phase2 exchange. With such settings, initiating a tunnel with ikev1 or ikev2 SBC would start the tunnel negotiation offering proposal that consist of dh-group2 transforms only.



Wireshark uncovers in this case in total 18 transforms, each assuming deprecated phase1 sh-group mod1024(dh-group2).

Way around being bound to dh-group2 are following changes to global ike-config:

```
SP_SBC# sho configuration ike-config
 ike-config
      state                    enabled
```

ike-version	1
log-level	INFO
udp-port	500
negotiation-timeout	15
event-timeout	60
phase1-mode	main
phase1-dh-mode	dh-group2 → change to “first-supported”
phase2-exchange-mode	dh-group2 → change to “same-as-phase1”
v2-ike-life-secs	86400
v2-ipsec-life-secs	28800
v2-rekey	enabled
anti-replay	enabled

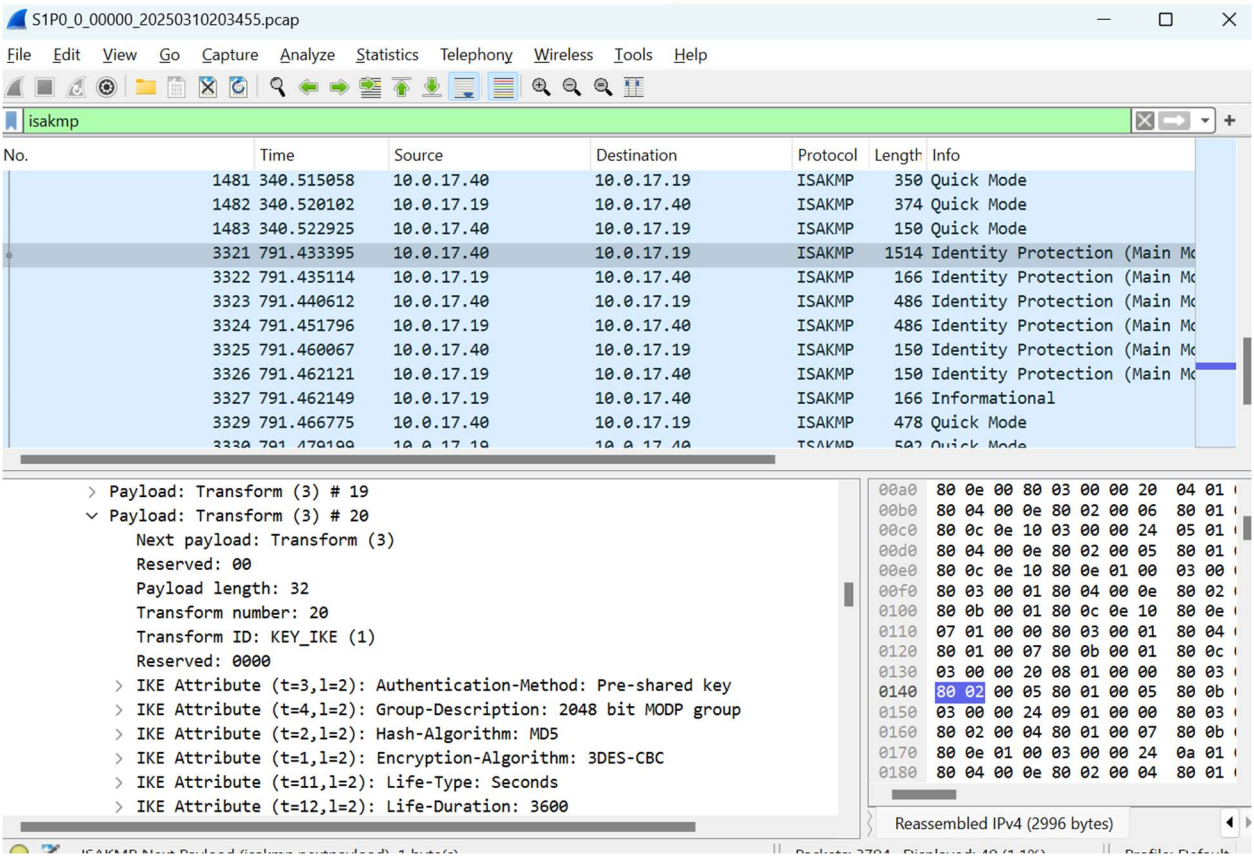
This change requires SBC reboot in maintenance window. For HA deployments however service will not be affected, exact steps to follow for HA:

1. Change ike-config as previously outlined.
2. Save/activate config.
3. Switchover: notify berpd force (We are not bringing down the tunnel).
4. Reboot standby.
5. Once it comes up, again switchover.
6. Reboot now old active (now standby). Tunnels will remain up.
7. Once this node is also up, tear down tunnel.
8. New tunnel now will be established with “first-supported”. Typically, it will be OPTIONS ping or any other traffic through the tunnel bringing it up.

When it comes to operation “tearing down” the tunnel following command is to be used:

security ipsec delete tunnel destIP [remote IPsec peer IP] spi [outbound SPI]

Capturing traffic after steps above we should see that SBC initiating a tunnel extends its proposal with transforms that include all dh-groups supported:



Already by the message size, it is obvious that new proposal is larger and this time it consists of 80 possible transforms involving all dh-groups supported.

Goal of this exercise was ONLY and ONLY to get flexibility in SBC to negotiate dh-groups supported in 9.3 release. Real outcome in reality will be the same tunnels built up again, just this time based on remote peer dh-group preference. As of this point customer may set up working sessions with remote peer-by-peer approach tuning the remaining tunnel parameters.

Customer1 working session

At the scheduled working appointment (maintenance window) with remote peer, SP should request dh-group preference change to the dh-group version that will be supported in 9.3(dh-group14 in example). Once remote peer confirms the change SP should tear down the tunnel and bring it back up (real traffic, OPTIONS ping, ICMP)

To identify the tunnel to be torn down following procedure is to be used:

sho security ipsec sad S1P0 detail

```
Inbound SPI: 11313131
        source-address              : 10.0.17.19
```

```
        destination-address       : 10.0.17.40
        vlan_id                   : 0
        ipsec-protocol            : ESP
        encr-algo                 : aes-256-ctr
        auth-algo                 : hmac-sha-512
        sa-installation-time      : 2025-03-11 13:09:53.138
        sa-duration               : 77042
        sa-installation-complete  : 0
        sa-installed-on-active    : 0
        tunnel-source             : 10.0.17.40
        tunnel-destination        : 10.0.17.19
        match fields:
                src-ip            : 10.0.17.19
                dst-ip            : 10.0.17.40
                src-port          : 0
                dst-port          : 0
                trans-proto       : any
        mask_fields:
                src-ip            : 255.255.255.255
                dst-ip            : 255.255.255.255
                src-port          : 0
                dst-port          : 0
                vlan-id           : 0xFFF
                protocol          : ALL
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
                soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
        hard limit -
                hard ms: 0x       0, hard ls : 0xFFFFFFFF
                soft ms: 0x       0, soft ls: 0xFFFFFFFF
                packets: 0x       8

Outbound SPI: 2655227280
Mirror SPI   : 11313131
        source-address            : 10.0.17.40
        destination-address       : 10.0.17.19
        source-port               : 0
        destination-port          : 0
        trans-proto               : any
        vlan_id                   : 0
        ipsec-protocol            : ESP
        encr-algo                 : aes-256-ctr
        auth-algo                 : hmac-sha-512
        sa-installation-time      : 2025-03-11 13:09:53.138
        sa-duration               : 77043
        sa-installation-complete  : 0
        sa-installed-on-active    : 0
        tunnel-source             : 10.0.17.40
        tunnel-destination        : 10.0.17.19
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
                soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
        time limit -
```

```
            hard ms: 0x       0, hard ls : 0xFFFFFFFF
            soft ms: 0x       0, soft ls: 0xFFFFFFFF
        sequence number -
            ms: 0x       0, ls: 0x       8
        packets -
            0x       8
```

Once outbound SPI is identified, we can tear down the tunnel. Remark that only issue to be fixed with customer1 is to get proper dh-group selection. Given the SBC is now offering full transform list and remote peer has confirmed upgrade to 9.3 supported group only thing that remains is tunnel down/up. This can be done from CLI with:

```
security ipsec delete tunnel destIP 10.0.17.19 spi 2655227280
```

Both tunnel ends in this setup are SIP OPTIONS monitored and tunnel quickly goes up gain this time with dh-group14(mod2048) used.

```
Outbound SPI: 2334756330
Mirror SPI   : 1288286270
        source-address              : 10.0.17.40
        destination-address         : 10.0.17.19
        source-port                 : 0
        destination-port            : 0
        trans-proto                 : any
        vlan_id                     : 0
        ipsec-protocol              : ESP
        encr-algo                   : aes-256-ctr
        auth-algo                   : hmac-sha-512
        sa-installation-time        : 2025-03-11 13:19:33.975
        sa-duration                 : 4285
        sa-installation-complete    : 0
        sa-installed-on-active      : 0
        tunnel-source               : 10.0.17.40
        tunnel-destination          : 10.0.17.19
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
                soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
        time limit -
                hard ms: 0x       0, hard ls : 0xFFFFFFFF
                soft ms: 0x       0, soft ls: 0xFFFFFFFF
        sequence number -
                ms: 0x       0, ls: 0x       1
        packets -
                0x       1

Inbound SPI: 1288286270
        source-address              : 10.0.17.19
        destination-address         : 10.0.17.40
        vlan_id                     : 0
```

```
        ipsec-protocol              : ESP
        encr-algo                   : aes-256-ctr
        auth-algo                   : hmac-sha-512
        sa-installation-time        : 2025-03-11 13:19:33.975
        sa-duration                 : 4285
        sa-installation-complete    : 0
        sa-installed-on-active      : 0
        tunnel-source               : 10.0.17.40
        tunnel-destination          : 10.0.17.19
        match fields:
                src-ip              : 10.0.17.19
                dst-ip              : 10.0.17.40
                src-port            : 0
                dst-port            : 0
                trans-proto         : any
        mask_fields:
                src-ip              : 255.255.255.255
                dst-ip              : 255.255.255.255
                src-port            : 0
                dst-port            : 0
                vlan-id             : 0xFFF
                protocol            : ALL
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
                soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
        hard limit -
                hard ms: 0x       0, hard ls : 0xFFFFFFFF
                soft ms: 0x       0, soft ls: 0xFFFFFFFF
                packets: 0x       1
```

Right after tunnel is up with SAs being re-build and counters freshly show just single packet (sip OPTIONS) out and single packet in(200OK for SIP OPTIONS). As of now customer1 tunnel is ready for migration to 9.3.

Customer2 working session

At customer2 appointment to tune the tunnel parameters further, we have more things to do. With customer2, we need to get 9.3-supported dh-group to be chosen but also we need to upgrade IPSec SA encryption and authentication algorithms, as currently used ones are not supported in 9.3. We will start by identifying the customer2 security associations:

```
Inbound SPI: 3821119041
        source-address              : 10.0.17.19
        destination-address         : 10.0.17.41
        vlan_id                     : 0
        ipsec-protocol              : ESP
        encr-algo                   : 3des
        auth-algo                   : hmac-sha1
        sa-installation-time        : 2025-03-11 13:09:53.175
        sa-duration                 : 585086
        sa-installation-complete    : 0
        sa-installed-on-active      : 0
        tunnel-source               : 10.0.17.41
        tunnel-destination          : 10.0.17.19
        match fields:
                src-ip              : 10.0.17.19
                dst-ip              : 10.0.17.41
                src-port            : 0
                dst-port            : 0
                trans-proto         : any
        mask_fields:
                src-ip              : 255.255.255.255
                dst-ip              : 255.255.255.255
                src-port            : 0
                dst-port            : 0
                vlan-id             : 0xFFF
                protocol            : ALL
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
                soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
        hard limit -
                hard ms: 0x       0, hard ls : 0xFFFFFFFF
                soft ms: 0x       0, soft ls: 0xFFFFFFFF
                packets: 0x      3B

Outbound SPI: 2464010320
Mirror SPI  : 3821119041
        source-address              : 10.0.17.41
        destination-address         : 10.0.17.19
        source-port                 : 0
        destination-port            : 0
        trans-proto                 : any
        vlan_id                     : 0
        ipsec-protocol              : ESP
        encr-algo                   : 3des
        auth-algo                   : hmac-sha1
        sa-installation-time        : 2025-03-11 13:09:53.175
        sa-duration                 : 585087
        sa-installation-complete    : 0
        sa-installed-on-active      : 0
        tunnel-source               : 10.0.17.41
        tunnel-destination          : 10.0.17.19
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
```

```
        soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
time limit -
        hard ms: 0x       0, hard ls : 0xFFFFFFFF
        soft ms: 0x       0, soft ls: 0xFFFFFFFF
sequence number -
        ms: 0x       0, ls: 0x      3B
packets -
        0x      3B
```

Relevant ike-sainfo in SP configuration is below:

ike-sainfo
- name customer2
- security-protocol esp-auth
- auth-algo sha1
- encryption-algo 3des
- ipsec-mode tunnel
- tunnel-local-addr 10.0.17.41
- tunnel-remote-addr 10.0.17.19
- last-modified-by admin@10.0.15.149
- last-modified-date 2025-03-11 08:44:25

Customer2 has to confirm that on its side it has moved to dh-group supported in 9.3(like dh-group14), also customer2 has to confirm that they adjusted encryption and authentication algorithms to those supported in SBC 9.3 software release. SP (IPsec concentrator) should swap to same ciphers on its side as well, looking in example as below:

ike-sainfo
- name customer2
- security-protocol esp-auth
- auth-algo sha2-384
- encryption-algo aes-ctr
- ipsec-mode tunnel
- tunnel-local-addr 10.0.17.41
- tunnel-remote-addr 10.0.17.19
- last-modified-by admin@10.0.15.149
- last-modified-date 2025-03-11 08:44:25

Changes above take effect on tunnel down/up that we will do from CLI:

```
security ipsec delete tunnel destIP 10.0.17.19 spi 2464010320
```

Once tunnel is promptly up it can be seen that this time encryption and authentication algorithms negotiated are within the list of those supported in 9.3 SBC software release.

```
Mirror SPI   : 4280153014
        source-address              : 10.0.17.41
        destination-address         : 10.0.17.19
        source-port                 : 0
        destination-port            : 0
        trans-proto                 : any
        vlan_id                     : 0
        ipsec-protocol              : ESP
        encr-algo                   : aes-256-ctr
        auth-algo                   : hmac-sha-384
        sa-installation-time        : 2025-03-11 13:48:11.455
        sa-duration                 : 16616
        sa-installation-complete    : 0
        sa-installed-on-active      : 0
        tunnel-source               : 10.0.17.41
        tunnel-destination          : 10.0.17.19
        byte count limit -
                hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
                soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
        time limit -
                hard ms: 0x       0, hard ls : 0xFFFFFFFF
                soft ms: 0x       0, soft ls: 0xFFFFFFFF
        sequence number -
                ms: 0x       0, ls: 0x       2
        packets -
                0x       2

Inbound SPI: 4280153014
        source-address              : 10.0.17.19
        destination-address         : 10.0.17.41
        vlan_id                     : 0
        ipsec-protocol              : ESP
        encr-algo                   : aes-256-ctr
        auth-algo                   : hmac-sha-384
        sa-installation-time        : 2025-03-11 13:48:11.455
        sa-duration                 : 16615
        sa-installation-complete    : 0
        sa-installed-on-active      : 0
        tunnel-source               : 10.0.17.41
        tunnel-destination          : 10.0.17.19
        match fields:
                src-ip              : 10.0.17.19
                dst-ip              : 10.0.17.41
                src-port            : 0
                dst-port            : 0
                trans-proto         : any
```

```
mask_fields:
        src-ip              : 255.255.255.255
        dst-ip              : 255.255.255.255
        src-port            : 0
        dst-port            : 0
        vlan-id             : 0xFFF
        protocol            : ALL
byte count limit -
        hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
        soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
hard limit -
        hard ms: 0x       0, hard ls : 0xFFFFFFFF
        soft ms: 0x       0, soft ls: 0xFFFFFFFF
        packets: 0x       2
```

At this point SBC is ready for customer2 tunnel regular 9.3 upgrade.

CustomerN working session

CustomerN reference in this BCP stands for a case where SP SBC Tunnel concentrator acts for certain tunnel as a responder. Same procedure to tune the tunnel apply for such customers as for those where IPSec concentrator acts as tunnel initiator. Once tunnel details are uncovered looking into SA details remote peer should be advised in a working session that acting as responder SBC in 9.3 will not negotiate DH group 2 and deprecated encryption and authentication algorithms and that acting as initiator they should include in their offer ciphers available in 9.3

Summary of configuration changes

1. In first phase, CSP should modify global ike-config to expose its support to all IKE dh-groups available in the given software release, check “DH group selection” chapter carefully. Change, to kick in, requires reboot.
2. In second phase, CSP should work with each remote peer to tune the tunnel settings with respect to new 9.3 requirements. This may require or may not require specific remote peer ike-sainfo configuration change. Change, to kick in, requires manual tunnel down/up operation.
3. Once tunnel parameters are modified with all remote peers SBC is ready for regular 9.3 upgrade.