CUPS での IPSec

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.25

機能説明

IPSec は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピアセキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

IPSec AH および ESP

認証ヘッダー（AH）とカプセル化セキュリティペイロード（ESP）は、IPSec で使用される 2 つの主要なワイヤレベルプロトコルです。IPSec 接続を介して流れるデータを認証（AH）し、暗号化して認証（ESP）します。

- AH は、IP トラフィックの認証に使用されるもので、暗号化には使用されません。認証は、IP パケットのほぼすべてのフィールド（TTL やヘッダーチェックサムなど、転送中に変更される可能性があるフィールドを除く）に対する暗号化ハッシュベースのメッセージ認証コードを計算することによって実行されます。計算されたメッセージ認証コードは、

新たに追加される AH ヘッダーに格納され、相手側に送信されます。AH ヘッダーは、元の IP ヘッダーとペイロードの間に挿入されます。

- ESP は暗号化と、オプションとして認証を提供します。ESP には、暗号化とオプションである認証をサポートするヘッダーフィールドとトレーラフィールドが含まれます。IP ペイロードの暗号化は転送モードでサポートされ、パケット全体の暗号化はトンネルモードでサポートされます。認証は、ESP ヘッダーと暗号化されたデータが対象となります。

IPsec トランスポートモードとトンネルモード

トランスポートモードでは IP ペイロードがカプセル化されるため、2 つのエンドポイント間にセキュアな接続が提供されますが、トンネルモードでは IP パケット全体がカプセル化されて、2 つのゲートウェイ間に仮想「セキュアホップ」が提供されます。

トンネルモードでは、IP パケット全体が別の内部にカプセル化されて、接続先に配信される、より一般的な VPN 機能が形成されます。完全な IP ヘッダーとペイロードがカプセル化されます。

（注） IPSec を介した UP:UP ICSR は、トンネルモードでのみ機能します。トランスポートモードはサポートされていません。

IPSec 用語

暗号アクセス制御リスト

アクセス制御リストでは、特定の条件を満たすサブスクライバ データ パケットを処理するためのルール（通常は権限）を定義します。ただし、暗号 ACL では、IPSec トンネルを介してルーティングされるサブスクライバ データ パケットに対応するために必要な条件を定義します。

インターフェイス、コンテキスト、または 1 つ以上のサブスクライバに適用される他の ACL とは異なり、暗号 ACL はクリプトマップと照合されます。また、暗号 ACL には 1 つのルールのみが含まれますが、他の ACL タイプは複数のルールで構成できます。

ルーティングの前に、システムは各サブスクライバデータ パケットのプロパティを調べます。パケットのプロパティが暗号 ACL で指定された条件と一致する場合に、システムはクリプトマップで指定された IPSec ポリシーを開始します。

トランスフォームセット

トランスフォームセットは、IPSec セキュリティ アソシエーション（SA）を定義するために使用されます。IPSec SA では、パケットを保護するために使用する IPSec プロトコルを指定します。

トランスフォームセットは、IPSec 確立のフェーズ 2 で使用されます。このフェーズでは、システムとピア セキュリティ ゲートウェイが、パケットを保護するためのルールを含む 1 つ以上のトランスフォームセット（IPSec SA）をネゴシエートします。このネゴシエーションにより、両方のピアがパケットを適切に保護および処理できるようになります。

ISAKMP ポリシー

Internet Security Association Key Management Protocol（ISAKMP）ポリシーを使用すると、インターネット キー エクスチェンジ（IKE）SA を定義できます。IKE SA は、システムとピア セキュリティ ゲートウェイ間の共有セキュリティパラメータ（使用する暗号化パラメータ、リモート ピアの認証方法など）を指定します。

IPSec 確立のフェーズ 1 では、システムとピア セキュリティ ゲートウェイが IKE SA をネゴシエートします。これらの SA は、IPSec SA ネゴシエーション プロセスを含むピア間の後続の通信を保護するために使用されます。

クリプト マップ

クリプトマップは、サブスクライバ データ パケットに IPSec を実装する方法を決定するトンネルポリシーを定義します。

CUPS では、いくつかのタイプのクリプトマップがサポートされています。その内容は次のとおりです。

- 手動クリプトマップ
- IKEv2 クリプトマップ
- ダイナミッククリプトマップ

暗号テンプレート

暗号テンプレートは、IKEv2 IPSec ポリシーを設定します。これには、暗号化および認証アルゴリズムのほとんどの IPSec パラメータと IKEv2 ダイナミックパラメータが含まれます。セキュリティ ゲートウェイ サービスは、暗号化テンプレートが設定されていなければ機能しません。

サービスごとに設定できる暗号テンプレートは 1 つのみです。ただし、1 つの StarOS インスタンスで、同じサービスの複数のインスタンスを実行することは可能で、これらのインスタンスそれぞれが該当する暗号テンプレートに関連付けられます。

ESP パケットの DSCP マーキング

SRP、SX、RCM、LI、TACACS などのアプリケーションは、異なるネットワークに展開されたノード間で動作します。これらすべてのアプリケーションでは、リモートシステムとの通信中に迅速なターンアラウンドが要求されます。Differentiated Services Code Point（DSCP）などの Quality of Service（QoS）を使用したカプセル化セキュリティペイロード（ESP）パケットのマーキングは、各タイプのパケットのトラフィック分類を決定するのに役立ちます。この機能

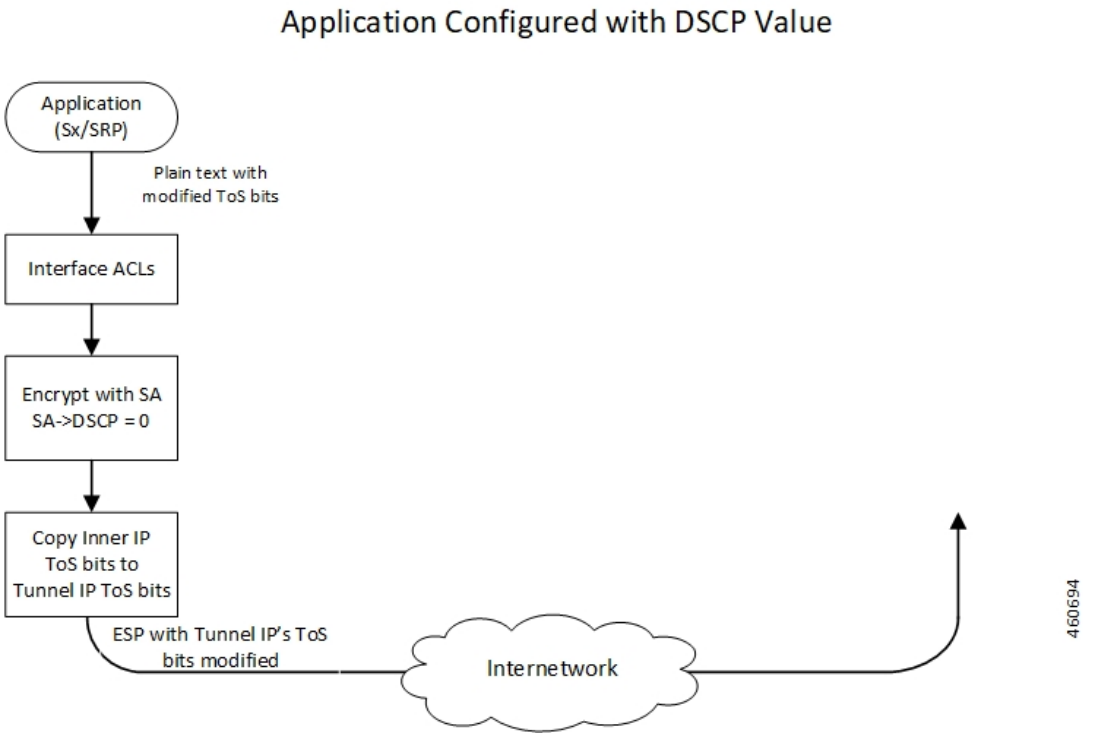
により、IP コアネットワーク内の IPsec パケットの優先順位付けが可能になり、IPsec を使用した Sx や SRP などのインターフェイスの拡張性が向上します。

ESP パケットに DSCP 値を適用する方法には、次の 2 つがあります。

- DSCP 値が設定されたアプリケーション経由
- DSCP 値が設定された暗号マップ経由

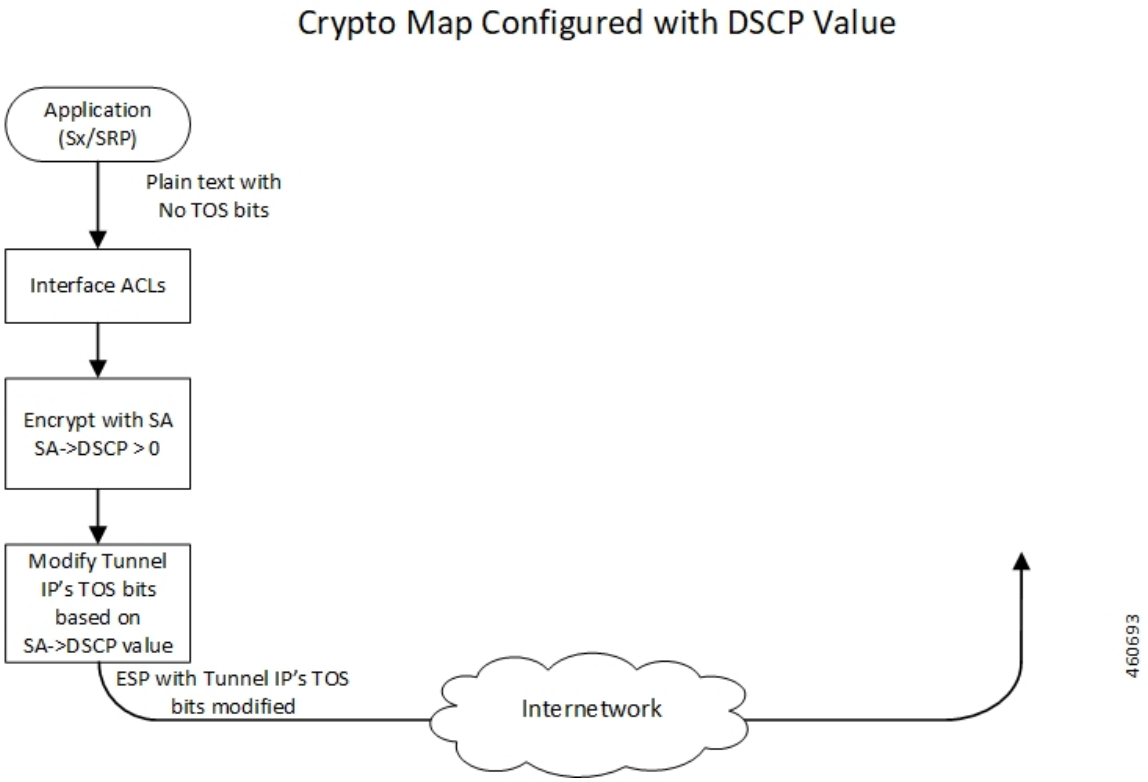
DSCP 値で設定されたアプリケーション

SRP、SX、LI などのアプリケーションが DSCP 設定をサポートしている場合、暗号化後の ESP パケットは、タイプオブサービス（ToS）ビットがアプリケーションの IP ヘッダーに設定されているかどうかを確認します。アプリケーションの IP ヘッダーの ToS ビットがゼロ以外の場合、内部 ToS ビットをトンネルの IP ヘッダーの ToS ビットにコピーしてから、パケットを出力します。次の図は、この処理の流れを示しています。



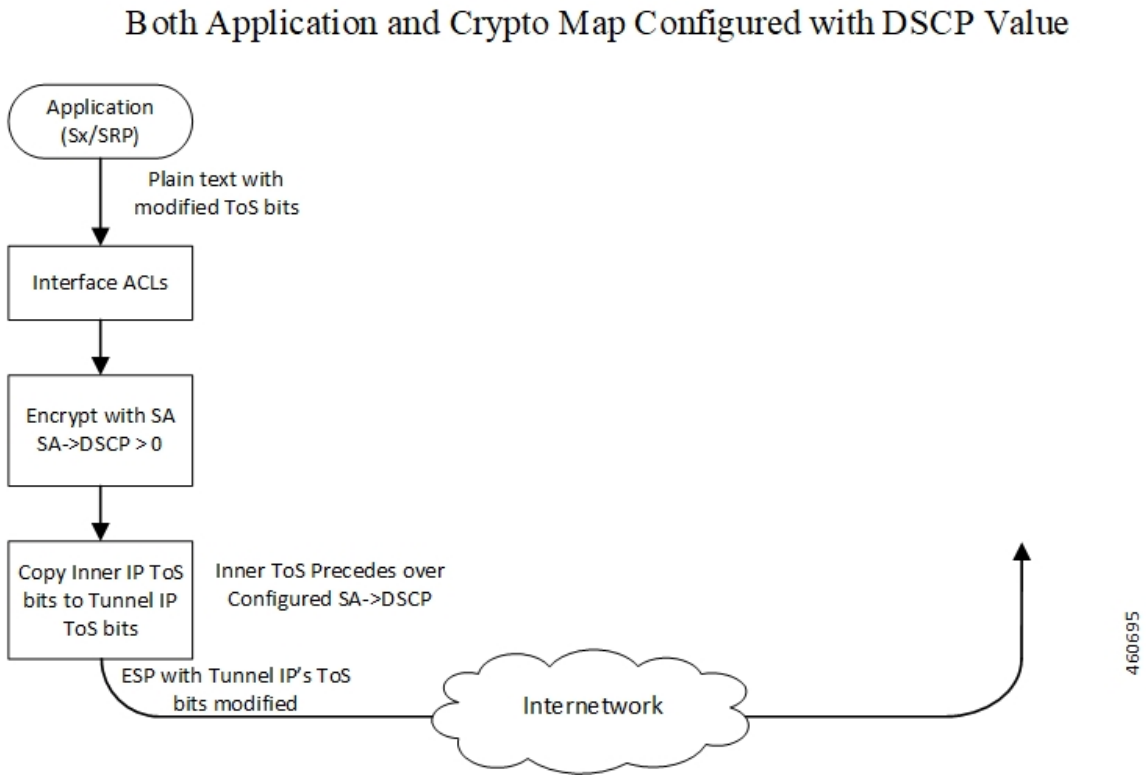
DSCP 値で設定されたクリプトマップ

暗号化が必要なすべてのアプリケーションには、ユーザーが設定できるクリプトマップが関連付けられています。特定のインターフェイスでクリプトマップを有効にすると、このクリプトマップのセキュリティ アソシエーション（SA）データベースで DSCP 値が更新されます。DSCP 値を保持するための新しいフィールドが SA データベース構造に定義されています。パケットが暗号化されると、SA データベースに有効な DSCP 値があるかどうかがチェックされます。有効な DSCP 値が見つかった場合、この DSCP 値はトンネル IP ヘッダーの ToS ビットにコピーされ、パケットは出力されます。次の図は、この処理の流れを示しています。



DSCP 値で設定されたアプリケーションとクリプトマップ

DSCP 値がクリプトマップとアプリケーション IP ヘッダーの両方で設定されている場合、アプリケーション ToS ビットが優先され、この値はトンネル IP ヘッダーの ToS ビットにコピーされます。次の図は、この処理の流れを示しています。



サポートされるアルゴリズム

CUPS の IPSec は、RFC 5996 で指定されている次の表のプロトコルをサポートします。

プロトコル	タイプ	サポートされるオプション（VPP なし）	サポートされるオプション（VPP あり）
インターネットキー	IKEv2 暗号化	DES-CBC、3DES-CBC、AES-CBC-128、AES-CBC-256	

プロトコル	タイプ	サポートされるオプション（VPP なし）	サポートされるオプション（VPP あり）
Exchange バージョン 2	IKEv2 疑似ランダム関数	PRF-HMAC-SHA1、PRF-HMAC-MD5、AES-XCBC-PRF-128	PRF-HMAC-SHA1、PRF-HMAC-MD5、AES-XCBC-PRF-128
	IKEv2 整合性	HMAC-SHA1-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192 HMAC-SHA2-512-256、HMAC-MD5-96、AES-XCBC-96	HMAC-SHA1-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192 HMAC-SHA2-512-256、HMAC-MD5-96、AES-XCBC-96
	IKEv2 Diffie-Hellman グループ	グループ 1（768 ビット）、グループ 2（1,024 ビット）、グループ 5（1,536 ビット）、グループ 14（2,048 ビット）	グループ 1（768 ビット）、グループ 2（1,024 ビット）、グループ 5（1,536 ビット）、グループ 14（2,048 ビット）
IP Security	IPSec カプセル化セキュリティペイロード暗号化	NULL、DES-CBC、3DES-CBC、AES-CBC-128、AES-CBC-256、AES-128-GCM-128、AES-128-GCM-64、AES-128-GCM-96、AES-256-GCM-128、AES-256-GCM-64、AES-256-GCM-96	NULL、DES-CBC、3DES-CBC、AES-CBC-192、AES-CBC-128、AES-CBC-256、AES-128-GCM-128、AES-128-GCM-64、AES-128-GCM- 96、AES-192-GCM、AES-256-GCM-128、AES-256-GCM-64、AES-256-GCM-96
	拡張シーケンス番号	0 またはオフの値がサポートされます（ESN 自体はサポートされません）。	0 またはオフの値がサポートされます（ESN 自体はサポートされません）。
	IPSec 整合性	NULL、HMAC-SHA1-96、HMAC-MD5-96、AES-XCBC-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192、HMAC-SHA2-512-256 **重要** HMAC-SHA2-384-192 および HMAC-SHA2-512-256 は、ハードウェアに暗号化ハードウェアがない場合、VPC-DI および VPC-SI プラットフォームではサポートされません。	NULL、HMAC-SHA1-96、HMAC-MD5-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192、HMAC-SHA2-512-256 **重要** HMAC-SHA2-384-192 および HMAC-SHA2-512-256 は、ハードウェアに暗号化ハードウェアがない場合、VPC-DI および VPC-SI プラットフォームではサポートされません。

（注） IPSec の詳細については、StarOS IPSec リファレンス [英語] を参照してください。すべての機能が CUPS に適用されるわけではないことに注意してください。

IPSec for Sx、LI、SRP などの詳細については、CUPS CP ガイド [英語]、CUPS UP ガイド [英語]、Sx インターフェイスガイド [英語]、および CUPS LI ガイド [英語] の関連する章を参照してください。

制限事項と制約事項

この機能には次の既知の制限事項と制約事項があります。

- この機能は、アプリケーション ToS の変更をサポートしていません。
- 暗号マップ CLI コマンドの DSCP 値の設定は、アプリケーションが UP の **Day-1** 設定として設定されているコンテキストと同じコンテキストに追加する必要があります。
- トンネルの作成後に DSCP 設定を適用する場合は、関連付けられた暗号マップをインターフェイスに再適用する必要があります。
- SA でパケットの順序変更が発生すると、アンチリプレイメカニズムが原因で、レシーバでパケットが廃棄される可能性があります。

暗号マップでの DSCP の設定

特定のトランスフォームセットの DSCP 値を適用するには、次の CLI コマンドを使用します。

```
configure
   context context_name
     ipsec transform-set set_name
       dscp dscp_value
       exit
     exit
   end
```

設定例

以下に設定例を示します。

```
context ipsec-d
    ip access-list foo0
      permit tcp 209.165.200.225 209.165.200.250 209.165.200.245 209.165.200.250

    #exit

    ip access-list foo1
      permit tcp 209.165.200.225 209.165.200.250 209.165.200.247 209.165.200.250
```

```
    #exit
    ipsec transform-set A-foo
    dscp 0x28
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key encrypted key encrypted_key
      authentication remote pre-shared-key encrypted key encrypted_key
      ikev2-ikesa max-retransmission 3

      ikev2-ikesa retransmission-timeout 15000

      ikev2-ikesa setup-timer 60

      ikev2-ikesa transform-set list ikesa-foo

      ikev2-ikesa rekey

      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
        lifetime 9000
        rekey keepalive
      #exit
      peer 209.165.201.1

      ikev2-ikesa policy error-notification

    #exit
    crypto map foo1 ikev2-ipv4

      match address foo1

      authentication local pre-shared-key encrypted key encrypted_key
      authentication remote pre-shared-key encrypted key encrypted_key
      ikev2-ikesa max-retransmission 3

      ikev2-ikesa retransmission-timeout 15000

      ikev2-ikesa transform-set list ikesa-foo

      ikev2-ikesa rekey

      payload foo-sa0 match ipv4

        ipsec transform-set list A-foo

        lifetime 9000

        rekey keepalive

      #exit

      peer 209.165.201.2

      ikev2-ikesa policy error-notification

    #exit
```

QoS の設定

DSCP でマーキングされた ESP パケットは、基盤となる L2 マーキング インフラストラクチャに従います。

DSCP に基づく QoS 設定により、シャーシからの出力前に ESP パケットの L2 マーキングがトリガーされます。

以下に設定例を示します。

```
Config
  qos ip-dscp-iphb-mapping dscp 0x28 internal-priority cos 0x1
  qos l2-mapping-table name l2Marktable
    internal-priority cos 0x1 color 0x0 802.1p-value 0x4 mpls-tc 0x6
   exit
end
```

注：

- **qos ip-dscp-iphb-mapping**：QoS プロファイルを作成します。
- **dscp***dscp_value*：IP DSCP 値を内部 QoS にマッピングします。
- **internal-priority cos** *class_of_service_value* **color** *color_value* **802.1p-value** *mpls_tc_value*：内部 QoS の優先順位を COS 値にマッピングします。

IPSec コンテキストで L2 マッピングテーブルを関連付けるための設定例を以下に示します。

```
config
   context ipsec-s
      associate l2-mapping-table name l2Marktable
end
```

注：

- **associate l2-mapping-table**：QoS を内部 QoS から l2 値にマッピングします。
- **name** *table_name*：QoS を内部 QoS から l2 値にマッピングするテーブルの名前を指定します。*table_name* は、1 ～ 80 文字の英数字にする必要があります。

モニタリングおよびトラブルシューティング

ここでは、ESP パケット機能の DSCP マーキングのモニタリングや障害対応に使用できる CLI コマンドについて説明します。

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show crypto map tag *tag_name*：このコマンドを使用して、設定された DSCP 値を表示します。

```
Map Name: foo0
========================================

  IPSec Manager: 54
  Map status: Complete
  Payload:
 ACLs:
   foo0
 Rules:
   permit tcp 209.165.200.225 209.165.200.250 209.165.200.245 209.165.200.250 eq 6002
  Crypto Map Type: IPSEC IKEv2 over IPv4
  IKE SA Transform 1/1
    Transform Set:
      Encryption Cipher: aes-cbc-128
      Encryption Accel: None
      Pseudo Random Function: sha1
      Hashed Message Authentication Code: sha1-96
      HMAC Accel: None
      Diffie-Hellman Group: 2
  IKE SA DSCP Value:  0x28

  IKE SA IDi [Peer]: Disabled

  IKE SA DH Exponentials reuse groups : None

  IKEv2 IKESA DDOS Mitigation Params:
    Half Open Timer: Disabled
    Decrypt Fail Count: Disabled
    Max IKEv2 requests Allowed : Disabled
    Message Queue Size: Disabled
    Rekey Rate: Disabled
    Max Certificate Size: Disabled

  IKEv2 Notify Payload:
    Device Identity: Enabled[Default]
  Notify Payload Error Message Type:
    UE: 0
    Network Transient Minor: 0
    Network Transient Major: 0
    Network Permanent: 0

  Blacklist/Whitelist : None

  OCSP Status         : Disabled
  OCSP Nonce Status  : Enabled
  OCSP Responder Address :None
  OCSP HTTP version : 1.0


  Remote-secret-list: <not-configured>

  Authentication Local:
   Phase 1 - Pre-Shared Key (Size = 7)

  Authentication Remote:
   Phase 1 - Pre-Shared Key (Size = 7)


  Self-Certificate Validation: Disabled
  Certificate Server Timeout: 20 Sec
  Minimum Certificate Key Size Validation: Disabled
```

```
Max Dhost Connections: 40

IPSec SA Payload 1/1
  Name : foo-sa0
  Payload Maximum Child SA: 1 [Default]
  Payload Ignore Ikesa Rekey: Disabled
  Payload Lifetime Params:
    Seconds: 90
    Sequence Number: 4293918720 [Default]
  Payload TSI Start Address: Address Endpoint
  Payload TSI End Address: Address Endpoint

  IPSec SA Transform 1/1
    Transform Set:
      Protocol: esp
      Encryption Cipher: aes-cbc-128
      Encryption Accel: None
      Hashed Message Authentication Code: sha1-96
      HMAC Accel: None
      Diffie-Hellman Group: none
      ESN: Disabled
      Dscp: 0x28
Dont Fragment: Copy bit from inner header
IPv4 Payload fragment type: outer
MTU: 1438 [Default]

NATT: Disabled


IKEv2 Fragmentation: Enabled
IKEv2 MTU Size IPv4/IPv6: 1384/1364

CERT Enc Type URL Allowed: Disabled
Custom FQDN Allowed: Disabled
DNS Handling: Normal [Default]

interface using this crypto-map: saegw-li1-loopback-ipv4

Local Gateway: 209.165.202.129
Remote Gateway: 209.165.201.1
```

show qos ip-dscp-iphb-mapping：このコマンドを使用して、パケット内の QoS 情報から internal-qos マーキングへのマッピングを表示します。

```
--------------+-----------------
    DSCP      |     Internal Qos
--------------+-----------------
   0x00       |          0
   0x01       |          0
   0x02       |          0
   0x03       |          0
   0x04       |          0
   0x05       |          0
   0x06       |          0
   0x07       |          0
--------------+-----------------
   0x08       |          0
   0x09       |          0
   0x0a       |          0
   0x0b       |          0
   0x0c       |          0
   0x0d       |          0
```

```
   0x0e       |          0
   0x0f       |          0
--------------+-----------------
   0x10       |          0
   0x11       |          0
   0x12       |          0
   0x13       |          0
   0x14       |          0
   0x15       |          0
   0x16       |          0
   0x17       |          0
--------------+-----------------
   0x18       |          0
   0x19       |          0
   0x1a       |          0
   0x1b       |          0
   0x1c       |          0
   0x1d       |          0
   0x1e       |          0
   0x1f       |          0
--------------+-----------------
   0x20       |          0
   0x21       |          0
   0x22       |          0
   0x23       |          0
   0x24       |          0
   0x25       |          0
   0x26       |          0
   0x27       |          0
--------------+-----------------
  0x28        |          1
   0x29       |          0
   0x2a       |          0
   0x2b       |          0
   0x2c       |          0
   0x2d       |          0
   0x2e       |          0
   0x2f       |          0
--------------+-----------------
   0x30       |          0
   0x31       |          0
   0x32       |          0
   0x33       |          0
   0x34       |          0
   0x35       |          0
   0x36       |          0
   0x37       |          0
--------------+-----------------
   0x38       |          0
   0x39       |          0
   0x3a       |          0
   0x3b       |          0
   0x3c       |          0
   0x3d       |          0
   0x3e       |          0
   0x3f       |          0
--------------+-----------------
```

show qos l2-mapping-table name *table_name* ：このコマンドを使用して、L2 マッピング値への内部の名前付きテーブルを表示します。

```
Table: l2Marktable
------------------------+-------+-------
    Internal Priority    |802.1p | MPLS
```

Class-of-service	Color		
0	0	0x0	0
0	1	0x0	0
0	2	0x0	0
0	3	0x0	0
1	**0**	**0x4**	**6**
1	1	0x2	1
1	2	0x2	1
1	3	0x2	1
2	0	0x4	2
2	1	0x4	2
2	2	0x4	2
2	3	0x4	2
3	0	0x6	3
3	1	0x6	3
3	2	0x6	3
3	3	0x6	3
4	0	0x8	4
4	1	0x8	4
4	2	0x8	4
4	3	0x8	4
5	0	0xa	5
5	1	0xa	5
5	2	0xa	5
5	3	0xa	5
6	0	0xc	6
6	1	0xc	6
6	2	0xc	6
6	3	0xc	6
7	0	0xe	7
7	1	0xe	7
7	2	0xe	7
7	3	0xe	7

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。