IPsec と Quality of Service

IPsec と Quality of Service 機能を使用すれば、Cisco IOS Quality of Service（QoS）ポリシーを、QoS グループに基づいて、IP Security（IPsec）パケット フローに適用できます。QoS グループは、現在の Internet Security Association and Key Management Protocol（ISAKMP）プロファイルに適用できます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の検索

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザー名やパスワードを忘れた場合は、ログインダイアログボックスで **[Cancel]** をクリックし、表示される説明に従ってください。

IPsec と Quality of Service の前提条件

- IPsec、および ISAKMP プロファイルの概念についての知識が必要です。
- Cisco IOS QoS の知識が必要です。

IPsec と Quality of Service の制約事項

- この機能を適用できるのはISAKMPプロファイルを介してだけです。QoSアプリケーションに対して使用できる QoS グループは 128 個までという制限はこの機能にも当てはまります。
- IPsec QoS グループを適用できるのは、発信サービス ポリシーに対してだけです。
- QoS は、ソフトウェア暗号化に関してはサポートされません。

IPsec と Quality of Service に関する情報

IPsec と Quality of Service の概要

IPsec と Quality of Service 機能を使用すれば、QoS グループを ISAKMP プロファイルに追加することによって、トラフィック ポリシングおよびシェーピングなどの QoS ポリシーを QoS ポリシーに適用できます。QoSグループが追加されると、このグループの値が、QoSクラスマップ内で定義されたものと同じ QoS グループにマッピングされます。この QoS グループ タグを利用している現在の QoS 方式はすべて、IPsec パケット フローに適用できます。パケット フローの共通グルーピングには、IPsec QoS グループを QoS メカニズムにとって使用可能にすることによって、特定のポリシー クラスを適用できます。IPsecフローをマーキングすれば、QoSメカニズムを、特定のグループが使用可能な帯域幅の制限や特定のフロー上のタイプオブサービス（ToS）ビットのマーキングなどをサポート可能なトラフィックのクラスに適用できます。

ISAKMPプロファイルは、アイデンティティ照合基準方式によってデバイスを一意に識別できるプロファイルなので、QoS グループのアプリケーションは、ISAKMP プロファイル レベルで適用されます。これらの基準は、インターネットキー交換（IKE）IDに基づいています。この ID は、受信 IKE 接続によって提供され、IP アドレス、完全修飾ドメイン名（FQDN）、およびグループ（つまり、バーチャル プライベート ネットワーク [VPN] リモート クライアント グルーピング）などが格納されます。アイデンティティ照合基準の粒度によって、指定された QoS ポリシーの粒度に制約が課せられます。たとえば、「Engineering」という名前の VPN クライアント グループに所属するすべてのトラフィックを、「TOS 5」としてマーキングします。指定した QoS ポリシーの粒度に制約を課すその他の例としては、発信 WAN リンクの 30 パーセントをリモート VPN デバイスの特定のグループへ割り当てるなどがあります。

IPsec と Quality of Service の設定方法

IPsec と Quality of Service の設定

QoS ポリシーを ISAKMP プロファイルに適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp-profile** *profile-number*
4. **qos-group** *group-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp-profile** *profile-number* 例： `Router (config)# crypto isakmp-profile vpnprofile`	ISAKMP プロファイルを定義し、IPsec ユーザ セッションを監査し、ISAKMP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**qos-group** *group-number* 例： `Router(config-isa-prof)# qos-group 1`	QoS グループ値を ISAKMP プロファイルに適用します。

IPsec と Quality of Service セッションの確認

IPsec and QoS セッションを確認するには、次の手順を実行します。**show** コマンドは、任意の順序か互いに独立させて使用できます。

手順の概要

1. **enable**
2. **show crypto isakmp profile**
3. **show crypto ipsec sa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**show crypto isakmp profile** 例： `Router# show crypto isakmp profile`	QoS グループがプロファイルに適用されていることを表示します。
ステップ 3	**show crypto ipsec sa** 例： `Router# show crypto ipsec sa`	QoS グループが、IPsec セキュリティ アソシエーション（SA）の特定のペアに適用されていることを表示します。

トラブルシューティングのヒント

IPsec セッションおよび QoS セッションに問題が発生した場合、次が実行されているかどうかを確認します。

- 『*Cisco IOS Quality of Service Solutions Command Reference*』に記載されている QoS 専用コマンドを使用して、QoS の適用を QoS サービスごとに確認している。
- クラス マップ一致基準に指定されたものと同じ QoS グループと一致しているルータ上の QoS ポリシーを設定している。
- クリプト マップが適用されるものと同じインターフェイスにサービス ポリシーを適用している。

IPsec と Quality of Service の設定例

リモート ユーザの 2 つのグループに適用された QoS ポリシーの例

次に、特定の QoS ポリシーがリモート ユーザの 2 つのグループに適用されている例を示します。2 つのプロファイルが、IKE を介した最初の接続上でリモート ユーザが特定のプロファイルにマッピングされるように設定されています。そのプロファイルから、そのリモートに対して作成されたすべての IPsec SA が特定の QoS グループでマーキングされます。トラフィックが発信インターフェイスを出ると、QoS サービスによって、その発信インターフェイス上で適用されているサービス ポリシーを構成するクラス マップ内で指定された QoS グループで IPsec 設定 QoS グループがマッピングされます。

```
version 12.3
!
aaa authentication login group group radius
aaa authorization network autho local
aaa accounting update periodic 1
```

```
aaa session-id common
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
class-map match-all yellow
 match qos-group 3
class-map match-all blue
match qos-group 2
!
!
policy-map clients
 class blue
  set precedence 5
 class yellow
  set precedence 7
!
!
crypto isakmp policy 1
 encr aes
 hash sha
 authentication pre-share
 group 14
 lifetime 300
!
crypto isakmp keepalive 10 periodic
crypto isakmp xauth timeout 20
!
crypto isakmp client configuration group blue
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 pool blue
 save-password
 include-local-lan
 backup-gateway corky1.cisco.com
!
crypto isakmp client configuration group yellow
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.5
 pool yellow
!
crypto isakmp profile blue
   match identity group cisco
   client authentication list autho
   isakmp authorization list autho
   client configuration address respond
   qos-group 2
crypto isakmp profile yellow
   match identity group yellow
   match identity address 10.0.0.11 255.255.255.255
   client authentication list autho
   isakmp authorization list autho
   client configuration address respond
   qos-group 3
!
!
crypto ipsec transform-set combo ah-sha-hmac esp-aes esp-sha-hmac
crypto ipsec transform-set client esp-aes esp-sha-hmac comp-lzs
!
crypto dynamic-map mode 1
 set security-association lifetime seconds 180
```

```
 set transform-set client
 set isakmp-profile blue
 reverse-route
crypto dynamic-map mode 2
 set transform-set combo
 set isakmp-profile yellow
 reverse-route
!
crypto map mode 1 ipsec-isakmp dynamic mode
!
interface FastEthernet0/0
 ip address 10.0.0.110 255.255.255.0
 no ip redirects
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
 crypto map mode
 service-policy out clients
!
ip local pool yellow 192.168.2.1 192.168.2.10
ip local pool blue 192.168.6.1 192.168.6.6
no ip classless
!
radius-server host 10.0.0.13 auth-port 1645 acct-port 1646
radius-server key XXXXXX
radius-server vsa send accounting
radius-server vsa send authentication
```

show crypto isakmp profile コマンドの例

次の出力では、QoS グループ「2」が ISAKMP プロファイル「blue」に適用され、QoS グループ「3」が ISAKMP プロファイル「yellow」に適用されていることを示しています。

```
Router# show crypto isakmp profile
ISAKMP PROFILE blue
   Identities matched are:
    group blue
   QoS Group 2 is applied
ISAKMP PROFILE yellow
   Identities matched are:
    ip-address 10.0.0.13 255.255.255.255
    group yellow
   QoS Group 3 is applied
```

show crypto ipsec sa コマンドの例

次の出力では、QoS グループが IPsec SA の特定のペアに適用されていることを示しています。

```
Router# show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: mode, local addr. 10.0.0.110
   protected vrf:
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.12.12.0/255.255.255.0/0/0)
   current_peer: 10.0.0.11:500
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
 qos group is set to 2
```

その他の参考資料

ここでは、IPsec と Quality of Service 機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IPSec	IPsec を使用した VPN のセキュリティの設定
QoS オプション	『*Cisco IOS Quality of Service Solutions Configuration Guide*』（Cisco.com）
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更されたRFCはありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec と Quality of Service の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IPsec* と *Quality of Service* の機能情報

機能名	リリース	機能情報
IPsec と Quality of Service	Cisco IOS XE Release 3.9S	IPsec と Quality of Service 機能を使用すれば、Cisco IOS Quality of Service（QoS）ポリシーを、QoS グループに基づいて、IP Security（IPsec）パケット フローに適用できます。QoS グループは、現在の Internet Security Association and Key Management Protocol（ISAKMP）プロファイルに適用できます。 次のコマンドが導入または変更されました。 **qos-group.**

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。