IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化

Cisco IP security（IPsec; IP セキュリティ）認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチ リプレイ保護が提供されます。それらの番号に基づいて、デクリプタが検知したパケットを追跡します。現在、デフォルトのウィンドウ サイズは、64 パケットです。一般的にはこの数字（ウィンドウ サイズ）で十分ですが、このウィンドウ サイズを拡張する必要がある場合もあります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能履歴

リリース	変更点
12.3(14)T	この機能が追加されました。
12.2(33)SRA	この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(18)SXF6	この機能は、Cisco IOS Release 12.2(18)SXF6 に統合されました。

プラットフォーム、Cisco IOS ソフトウェア イメージ、および Catalyst OS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS 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。Cisco.com のアカウントは必要ありません。

この章の構成

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化の前提条件

- この機能を設定する前に、クリプト マップまたは暗号プロファイルを作成しておく必要があります。

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化に関する情報

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を設定するには、次の概念を理解しておく必要があります。

- 「IPsec アンチ リプレイ ウィンドウ」（P.2）

IPsec アンチ リプレイ ウィンドウ

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチ リプレイ保護が提供されます（セキュリティ アソシエーション（SA）アンチ リプレイは、受信側が、リプレイ アタックから自身を保護するために、古いまたは重複したパケットを拒否できるセキュリティ サービスです）。すでに検知したシーケンス番号はデクリプタによって対象から外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X まで（N はウィンドウ サイズ）のシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットは廃棄されます。現在、N は 64 に設定されているので、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケットのウィンドウ サイズで不十分である場合もあります。たとえば、Cisco Quality of Service（QoS）によって、ハイプライオリティ パケットにプライオリティが与えられている場合、一部のロープライオリティ パケットが、それらがデクリプタによって受信された最新の 64 パケットの 1 つにもかかわらず、廃棄されてしまう可能性があります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

アンチ リプレイ ウィンドウ サイズを増加させても、スループットおよびセキュリティに影響はありません。メモリに対する影響は大きなものになります。デクリプタ上にシーケンス番号を保管するうえで必要なのは、着信 IPsec SA 毎に 128 バイトだけ余分であればよいからです。1024 ウィンドウ サイズをフルに使用して、アンチ リプレイ問題が発生する可能性を根絶することを推奨します。

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能の設定方法

ここでは、次の各手順について説明します。

- 「IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化のグローバル設定」（P.3）（任意）
- 「クリプト マップ上における IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化の設定」（P.3）（任意）

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化のグローバル設定

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化をグローバルに設定する（その結果、個々のクリプト マップに基づいて個別に上書きされるものを除き、作成されるすべての SA が影響を受けます）には、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association replay window-size** [*N*]
4. **crypto ipsec security-association replay disable**

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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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 ipsec security-association replay window-size** [*N*] **例：** `Router (config)# crypto ipsec security-association replay window-size 256`	SA リプレイ ウィンドウのサイズをグローバルに設定します。 **（注）** このコマンドまたは **crypto ipsec security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 4	**crypto ipsec security-association replay disable** **例：** `Router (config)# crypto ipsec security-association replay disable`	検査をグローバルにイネーブルにします。 **（注）** このコマンドまたは **crypto ipsec security-association replay window-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

クリプト マップ上における IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化の設定

クリプト マップ上で IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化を、特定のクリプト マップまたはプロファイルを使用して作成された SA に影響を与えるように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
4. **set security-association replay window-size** [*N*]
5. **set security-association replay disable**

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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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 map** *map-name seq-num* [**ipsec-isakmp**] **例：** `Router (config)# crypto map ETHO 17 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始し、動的に作成されるクリプト マップの設定のためのテンプレートを提供する暗号プロファイルを作成します。
ステップ 4	**set security-association replay window-size** [*N*] **例：** `Router (crypto-map)# set security-association replay window-size 128`	特定のクリプト マップ、ダイナミック クリプト マップ、または暗号プロファイルによって指定されたポリシーを使用して作成される SA を制御します。 **（注）** このコマンドまたは **set security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 5	**set security-association replay disable** **例：** `Router (crypto-map)# set security-association replay disable`	特定のクリプト マップ、ダイナミック クリプト マップ、または暗号プロファイルに対するリプレイ検査をディセーブルにします。 **（注）** このコマンドまたは **set security-association replay window-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

トラブルシューティングのヒント

- 受信されるパケットの数に対して十分高い数字がリプレイ ウィンドウ サイズに設定されていない場合、次のようなシステム メッセージが受信されます。

  ```
  *Nov 17 19:27:32.279: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
  connection id=1
  ```

  受信されたメッセージが、アンチ リプレイ ウィンドウの範囲を超えていると判断されると、上記メッセージが生成されます。

IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化の設定例

ここでは、次の設定例を示します。

アンチ リプレイ ウィンドウのグローバルな拡張とディセーブル化：例

次の例は、アンチ リプレイ ウィンドウ サイズがグローバルに 1024 に設定されていることを示しています。

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!

boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 192.165.201.2 !
crypto ipsec security-association replay window-size 1024 !
crypto ipsec transform-set basic esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp
 set peer 192.165.201.2
 set transform-set basic
 match address 101
!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 192.165.200.2 255.255.255.252  serial restart-delay 0  crypto map mymap !
ip classless
ip route 0.0.0.0 0.0.0.0 192.165.200.1
no ip http server
no ip http secure-server
!
!
```

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101
remark Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

特定のクリプト マップ、ダイナミック クリプト マップ、または暗号プロファイルのアンチ リプレイ ウィンドウの拡張およびディセーブル化の例

次の例では、アンチ リプレイ検査が、172.17.150.2 への IPsec 接続に関してディセーブルにされているが、172.17.150.3 および 172.17.150.4 への IPsec 接続に関してはイネーブル（および、デフォルトのウィンドウ サイズが 64）にされていることを示しています。

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname networkserver1
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1 enable password ww !
ip subnet-zero
!
cns event-service server

crypto isakmp policy 1
authentication pre-share

crypto isakmp key cisco170 address 172.17.150.2 crypto isakmp key cisco180 address
172.17.150.3 crypto isakmp key cisco190 address 172.17.150.4

crypto ipsec transform-set 170cisco esp-des esp-md5-hmac crypto ipsec transform-set
180cisco esp-des esp-md5-hmac crypto ipsec transform-set 190cisco esp-des esp-md5-hmac

crypto map ETH0 17 ipsec-isakmp
 set peer 172.17.150.2
 set security-association replay disable set transform-set 170cisco match address 170
crypto map ETH0 18 ipsec-isakmp  set peer 192.168.1.3 set transform-set 180cisco match
address 180 crypto map ETH0 19 ipsec-isakmp set peer 192.168.1.4 set transform-set
190cisco match address 190 !
interface Ethernet0
 ip address 172.17.150.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no mop enabled
 crypto map ETH0
!
interface Serial0
 ip address 172.16.160.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
```

```
!
ip classless
ip route 172.18.170.0 255.255.255.0 172.17.150.2 ip route 172.19.180.0 255.255.255.0
172.17.150.3 ip route 172.20.190.0 255.255.255.0 172.17.150.4 no ip http server !

access-list 170 permit ip 172.16.160.0 0.0.0.255 172.18.170.0 0.0.0.255 access-list 180
permit ip 172.16.160.0 0.0.0.255 172.19.180.0 0.0.0.255 access-list 190 permit ip
172.16.160.0 0.0.0.255 172.20.190.0 0.0.0.255 !
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
end
```

その他の参考資料

次の項では、IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化の関連資料を示します。

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Security Command Reference*』
IP セキュリティおよび暗号化	「*Configuring Security for VPNs with IPsec*」

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB 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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、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
この機能によってサポートされる新しい RFC や変更された RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **crypto ipsec security-association replay disable**
- **crypto ipsec security-association replay window-size**
- **set security-association replay disable**
- **set security-association replay window-size**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『Master Command List』を参照してください。