マスター キー タプル設定の実装

この機能は、TCP MD5 オプションを置き換える TCP 認証オプション（TCP-AO）を指定します。TCP-AO は、以下を提供するメッセージ認証コード（MAC）を使用します。

マスター キー タプル設定

この機能は、TCP MD5 オプションを置き換える TCP 認証オプション（TCP-AO）を指定します。TCP-AO は、以下を提供するメッセージ認証コード（MAC）を使用します。

- 長時間の TCP 接続のリプレイに対する保護
- TCP MD5 以外の TCP 接続でのセキュリティ アソシエーションの詳細
- 他のシステムや操作の変更を最小限に抑えた多数の MAC

TCP-AO は、マスター キー タプル（MKT）設定と互換性があります。TCP-AO は、接続の繰り返しインスタンスで同じ MKT を使用する場合も接続を保護します。TCP-AO は、MKT から導出されたトラフィック キーを使用して接続を保護し、エンドポイント間の変更を調整します。

（注） TCPAO と TCP MD5 を同時に使用することはできません。TCP-AO は IPv6 をサポートしており、TCP MD5 の交換に関して提案される要件と完全に互換性があります。

シスコでは、次の設定を介して MKT 設定を提供しています。

- キーチェーン設定
- tcp ao キーチェーン設定

システムは、キーチェーンの下にある 「key_id」 などの各キーを MKT として変換します。キーチェーン設定には、秘密、ライフタイム、アルゴリズムなどの設定の一部が含まれます。

「tcp ao キーチェーン」 モードには、MKT 用の TCP AO 固有の設定（send_id および receive_id）が含まれています。

キーチェーン設定

設定時の注意事項

設定を正常に実行するには、設定に関する注意事項に従ってください。

- Send_ID と Receive_ID の両方で許可されている値の範囲は 0 ～ 255 です。
- アプリケーション ネイバーには、1 つのキーチェーンのみをリンクできます。
- 同一のキーチェーンで、ライフタイムが重複しているキーの下に同じ send_id キーを再度設定すると、設定を修正するまで古いキーは使用できなくなります。
- 次のシナリオでは、システムから警告メッセージが送信されます。
  - Send_ID または Receive_ID が変更された場合。
  - 対応するキーが現在アクティブで、一部の接続で使用されている場合。
- BGP ネイバーは、次のいずれかの認証オプションのみを使用できます。
  - MD5
  - EA
  - AO

（注） これらのオプションのいずれかを設定すると、設定時にシステムによって他の認証オプションが拒否されます。

TCP AO BGP ネイバーの設定時の注意事項

設定時の注意事項は次のとおりです。

- key_id を使用する必要があるライフタイムを指定して、key_id ですべての必要な設定（key_string、MAC_algorithm、send_lifetime、accept_lifetime、send_id、receive_id）を行います。
- ピア側で、一致する MKT をまったく同じライフタイムで設定します。
- キーチェーンキーが tcp-ao にリンクされた後は、キーのコンポーネントを変更しないでください。TCP に別のキーの使用を検討させる場合は、そのキーを動的に設定できます。送信ライフタイムの「start-time」に基づいて、TCP AO はキーを使用します。

- （キーチェーンの下にある）key_id の Send_ID と Receive_ID は、ライフタイム範囲が同じである必要があります（たとえば、send-lifetime==accept-lifetime）。

  TCP は send-lifetime の期限切れのみを考慮して次のアクティブ キーに移行します。accept-lifetime はまったく考慮されません。

- 特定のキーの send-lifetime でカバーされる send-lifetime を別のキーに設定しないでください。

  たとえば、既存のキーの send-lifetime が「04:00:00 November 01, 2017 07:00:00 November 01, 2017」に設定されている場合、ユーザが別のキーの send-lifetime を「05:00:00 November 01, 2017 06:00:00 November 01, 2017」に設定すると、接続フラップが発生する可能性があります。

  新しいキーが期限切れになると、TCP AO は古いキーに戻そうとします。ただし、新しいキーがすでに期限切れになっている場合、TCP AO はこのキーを使用できないため、セグメント損失や接続フラップが発生する可能性があります。

- 重複する 2 つのキー間の重複時間は 15 分以上に設定します。TCP は期限が切れたキーを使用しないため、そのキーを使用した不適切なセグメントはドロップされます。

- 簡素化のために、key_id に設定する send_id と receive_id を同一にすることを推奨します。

- TCP には、キーチェーンに含まれるキーチェーンおよびキーの数に関する制限はありません。システムでは 4000 を超えるキーチェーンはサポートされません。4000 を超えると、予期しない動作が発生する可能性があります。

キーチェーン設定

```
key chain <keychain_name>
   key <key_id>
      accept-lifetime <start-time> <end-time>
      key-string <master-key>
      send-lifetime <start-time> <end-time>
      cryptographic-algorithm <algorithm>
   !
!
```

TCP 設定

TCP は、各キーチェーンの key_id ごとに SendID および ReceiveID を指定する新しい tcp ao サブモードを提供します。

```
tcp ao
    keychain <keychain_name1>
        key-id <key_id> send_id <0-255> receive_id <0-255>
        !
```

例：

```
tcp ao
 keychain bgp_ao
  key 0 SendID 0 ReceiveID 0
  key 1 SendID 1 ReceiveID 1
```

```
 key 2 SendID 3 ReceiveID 4
!
keychain ldp_ao
 key 1 SendID 100 ReceiveID 200
 key 120 SendID 1 ReceiveID 1
!
```

BGP 設定

BGP などのアプリケーションは、tcp-ao キーチェーンと、ネイバーごとに使用する関連情報を提供します。次に、tcp-ao キーチェーンごとのオプション設定を示します。

- include-tcp-options
- accept-non-ao-connections

```
router bgp <AS-number>
neighbor <neighbor-ip>
  remote-as <remote-as-number>
  ao <keychain-name> include-tcp-options enable/disable  <accept-ao-mismatch-connections>
!
```

XML 設定

BGP XML

TCP-AO XML

```
<?xml version="1.0" encoding="UTF-8"?>
<Request>
 <Set>
  <Configuration>
   <IP_TCP>
    <AO>
      <Enable>
       true
      </Enable>
      <KeychainTable>
        <Keychain>
         <Naming>
          <Name> bgp_ao_xml </Name>
         </Naming>
         <Enable>
          true
         </Enable>
          <KeyTable>
           <Key>
            <Naming>
             <KeyID> 0 </KeyID>
            </Naming>
             <SendID> 0 </SendID>
             <ReceiveID> 0 </ReceiveID>
           </Key>
          </KeyTable>
        </Keychain>
      </KeychainTable>
    </AO>
   </IP_TCP>
```

```
  </Configuration>
 </Set>
 <Commit/>
</Request>
```

確認

キーチェーン データベースを確認するには、EXEC モードで show tcp authentication keychain <keychain-name> コマンドを使用します。次の出力には、キーチェーン データベースの詳細がすべて表示されます。

```
Keychain name: tcp_ao_keychain1, configured for tcp-ao
Desired key: 1
Detail of last notification from keychain:
Time: 'Jan 23 12:07:39.128', event: Config update, attr: Crypto algorithm, key: 1
Total number of keys: 1
Key details:
    Key ID: 1, Active, Valid
    Active_state: 1, invalid_bits: 0x0, state: 0x110
    Key is configured for tcp-ao, Send ID: 1, Receive ID: 1
    Crypto algorithm: AES_128_CMAC_96, key string chksum: 00028222
    Detail of last notification from keychain:
    Time: 'Jan 23 12:07:39.128', event: Config update, attr: Crypto algorithm
    No valid overlapping key
    No keys invalidated

Total number of usable (Active & Valid) keys: 1
    Keys: 1,
Total number of peers: 24
Peer details:
    Peer: 0x7fc2f00242f8,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

    Peer: 0x7fc2f0024618,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

    Peer: 0x7fc2f00247f8,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

    Peer: 0x7fc2f00249d8,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

    Peer: 0x7fc2f0024bb8,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

    Peer: 0x7fc320037a08,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

    Peer: 0x7fc320037d78,
    Current key not yet available
```

```
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc3200386d8,
Current key not yet available
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc3200388b8,
Current key not yet available
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc320038a98,
Current key not yet available
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc35000d3f8,
Current key: 1
Traffic keys: send_non_SYN: 00476017, recv_non_SYN: ffd520f9
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
Last 1 keys used:
    key: 1, time: Jan 23 12:07:41.953, reason: Peer requested rollover

Peer: 0x7fc320038e78,
Current key not yet available
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc350012758,
Current key not yet available
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc2f0026bc8,
Current key not yet available
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Peer: 0x7fc320048b08,
Current key: 1
Traffic keys: send_non_SYN: 004a05b5, recv_non_SYN: fff639b2
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
Last 1 keys used:
    key: 1, time: Jan 23 12:07:44.209, reason: No current key set

Peer: 0x7fc2f4008388,
Current key: 1
Traffic keys: send_non_SYN: 0029837c, recv_non_SYN: 002af030
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
Last 1 keys used:
    key: 1, time: Jan 23 12:07:44.229, reason: No current key set

Peer: 0x7fc350017198,
Current key: 1
Traffic keys: send_non_SYN: ffdb7322, recv_non_SYN: fff1fb23
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
Last 1 keys used:
    key: 1, time: Jan 23 12:07:45.419, reason: Peer requested rollover
```

```
    Peer: 0x7fc320049098,
    Current key: 1
    Traffic keys: send_non_SYN: ffed0d67, recv_non_SYN: ffe4f959
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
    Last 1 keys used:
        key: 1, time: Jan 23 12:07:55.180, reason: No current key set

    Peer: 0x7fc32005d2a8,
    Current key: 1
    Traffic keys: send_non_SYN: 0021b461, recv_non_SYN: fffe679e
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
    Last 1 keys used:
        key: 1, time: Jan 23 12:07:56.894, reason: No current key set

    Peer: 0x7fc350035c88,
    Current key: 1
    Traffic keys: send_non_SYN: 00296167, recv_non_SYN: fff1c236
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
    Last 1 keys used:
        key: 1, time: Jan 23 12:07:57.859, reason: Peer requested rollover

    Peer: 0x7fc35003fb18,
    Current key: 1
    Traffic keys: send_non_SYN: ffc95844, recv_non_SYN: ffcdfd4f
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
    Last 1 keys used:
        key: 1, time: Jan 23 12:08:00.754, reason: Peer requested rollover

    Peer: 0x7fc350049638,
    Current key: 1
    Traffic keys: send_non_SYN: 002ff48b, recv_non_SYN: ffbe71b9
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
    Last 1 keys used:
        key: 1, time: Jan 23 12:08:10.014, reason: Peer requested rollover

    Peer: 0x7fc350053928,
    Current key: 1
    Traffic keys: send_non_SYN: 00206914, recv_non_SYN: 001df9bc
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
    Last 1 keys used:
        key: 1, time: Jan 23 12:08:12.422, reason: Peer requested rollover

    Peer: 0x7fc2f401f3b8,
    Current key not yet available
    RNext key: 1
    Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000

Total number of Send IDs: 1
Send ID details:
    SendID: 1, Total number of keys: 1
        Keys: 1,
Total number of Receive IDs: 1
Receive ID details:
    ReceiveID: 1, Total number of keys: 1
        Keys: 1,

RP/0/RP0/CPU0:stoat#
```

確認