統合デバッグ情報

このセクションでは、統合デバッグ情報について説明します。

Cisco 適応型セキュリティ アプライアンスのデバッグ情報

ここでは、Cisco 適応型セキュリティ アプライアンスのデバッグ情報について説明します。

Cisco 適応型セキュリティ アプライアンス デバッグ コマンド

次の表に、Cisco 適応型セキュリティ アプライアンスのデバッグ コマンドをリストします。

表 *1 : Cisco* セキュリティ アプライアンスのデバッグ コマンド

送信先	コマンドを使用します。	注記
Cisco 適応型セキュリティ アプライアンス インターフェイスへの ping の ICMP パケット情報を表示します。	**debug icmp trace**	トラブルシューティングが完了グ メッセージを無効にするこます。すべてのデバッグ メッするには、**no debug icmp trac**用します。

送信先	コマンドを使用します。	注記
IM and Presence Service /Cisco 適応型セキュリティ アプライアンス または Cisco 適応型セキュリティ アプライアンス/外部ドメイン間の証明書検証に関連するメッセージを表示します。	**debug crypto ca**	このコマンドに log level パラメー ることで、Cisco 適応型セキュリテ アンス のログレベルを上げること す。次に例を示します。 **debug crypto ca 3**
	debug crypto ca messages	入力および出力メッセージのデバ セージだけを表示します。
	debug crypto ca transactions	トランザクションのデバッグ メッ を表示します。
Cisco 適応型セキュリティ アプライアンスを介して送信された SIP メッセージを表示します。	**debug sip**	
ログメッセージをバッファに送信する（後で表示するため）	**terminal monitor**	
システム ログ メッセージを有効にします。	**logging on**	トラブルシューティングが完了し テム ログ メッセージを無効にする 推奨します。システム ログ メッセ セーブルにするには、 **no logging** ドを使用します。
バッファへのシステム ログ メッセージの送信	**logging buffer debug**	
Telnet または SSH セッションに送信されるシステム ログ メッセージの設定	**logging monitor debug**	
システム ログ メッセージを受信する（syslog）サーバーを指定します	**logging host** *interface_name ip_address*	• interface_name 引数は、syslog アクセスするときの Cisco 適 リティ アプライアンス インタ を指定します。 • ip_address 引数には、syslog サ アドレスを指定します。

送信先	コマンドを使用します。	注記
インターフェイスを ping する	一緒に	Cisco 適応型セキュリティ アプ ンターフェイスへの ping の詳細 フィックが Cisco 適応型セキュ イアンス を正常に通過できる ための異なるインターフェイス での ping の詳細については、 *Appliance Command Line Config* の「Troubleshooting」セクショ ださい。 [ツール（**Tools**）] **[ping** > （**Pi** て、ASDM のインターフェイス することもできます。 （注） パブリック IM and Prese IP アドレスに ping を実行 きません。ただし、Cisc リティ アプライアンスの フェイスの MAC アドレ ブル（**arp –a**）に表示さ ります。
パケットのルートをトレースする	**traceroute**	ASDM でパケットのルートを ともでき、**[ツール（Tools）]**> ト（**Traceroute**）] を選択しま
Cisco 適応型セキュリティ アプライアンスを介したパケットのライフスパンをトレースする	**packet-tracer**	ASDM でパケットのライフスパ することもでき、**[ツール（To** **ト トレーサー（Packet Tracer** す。

関連情報 -

TLS プロキシ デバッグ コマンド

内部および外部インターフェイスでの出力のキャプチャ

ステップ 1 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

ステップ 2 キャプチャするトラフィックを指定するアクセス リストを定義します。次に例を示します。

```
access-list cap extended permit ip 10.53.0.0 255.255.0.0 10.53.0.0 255.255.0.0
```

ステップ 3 テストを開始する前に、キャプチャ コンテンツをクリアすることをお勧めします。内部インターフェイスのキャプチャをクリアするには、「clear capture in」 コマンドを使用し、外部インターフェイスのキャプチャをクリアするには、コマンド「clear capture out」 を使用します。

ステップ 4 次のコマンドを入力して、内部インターフェイスでパケットをキャプチャします。

```
cap in interface inside access-list cap
```

ステップ 5 次のコマンドを入力して、外部インターフェイスでパケットをキャプチャします。

```
cap out interface outside access-list cap
```

ステップ 6 TLS 固有のパケットをキャプチャするには、次のコマンドを入力します。

```
capture capture_name type tls-proxy interface interface_name
```

ステップ 7 パケット キャプチャを取得するには、次のコマンドを入力します。

```
copy /pcap capture:in tftp://xx.xx.xx.xx copy /pcap capture:out tftp://xx.xx.xx.xx
```

出力をディスクにコピーし、ASDM を使用して取得するには、次のコマンドを入力します（**[アクション（Actions）]**、> **[ファイル管理（File Management）]**、> **[ファイル転送（File Transfer）]** を選択）。

```
copy /pcap capture:in disk0:in_1
```

TLS プロキシ デバッグ コマンド

次の表に、TLS プロキシのデバッグ コマンドを示します。

表 *2: TLS* プロキシ デバッグ コマンド

送信先	コマンドを使用
TLS プロキシ関連のデバッグおよび syslog 出力の有効化	**debug inspect tls-proxy events** **debug inspect tls-proxy errors** **debug inspect tls-proxy all**
TLS プロキシ セッションの出力を表示します。	**show log**
アクティブな TLS プロキシ セッションを確認します。	**show tls-proxy**
現在のTLSプロキシセッションの詳細を表示します （Cisco 適応型セキュリティ アプライアンス が IM and Presence サービス および外部ドメインとの接続を正常に確立した場合に使用）	**show tls-proxy session detail**

Access Edge および OCS サーバーのデバッグ

このセクションでは、Access Edge と OCS サーバーのデバッグについて説明します。

OCS/アクセスエッジでのデバッグセッションの開始

ステップ 1 外部 Access Edge サーバーで、**[開始（Start）] > [管理ツール（Administrative Tools）] > [コンピュータ管理（Computer Management）]** を選択します。

ステップ 2 左側のペインで、**[Microsoft Office Communications Server 2007]** を右クリックします。

ステップ 3 **[ロギング ツール（Logging Tool）] > [新しいデバッグセッション（New Debug Session）]** を選択します。

ステップ 4 [ロギングオプション（Logging Options）] で、**[SIP スタック（SIP Stack）]** を選択します。

ステップ 5 [レベル（Level）] の値として、**[すべて（All）]** を選択します。

ステップ 6 **[ロギングの開始（Start Logging）]** をクリックします。

ステップ 7 完了したら、**[ロギングの停止（Stop Logging）]** をクリックします。

ステップ 8 **[ログファイルの分析（Analyze Log Files）]**をクリックします。

Access Edge 上での DNS 構成の確認

ステップ 1 外部 Access Edge サーバーで、**[開始（Start）] > [管理ツール（Administrative Tools）] > [コンピュータ管理（Computer Management）]** を選択します。

ステップ 2 左側のペインで **[Microsoft Office Communications Server 2007]** を右クリックします。

ステップ 3 **[ブロック（Block）]** タブを選択します。

ステップ 4 IM and Presence Service の管理対象ドメインがブロックされていないことを確認します。

ステップ 5 **[アクセス方法（Access Methods）]** ペインで次のオプションが選択されていることを確認します。

a) 他のドメインとのフェデレーション
b) フェデレーション パートナーの検出を許可する

ステップ 6 アクセス エッジが DNS SRV レコードを公開していることを確認します。

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。