統合のデバッグ情報

Cisco Adaptive Security Appliance のデバッグ情報

Cisco Adaptive Security Appliance のデバッグ コマンド

次の表は、Cisco Adaptive Security Appliance のデバッグ コマンドの一覧です。

表 *1*：*Cisco Security Appliance* のデバッグ コマンド

用途	使用するコマンド	注意事項
Show ICMP packet information for pings to the Cisco Adaptive Security Appliance インターフェイスに ping を送信するための 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終わったら、デバッグ メッセージをディセーブルにすることを強くお勧めします。ICMP デバッグ メッセージをディセーブルにするには、**no debug icmp** trace コマンドを使用します。

用途	使用するコマンド	注意事項
IM and Presence/Cisco Adaptive Security Appliance または Cisco Adaptive Security Appliance/外部ドメイン間の証明書の検証に関連するメッセージを表示します	debug crypto ca	ASA のログ レベルを上げるには、次のように、このコマンドにログ レベル パラメータを追加します。 debug crypto ca 3
	debug crypto ca messages	入力および出力メッセージのデバッグ メッセージのみ表示します
	debug crypto ca transactions	トランザクションのデバッグ メッセージのみを表示します
Cisco Adaptive Security Appliance を介して送信された SIP メッセージを表示します	debug sip	
（後で確認するために）ログ メッセージをバッファに送信します	terminal monitor	
システム ログ メッセージをイネーブルにします	logging on	トラブルシューティングが終わったら、システム ログをディセーブルにすることを強くお勧めします。 システム ログ メッセージをディセーブルにするには、**no logging on** コマンドを使用します。
システム ログ メッセージをバッファに送信します	logging buffer debug	
Telnet セッションまたは SSH セッションに送信するシステム ログ メッセージを設定します	logging monitor debug	
システム ログ メッセージを受信する（syslog）サーバを指定します	**logging host** <interface_name> <ip_address>	• interface_name 引数に、syslog サーバにアクセスする Cisco Adaptive Security Appliance インターフェイスを指定します。 • ip_address 引数には、syslog サーバの IP アドレスを指定します。

用途	使用するコマンド	注意事項
インターフェイスに ping を送信します	ping	トラフィックが Cisco Adaptive Security Appliance を経由できることを確認するために、Cisco Adaptive Security Appliance インターフェイスに ping を送信する操作、異なるインターフェイスにあるホスト間で ping を送信する操作の詳細については、『Cisco Security Appliance Command Line Configuration Guide』の「Troubleshooting」を参照してください。 また、ADSM で [ツール（Tools）] > [ping] を選択してインターフェイスに ping を送信することもできます。 （注） IM and Presence のパブリック IP アドレスに ping を送信することはできません。ただし、インターフェイスではない ASA の MAC アドレスが ARP テーブルに表示されます（**arp –a**）。
パケットのルートをトレースします	traceroute	[ツール（Tools）] > [トレースルート（Traceroute）] を使用して ASDM のパケットのルートをトレースすることもできます。
Cisco Adaptive Security Appliance を介するパケットの存続期間をトレースします	packet-tracer	[ツール（Tools）] > [Packet Tracer] を使用して ASDM のパケットの存続期間をトレースすることもできます。

関連トピック

TLS プロキシのデバッグ コマンド, （5 ページ）

内部インターフェイスと外部インターフェイスの出力をキャプチャする

手順

ステップ 1 設定モードで、次のように入力します。

```
>Enable >password
>config t
```

ステップ 2 キャプチャするトラフィックを指定する access-list 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 キャプチャ内容をクリアしてから、テストすることをお勧めします。“clear capture in” コマンドを使用して内部インターフェイスのキャプチャをクリアし、“clear capture out” コマンドを使用して外部インターフェイスのキャプチャをクリアします。

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の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の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 次のコマンドを入力して、TLS 固有のパケットをキャプチャします。

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

ステップ 7 次のコマンドを入力して、パケットのキャプチャを取得します。

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

次のコマンドを入力して、出力をディスクにコピーし、ASDM（[操作（Actions）] > [ファイル管理（File Management）] > [ファイル転送（File Transfer）]）を使用して取得します。

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

TLS プロキシのデバッグ コマンド

次の表は、TLS プロキシのデバッグ コマンドの一覧です。

表 *2*：*TLS* プロキシのデバッグ コマンド

用途	使用するコマンド
TLS プロキシ関連のデバッグおよび syslog の出力をイネーブルにします	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 セッションの詳細情報を表示します （Cisco Adaptive Security Appliance が IM and Presence および外部ドメインとの接続を正常に確立したときに使用します）	show tls-proxy session detail

Access Edge および OCS サーバのデバッグ

OCS/Access Edge でデバッグ セッションを開始する

手順

ステップ 1 外部アクセス エッジ サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（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 [ログ オプション（Logging Options）] の [SIP スタック（SIP Stack）] を選択します。

ステップ 5 [レベル（Level）] 値に [すべて（All）] を選択します。

ステップ 6 [ログの開始（Start Logging）] を選択します。

ステップ 7 完了したら、[ログの停止（Stop Logging）] を選択します。

ステップ 8 [ログ ファイルの解析（Analyze Log Files）] を選択します。

Access Edge の DNS 設定を検証する

手順

ステップ 1 外部アクセス エッジ サーバサーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。

ステップ 2 左側のペインの [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 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) 他のドメインとフェデレーションを行う（Federate with other domains）

b) フェデレーション パートナーの検出を許可する（Allow discovery of federation partners）

ステップ 6 Access Edge が DNS SRV レコードを公開していることを確認します。