PIX および ASA を経由した接続のトラブルシューティング

目次

概要
前提条件
要件
使用するコンポーネント
関連製品
表記法
背景説明
問題
解決策
ステップ 1：ユーザの IP アドレスの検出
ステップ 2：問題の原因をつきとめる
ステップ 3：アプリケーション トラフィックの確認と監視
次のステップ
問題：「Terminating TCP-Proxy Connection」エラー メッセージ
解決策
問題："%「%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface」エラー メッセージ
解決策
問題：「%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows」というエラー メッセージが表示され、ASA によって接続がブロックされる
解決策
問題：「%ASA-5-321001: Resource 'conns' limit of 10000 reached for system」というエラー メッセージが表示される
解決策
問題：「%PIX-1-106021: Deny TCP/UDP reverse path check from src_addr to dest_addr on interface int_name」というエラー メッセージが表示される
解決策
問題：脅威の検出によるインターネット接続の中断
解決策
関連情報

概要

このドキュメントでは、Cisco ASA 5500 シリーズ Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）と Cisco PIX 500 シリーズ セキュリティ アプライアンスを使用する場合にトラブルシューティングを行うためのヒントと推奨事項について説明しています。 多くの場合、アプリケーションやネットワークのソースで障害が発生したり使用できなくなったりす

ると、ファイアウォール（PIX または ASA）がまず疑われ、停止の原因として非難される傾向があります。 ASA または PIX でテストをいくつか行うことで、管理者は ASA または PIX が問題の原因であるかどうかを判断できます。

Cisco ASA をバージョン 8.2 以前と同じ構成にする場合は、『PIX/ASA： Cisco セキュリティ アプライアンス経由の接続の確立とトラブルシューティング』を参照してください。

注: このドキュメントでは ASA と PIX を重点的に取り上げています。 ASA または PIX でのトラブルシューティングを完了した後に、他のデバイス（ルータ、スイッチ、サーバなど）での追加的なトラブルシューティングが必要になる場合があります。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、OS 7.2.1 および 8.3 が稼働する Cisco ASA 5510 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- ASA および PIX OS 7.0、7.1、8.3 以降
- Firewall Services Module（FWSM; ファイアウォール サービス モジュール）2.2、2.3、および 3.1

注: 具体的なコマンドと構文はソフトウェアのバージョンによって異なります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ここでの例では、ASA や PIX が実稼働状態にあることを想定しています。 ASA や PIX の設定は、比較的単純（設定行が 50 程度）な場合もあれば、複雑（設定行が数百から数千）な場合もあります。 ユーザ（クライアント）やサーバは、セキュアなネットワーク（Inside）である場合もあれば、セキュアではないネットワーク（DMZ や Outside）である場合もあります。

ASA は次の設定で開始されます。 この設定の目的は、ラボに対して参照点を提供することです。

ASA の初期設定

```
ciscoasa#show running-config : Saved : ASA Version
7.2(1) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 172.22.1.160
255.255.255.0 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet0/2 nameif dmz security-level 50 ip
address 10.1.1.1 255.255.255.0 ! interface Management0/0
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www access-list inside_acl extended
permit icmp 192.168.1.0 255.255.255.0 any access-list
inside_acl extended permit tcp 192.168.1.0 255.255.255.0
any eq www access-list inside_acl extended permit tcp
192.168.1.0 255.255.255.0 any eq telnet pager lines 24
mtu outside 1500 mtu inside 1500 mtu dmz 1500 no asdm
history enable arp timeout 14400 global (outside) 1
172.22.1.253 nat (inside) 1 192.168.1.0 255.255.255.0 !-
-- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

問題

ユーザから IT 部門に連絡があり、アプリケーション X が動作しなくなったことが報告されます。 この問題は、ASA や PIX の管理者に報告されます。 管理者には、この特定のアプリケーションに関する知識がほとんどありません。 管理者は ASA や PIX を使用して、どのポートとプロトコルがアプリケーション X で使用され、何が問題の原因なのかを突き止めます。

解決策

ASA や PIX の管理者は、できるだけ多くの情報をユーザから収集する必要があります。 役に立つ情報には、次のようなものがあります。

- 送信元 IP アドレス：通常、これはユーザのワークステーションやコンピュータです。
- 宛先 IP アドレス：ユーザやアプリケーションによって接続が試行されるサーバ IP アドレスです。
- アプリケーションによって使用されるポートとプロトコル

多くの場合、管理者にとっては、これらの情報のいずれかが収集できれば好運です。 この例では、管理者はいずれの情報も収集できません。 ASA や PIX の syslog メッセージのレビューは理想的ですが、管理者がその検索対象を把握していない場合、問題をつきとめることは困難です。

ステップ 1：ユーザの IP アドレスの検出

ユーザの IP アドレスを検出するためには、さまざまな方法があります。 このドキュメントでは ASA と PIX を対象としているため、この例では IP アドレスを検出するために ASA と PIX が使用されています。

ユーザが ASA や PIX への通信を試行します。 この通信は、ICMP、Telnet、SSH、または HTTP のいずれでもかまいません。 選択されたプロトコルは ASA や PIX でのアクティビティが制限されています。 この特定の例では、ユーザは ASA の Inside インターフェイスへ PING を発行しています。

管理者は、下記の 3 つのオプションのうち、1 つ以上設定してから、ASA の Inside インターフェイスに対する PING をユーザに実施させる必要があります。

- **Syslog**ロギングが有効になっていることを確認します。 ログレベルを **debug** に設定する必要があります。 ロギングはさまざまな場所に送信できます。 この例では、ASA ログ バッファを使用しています。 実稼働環境では、外部のログ収集サーバが必要な場合があります。 `ciscoasa(config)#`**`logging enable`** `ciscoasa(config)#`**`logging buffered debugging`** ユーザは ASA の Inside インターフェイスへ PING を発行します（ping 192.168.1.1）。 次の出力が表示されます。`ciscoasa#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-6-302020: Built ICMP connection for faddr` **`192.168.1.50`**`/512 gaddr 192.168.1.1/0 laddr 192.168.1.1/0 %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512 gaddr 192.168.1.1/0 laddr 192.168.1.1/0` *`!--- The user IP address is 192.168.1.50.`*
- **ASA キャプチャ機能**管理者は、ASA によってどのトラフィックをキャプチャする必要があるのかを定義するアクセス リストを作成する必要があります。 アクセス リストを定義した後、**capture** コマンドによってアクセス リストが組み込まれ、インターフェイスに適用されます。`ciscoasa(config)#`**`access-list inside_test permit icmp any host 192.168.1.1`** `ciscoasa(config)#`**`capture inside_interface access-list inside_test interface inside`** ユーザは ASA の Inside インターフェイスへ PING を発行します（ping 192.168.1.1）。 次の出力が表示されます。`ciscoasa#`**`show capture inside_interface`** `1: 13:04:06.284897` **`192.168.1.50`** `> 192.168.1.1: icmp: echo request` *`!--- The user IP address is 192.168.1.50.`* **注:** Ethereal などへ利用するためにシステムにこのファイルをダウンロードするには、以下を実施してください。 *`!--- Open an Internet Explorer and browse with this https link format:`* **`https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap`** 『ASA/PIX: CLI および ASDM を使用したパケットのキャプチャの設定例』を参照してください。
- **デバッグdebug icmp trace** コマンドは、ユーザの ICMP トラフィックをキャプチャするために使用されます。`ciscoasa#`**`debug icmp trace`** ユーザは ASA の Inside インターフェイスへ PING を発行します（ping 192.168.1.1）。 コンソールに次の出力が表示されます。`ciscoasa#`

!--- Output is suppressed. ICMP echo request from **192.168.1.50** to 192.168.1.1 ID=512 seq=5120 len=32 ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32 *!--- The user IP address is 192.168.1.50.* **debug icmp trace** を無効にするには、次のコマンドのいずれかを使用します。**no debug icmp traceundebug icmp traceundebug all**、**Undebug all**、または **un all**

管理者が送信元 IP アドレスを判断するためには、これら 3 つのオプションはそれぞれ役に立ちます。 この例では、ユーザの送信元 IP アドレスは 192.168.1.50 です。 管理者は、アプリケーション X の詳細情報を収集し、問題の原因を特定する準備が整いました。

ステップ 2：問題の原因をつきとめる

このドキュメントの「ステップ 1」セクションに記載された情報を参照して、管理者はアプリケーション X セッションのソースを認識できるようになりました。 管理者は、アプリケーション X の詳細情報を収集し、問題である可能性の高い部分の特定を開始する準備が整いました。

ASA や PIX の管理者は、次に掲載した推奨事項の少なくとも 1 つを対象にして、ASA を準備する必要があります。 管理者の準備が整ったら、ユーザはアプリケーション X を開始しますが、追加的なユーザ アクティビティが混乱の原因となったり ASA または PIX の管理者に誤解を与える場合があるため、他のすべてのアクティビティを制限します。

- **syslog メッセージを監視します。**「ステップ 1」で検出したユーザの送信元 IP アドレスを検索します。 ユーザがアプリケーション X を開始します。 ASA 管理者は **show logging** コマンドを発行し、出力を確認します。ciscoasa#**show logging** *!--- Output is suppressed.* %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound **TCP** connection 90 for **outside:172.22.1.1/80** (172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025) ログによって、宛先 IP アドレスが 172.22.1.1、プロトコルが TCP、宛先ポートが HTTP/80、およびトラフィックが Outside インターフェイスに送信されることが明らかになります。
- **キャプチャ フィルタを修正します。**一つ前のステップで **access-list inside_test** コマンドが使用されていますが、ここでも使用されます。ciscoasa(config)#**access-list inside_test permit ip host 192.168.1.50 any** *!--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the ASA.* ciscoasa(config)#**access-list inside_test permit ip any host 192.168.1.50 any** *!--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.* ciscoasa(config)#**no access-list inside_test permit icmp any host 192.168.1.1** ciscoasa(config)#**clear capture inside_interface** *!--- Clears the previously logged data. !--- The **no capture inside_interface** removes/deletes the capture.* ユーザがアプリケーション X を開始します。 次に、ASA 管理者は **show capture inside_interface** コマンドを発行し、出力を確認します。ciscoasa(config)#**show capture inside_interface** 1: 15:59:42.749152 192.168.1.50.1107 > **172.22.1.1**.80: S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK> 2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.**80**: S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK> 3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80: **S** 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK> キャプチャされたトラフィックによって、管理者に貴重な情報がいくつか提供されます。宛先アドレス：172.22.1.1ポート番号：80/httpプロトコル：TCP (「S」または syn フラグに注意) また、管理者はアプリケーション X のデータ トラフィックが ASA に到達していることも認識します。一方、もしこの **show capture inside_interface** コマンドの出力が以下の形であった場合は、アプリケーション トラフィックが ASA に到達しなかったか、またはキャプチャ フィルタがトラフィックをキャプチャするように設定されていなかったこととなります。ciscoasa#**show capture inside_interface** 0 packet captured 0 packet shown この場合、管理者はユーザのコンピュータや、ユーザのコンピュータと ASA の間のパスにある任意のルータまたは他のネットワーク デバイスの調査を検討する必要があります。

注: トラフィックがインターフェイスに到達すると、**capture** コマンドにより、何らかの ASA セキュリティ ポリシーでトラフィックが分析されるよりも前にデータが記録されます。 たとえば、アクセス リストによってインターフェイス上のすべての着信トラフィックが拒否される場合でも、 **capture** コマンドでは、トラフィックの記録が継続します。 その後で、ASA セキュリティ ポリシーによってトラフィックが分析されます。

- **デバッグ**管理者はアプリケーション X を詳しく理解していないため、アプリケーション X 検査のためにどのデバッグ サービスを有効にする必要があるのかがわかりません。 この時点では、デバッグが最善のトラブルシューティング オプションとならない可能性があります。

ステップ 2 で収集された情報を使用して、ASA 管理者は貴重な情報をいくつか取得します。 管理者では、ASA の Inside インターフェイスへのトラフィックの到達、送信元 IP アドレス、宛先 IP アドレス、およびアプリケーション X によって使用されるサービス (TCP/80) が把握されています。 また、syslogs から、当初は通信が許可されていたことも認識されています。

ステップ 3 : アプリケーション トラフィックの確認と監視

ASA 管理者は、アプリケーション X のトラフィックが ASA から送信されていることを確認する必要があり、アプリケーション X サーバからのリターン トラフィックを監視する必要もあります。

- **syslog メッセージを監視します。**送信元 IP アドレス (192.168.1.50) または宛先 IP アドレス (172.22.1.1) を対象に、syslog メッセージをフィルタリングします。 コマンド ラインからは、syslog メッセージのフィルタリングは、**show logging | 192.168.1.50** または **show logging | include 172.22.1.1** のようになります。 次の例では、フィルタリングを行わずに **show logging** コマンドが使用されます。 この出力は、読みやすくするために省略されています。`ciscoasa#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)` **`%ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80 to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout`** `%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30 %ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 duration 0:01:00 %ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00` この syslog メッセージでは、SYN タイムアウトのために接続が閉じられていることが示されています。これによって、管理者は、ASA ではアプリケーション X サーバからの応答がまったく受信されなかったことがわかります。 Syslog メッセージの終了理由はさまざまです。スリーウェイ ハンドシェイクの完了 30 秒後に発生する強制的な接続終了を理由に、SYN タイムアウトがログされます。 通常、この問題は接続要求に対するサーバの応答が失敗すると発生するもので、ほとんどの場合、PIX/ASA 上での設定に関連するものではありません。この問題を解決するには、次のチェックリストを参照してください。スタティック コマンドが正確に入力されていて、たとえば、他のスタティック コマンドと重複していないことを確認する。`static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255`
  ASA 8.3 以降のスタティック NAT は次のように設定できます。`object network obj-y.y.y.y host y.y.y.y`
  `nat (inside,outside) static x.x.x.x`Outside からのグローバル IP アドレスへのアクセスを許可するために、アクセス リストが存在し、インターフェイスにバインドされていることを確認する。
  `access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www`
  `access-group OUTSIDE_IN in interface outside`
  サーバとの正常な接続には、サーバ上のデフォルト ゲートウェイによって、PIX/ASA の DMZ インターフェイスがポイントされている必要がある。syslog メッセージについての詳細

は、『ASA システム メッセージ』を参照してください。

- **新規のキャプチャ フィルタを作成します。**以前にキャプチャされたトラフィックと syslog メッセージから、管理者には、アプリケーション X のトラフィックが Outside インターフェイスを経由して ASA から送出されるはずであることがわかっています。

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80 !--- When you leave the source as 'any', it allows !--- the administrator to monitor any network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any !--- When you reverse the source and destination information, !--- it allows return traffic to be captured. ciscoasa(config)#capture outside_interface access-list outside_test interface outside
```

ユーザは、アプリケーション X を使用して新しいセッションを開始する必要があります。 ユーザが新しいアプリケーション X セッションを開始した後、ASA 管理者は ASA で **show capture outside_interface** コマンドを発行する必要があります。

```
ciscoasa(config)#show capture outside_interface 3 packets captured 1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80: S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK> 2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80: S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK> 3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80: S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK> 3 packets shown
```

このキャプチャでは、Outside インターフェイスから送出されているトラフィックが示されていますが、172.22.1.1 サーバからの応答トラフィックは何も示されていません。 このキャプチャには、データが ASA から送出されるところが示されています。

- **packet-tracer オプションを使用します。**これまでのセクションで、ASA 管理者は ASA で **packet-tracer** オプションを使用するのに十分な情報を収集しています。**注:** バージョン 7.2 以降、ASA では **packet-tracer** コマンドがサポートされます。

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http !--- This line indicates a source port of 1025. If the source !--- port is not known, any number can be used. !--- More common source ports typically range !--- between 1025 and 65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0 255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group inside_acl in interface inside access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www Additional Information: Phase: 6 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 7 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: NAT Subtype: Result: ALLOW Config: nat (inside) 1 192.168.1.0 255.255.255.0 match ip inside 192.168.1.0 255.255.255.0 outside any dynamic translation to pool 1 (172.22.1.254) translate_hits = 6, untranslate_hits = 0 Additional Information: Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028 using netmask 255.255.255.255 Phase: 9 Type: NAT Subtype: host-limits Result: ALLOW Config: nat (inside) 1 192.168.1.0 255.255.255.0 match ip inside 192.168.1.0 255.255.255.0 outside any dynamic translation to pool 1 (172.22.1.254) translate_hits = 6, untranslate_hits = 0 Additional Information: Phase: 10 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 11 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 12 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 13 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 14 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 94, packet dispatched to next module Phase: 15 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional Information: found next-hop 172.22.1.1 using egress ifc outside adjacency Active next-hop mac address 0030.a377.f854 hits 11 !--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the next host !--- that should receive the data packet. Result: input-interface: inside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: allow
```

packet-tracer コマンドの最も重要な出力は、最終行の Action: allow です。

ステップ 3 の 3 つの各オプションによって、管理者は ASA がアプリケーション X の問題の原因ではないことがわかります。 アプリケーション X のトラフィックは ASA から発信されていますが、ASA ではアプリケーション X サーバからの応答は受信されていません。

次のステップ

アプリケーション X が正常な動作を実現するために多くのコンポーネントがあります。 たとえば、ユーザのコンピュータ、アプリケーション X クライアント、ルーティング、アクセス ポリシー、およびアプリケーション X サーバなどです。 前記の例では、アプリケーション X のトラフィックは ASA で受信され、転送されることが証明されました。 この段階で、サーバとアプリケーション X の管理者が関与する必要があります。 管理者は、アプリケーション サービスが稼働していることを確認し、サーバ上のログをレビューし、ユーザのトラフィックがサーバとアプリケーション X によって受信されていることを確認する必要があります。

問題： 「Terminating TCP-Proxy Connection」エラー メッセージ

次のエラー メッセージが表示されます。

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

解決策

説明： このメッセージは、TCP セグメントの構成中に再構成バッファ制限を超えると表示されます。

- *source_address/source_port* : 接続を開始しているパケットの送信元 IP アドレスと送信元ポート
- *dest_address/dest_port* : 接続を開始しているパケットの宛先 IP アドレスと宛先ポート
- *interface_inside* : 接続を開始したパケットが到達するインターフェイスの名前
- *interface_outside* : 接続を開始したパケットが発信されるインターフェイスの名前
- *limit* : トラフィック クラスの設定済み初期接続制限

この問題の解決方法は、次に示すようにセキュリティ アプライアンスで RTSP 検査を無効にすることです。

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

詳細については、Cisco bug ID CSCsl15229 (登録ユーザ専用) を参照してください。

問題： "%「%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface」エラー メッセージ

ASA は、「error:%ASA-6-110003: `Routing failed to locate next-hop for protocol from src interface: src IP/src port to dest interface:` dest IP/dest port」というエラー メッセージを表示してトラフィックをドロップします。

解決策

このエラーは、ASA がインターフェイス ルーティング テーブルでネクスト ホップを見つけようとするときに発生します。 通常、このメッセージは、あるインターフェイス組み込まれている変換（xlate）と別のインターフェイスを示すルートが ASA にあるときに表示されます。 NAT ステートメントの設定ミスをチェックします。 エラーを解決することにより、設定ミスを解決できます。

問題： 「%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows」というエラー メッセージが表示され、ASA によって接続がブロックされる

接続が ASA によってブロックされ、次のエラー メッセージが表示されます。

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

解決策

NAT が実行されている場合、ASA はパケットの反転を試み、任意の変換をヒットするかどうかをチェックします。 任意の変換または別の NAT 変換をヒットしない場合、不一致があります。 同じ送信元および宛先からの発信および着信トラフィックに異なる NAT ルールが設定されている場合、このエラー メッセージは最も多く表示されます。 関心のあるトラフィックの NAT ステートメントをチェックします。

問題： 「%ASA-5-321001: Resource 'conns' limit of 10000 reached for system」というエラー メッセージが表示される

解決策

このエラーは、ASA 全体に配置されているサーバの接続が最大限度に到達したことを示します。 これは、ネットワーク内のサーバへ DoS 攻撃を示している可能性があります。 ASA 上の MPF を使用して、初期接続の制限を小さくします。 また、Dead Connection Detection（DCD）をイネーブルにします。 次の設定の抜粋を参照してください。

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

問題： 「%PIX-1-106021: Deny TCP/UDP reverse path check from src_addr to dest_addr on interface int_name」というエラー メッセージが表示される

解決策

この口グ メッセージは、リバース パスのチェックがイネーブルのときに表示されます。 次のコマンドを発行して、問題を解決し、リバース パスをディセーブルにします。

no ip verify reverse-path interface *<interface name>*

問題： 脅威の検出によるインターネット接続の中断

ASA で、次のエラー メッセージが表示されます。

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

解決策

このメッセージは、デフォルト設定による脅威の検出により、異常なトラフィックの動作が検出されたときに生成されます。 このメッセージは、TCP/UDP ポートである Miralix Licen 3000 を中心に説明します。 ポート 3000 を使用しているデバイスを特定します。 ASDM のグラフ表示の統計情報で脅威の検出をチェックし、上位の攻撃を調べてポート 3000 と送信元 IP アドレスが表示されていることを確認します。 正当なデバイスの場合、ASA の基本脅威検出率を増加してこのエラー メッセージを解決できます。

関連情報

- Cisco ASA コマンド リファレンス
- Cisco PIX コマンド リファレンス
- Cisco ASA エラーとシステム メッセージ
- Cisco PIX エラーとシステム メッセージ
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス サポート
- Cisco PIX 500 シリーズ セキュリティ アプライアンスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems