PIX/ASA 7.x： PIX/ASA 7.x：VoIP（SIP、MGCP、H323、SCCP）サービス有効化の設定例

目次

概要

このドキュメントでは、Outside インターフェイス上の Voice over IP（VoIP）プロトコル トラフィックを許可し、Cisco PIX/ASA セキュリティ アプライアンスの各プロトコルの検査を有効にする方法について説明しています。

このようなプロトコルには、次のものがあります。

- **Session Initiation Protocol（SIP; セッション開始プロトコル）**：SIP は、1 人以上の参加者とのセッションを作成、変更、および終了するアプリケーション層制御（シグナリング）プロトコルです。 これらのセッションには、インターネット電話による通話、マルチメディア配信、マルチメディア会議などが含まれます。SIP は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって定義されているとおり、VoIP コールを有効に

します。 SIP は、Session Descriptor Protocol（SDP）と連携してコール シグナリングを行います。 SDP は、メディア ストリームの詳細を指定します。 SIP が使用されていると、セキュリティ アプライアンスでは、あらゆる SIP（VoIP）ゲートウェイと VoIP プロキシ サーバをサポートできます。 SIP および SDP は、次の RFC で定義されています。SIP： セッション始動プロトコル、RFC 3261SDP: Session Description Protocol、RFC 2327セキュリティ アプライアンスで SIP コールをサポートできるようにするには、メディア接続に使用されるアドレスおよびポートの指定や初期接続を行うためのシグナリング メッセージを検査する必要があります。 これは、既知の宛先ポート（**UDP/TCP 5060**）経由でシグナリングを送信すると、メディア ストリームが動的に割り当てられるためです。 また、SIP によって、IP パケットのユーザ データ部に IP アドレスが埋め込まれます。 SIP 検査では、これらの埋め込まれた IP アドレスに、Network Address Translation（NAT; ネットワーク アドレス変換）が適用されます。**注:** きわめて限定的な状況で、セキュリティ アプライアンスによって保護されているネットワーク上の SIP プロキシへリモート エンドポイントが登録を行おうとすると、登録が失敗します。 この限定的な状況とは、Port Address Translation（PAT; ポート アドレス変換）がリモート エンドポイントに対して設定されている場合、SIP レジストラ サーバが Outside ネットワーク上にある場合、およびエンドポイントからプロキシ サーバに送信された REGISTER メッセージのコンタクト フィールドでポート情報が欠落している場合です。

- **Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）**：MGCP は、中央集中型の制御アーキテクチャ上に構築された、クライアント/サーバ型のコール制御プロトコルです。 ダイヤル プラン情報はすべて、個々のコール エージェントに存在します。 コール エージェントは、ゲートウェイのポートを制御し、コール制御を実行します。 ゲートウェイでは、外部コールに対して Public Switched Telephone Network（PSTN; 公衆電話交換網）と VoIP ネットワーク間のメディア変換を行います。 Cisco ベースのネットワークでは、CallManager がコール エージェントとして機能します。MGCP は、2705 、3435 などのいくつかの RFC で定義されている IETF 標準の 1 つです。 MGCP の機能は、Dual Tone MultiFrequency（DTMF）トーン、Secure RTP、コール保留、コール転送などが含まれるパッケージを使用して拡張できます。MGCP ゲートウェイの設定は、比較的簡単です。 コール エージェントはコール ルーティング情報をすべて保持しているため、そうでない場合に必要となるすべてのダイヤル ピアをゲートウェイに設定する必要がありません。 ただし、コール エージェントが常に使用可能である必要があるという欠点があります。 Cisco MGCP ゲートウェイでは、Survivable Remote Site Telephony（SRST）および MGCP フォールバックを使用することによって、CallManager が使用できない場合に H.323 プロトコルでローカル コール ルーティングを引き継いで提供できます。 この場合、H.323 でダイヤル ピアを使用できるようにゲートウェイで設定する必要があります。
- **H.323**：H.323 検査では、Cisco CallManager や VocalTec Gatekeeper などの H.323 準拠のアプリケーションがサポートされています。 H.323 は、国際電気通信連合によって定義された、LAN 経由でのマルチメディア会議のためのプロトコル セットです。 セキュリティ アプライアンスは H.323 のバージョン 4 までをサポートしています。これには、H.323 バージョン 3 の機能である、1 つのコール シグナリング チャネルでの複数コールも含まれています。 H.323 検査が有効になっていると、セキュリティ アプライアンスでは、H.323 バージョン 3 で導入された機能である同一コール シグナリング チャネルでの複数コールがサポートされます。 この機能によって、コール セットアップ時間が短縮され、セキュリティ アプライアンスでのポートの使用が削減されます。H.323 検査には、次の 2 つの主な機能があります。 H.225 および H.245 メッセージに埋め込まれた必須の IPv4 アドレスのネットワーク アドレス変換。 H.323 メッセージは PER 符号化フォーマットでエンコードされているため、セキュリティ アプライアンスは H.323 メッセージのデコードに ASN.1 デコーダを使用します。 ネゴシエートされた H.245 および RTP/RTCP 接続のダイナミックな割り当て。
- **Skinny（または Simple）Client Control Protocol（SCCP）**：SCCP は、VoIP ネットワークで

使用される簡素化プロトコルです。 SCCP を使用する Cisco IP Phone は、H.323 環境で共存できます。 Cisco CallManager とともに使用すると、SCCP クライアントでは、H.323 準拠の端末との相互運用が可能になります。 セキュリティ アプライアンスのアプリケーション層機能は、SCCP バージョン 3.3 を認識します。 アプリケーション層ソフトウェアの機能では、SCCP シグナリング パケットをネットワーク アドレス変換することによって、すべての SCCP シグナリング パケットおよびメディア パケットがセキュリティ アプライアンスを通過できるようになります。SCCP プロトコルの 5 バージョンがあります: 2.4、3.0.4、3.1.1、3.2、および 3.3.2。 セキュリティ アプライアンスでは、3.3.2 までのすべてのバージョンをサポートしています。 セキュリティ アプライアンスでは、SCCP に対する PAT と NAT の両方をサポートしています。 IP 電話で使用するグローバル IP アドレス数が制限されている場合、PAT が必要です。Cisco CallManager および Cisco IP Phone 間の通常のトラフィックでは SCCP が使用されており、特に設定のない限り SCCP 検査によって処理されます。 また、セキュリティ アプライアンスは、DHCP オプション 150 および 66 もサポートしています。これにより、セキュリティ アプライアンスは、TFTP サーバの場所を Cisco IP Phone やその他の DHCP クライアントに送信できます。 詳細は、『DHCP、DDNS、および WCCP サービスの設定』を参照してください。

前提条件

要件

このドキュメントでは、必要な VPN 設定がすべてのデバイスに対して行われていて、適切に動作することを前提としています。

『ASA/PIX: IOSルータ LAN間IPSECトンネル 設定例へのセキュリティ アプライアンス モデル詳細を VPN 設定について学ぶため。

ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： インターフェイス間の通信を有効に する方法の詳細についてはインターフェイス間の通信を有効に して下さい。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 7.x が稼働する Cisco 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）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

この設定は、ソフトウェア バージョン 7.x が稼働する Cisco 500 シリーズ PIX ファイアウォールにも適用できます。

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

SIP

SIP 検査では、SIP テキスト ベース メッセージがネットワーク アドレス変換され、メッセージの SDP 部分のコンテンツの長さ、およびパケット長とチェックサムが再計算されます。 SIP は、エンドポイントが受信するアドレス/ポートとして SIP メッセージの SDP 部分によって指定されたポートに対するメディア接続を動的にオープンします。

SIP 検査は、コール、発信元、および宛先を識別するための SIP ペイロードにて送信される CALL_ID/FROM/TO の各インデックスを持つデータベースがあります。 このデータベースに格納されているデータは、SDP メディア情報フィールドに格納されたメディア アドレスとメディア ポート、およびメディア タイプです。 1 つのセッションに対し、メディア アドレスとポートが複数ある場合があります。 これらのメディア アドレスとポートを使用して、2 つのエンドポイント間の RTP/RTCP 接続がオープンされます。

初期コール セットアップ (INVITE) メッセージでは、既知のポート 5060 を使用する必要があります。 ただし、その後のメッセージには、このポート番号がない場合があります。 SIP インスペクション エンジンは、シグナリング接続ピンホールをオープンし、これらの接続を SIP 接続としてマーク付けします。 これにより、メッセージが SIP アプリケーションに到達し、ネットワーク アドレス変換されるようになります。

コールがセットアップされると、SIP セッションは transient state と見なされます。 この状態は、宛先エンドポイントが受信する RTP メディア アドレスおよびメディア ポートを示す応答メッセージが届くまで継続します。 1 分以内に応答メッセージを受信しなかった場合、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに遷移し、シグナリング接続は BYE メッセージを受信するまで維持されます。

Inside エンドポイントから Outside エンドポイントにコールする場合、Outside インターフェイスにメディア ホールがオープンし、Inside エンドポイントからの INVITE メッセージで指定された Inside エンドポイントのメディア アドレスおよびメディア ポートに、RTP/RTCP UDP パケットを送信できるようになります。 Inside インターフェイスへの指定されていない RTP/RTCP UDP パケットは、セキュリティ アプライアンス設定で明示的に許可されていない限り、セキュリティ アプライアンスを通過することはありません。

接続がアイドル状態になって 2 分経過すると、メディア接続は切断されます。 このタイムアウト値は設定可能で、時間をより長くすることも短くすることもできます。

MGCP

MGCP を使用するには、通常、少なくとも次の 2 つの検査コマンドを設定する必要があります。 1 つはゲートウェイがコマンドを受信するポートの設定、もう 1 つはコール エージェントがコマンドを受信するポートの設定です。 通常、コール エージェントは、ゲートウェイに対してはデフォルトの MGCP ポート **2427** にコマンドを送信し、ゲートウェイは、コール エージェントに対してはデフォルトの MGCP ポート **2727** にコマンドを送信します。

MGCP メッセージは、**UDP** で伝送されます。 応答はコマンドの送信元アドレス (IP アドレスお

よび UDP ポート番号）に送り返されますが、必ずしもコマンドの送信先のアドレスと同じアドレスから到着するとは限りません。 これが発生するのは、複数のコール エージェントをフェールオーバー設定で使用している場合に、コマンドを受信したコール エージェントがバックアップのコール エージェントに制御を渡し、バックアップのコール エージェントが応答を返す場合です。

H.323

H.323 プロトコルのセットでは、全体で最大 2 つの TCP 接続と 4 ~ 6 の UDP 接続を使用できます。 FastConnect では 1 つの TCP 接続のみ、Reliability, Availability, and Serviceability（RAS）では 1 つの UDP 接続のみを登録、許可、ステータス管理に使用します。

H.323 クライアントでは、最初に、TCP ポート 1720 を使用して H.323 サーバとの TCP 接続を確立し、Q.931 コール セットアップを要求します。 コール セットアップ プロセスの一部として、H.323 端末は、H.245 TCP 接続で使用するポート番号をクライアントに提供します。 H.323 ゲートキーパーを使用している環境では、最初のパケットは UDP を使用して伝送されます。

H.323 検査は Q.931 TCP 接続を監視し、H.245 ポート番号を確認します。 H.323 端末が FastConnect を使用していない場合、H.225 メッセージの検査に基づいてセキュリティ アプライアンスが動的に H.245 接続を割り当てます。

各 H.245 メッセージ内で、H.323 エンドポイントは、後続の UDP データ ストリームで使用するポート番号を交換します。 H.323 検査は H.245 メッセージを検査し、これらのポートを識別してメディア交換のための接続を動的に作成します。 RTP ではネゴシエートされたポート番号が使用され、RTCP ではその次に大きいポート番号が使用されます。

H.323 制御チャネルでは、H.225、H.245、および H.323 RAS が制御されます。 H.323 検査では次のポートが使用されます。

- 1718：ゲートキーパー ディスカバリ UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

H.225 コール シグナリングのために、well-known ポートである H.323 ポート 1720 のトラフィックを許可する必要があります。 ただし、H.245 シグナリング ポートは、H.225 シグナリング内のエンドポイント間でネゴシエートされます。 H.323 ゲートキーパーを使用している場合、Admission Confirmation（ACF）メッセージの検査に基づいてセキュリティ アプライアンスが H.225 接続をオープンします。

H.225 メッセージの検査が終了すると、セキュリティ アプライアンスは H.245 チャネルをオープンし、H.245 チャネル経由で伝送されるトラフィックを検査します。 セキュリティ アプライアンスを通過する H.245 メッセージは、すべて H.245 アプリケーション検査を受けます。これにより、埋め込まれた IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルがオープンされます。

H.323 ITU 標準規格では、信頼性のある接続上に送信する前に、H.225 および H.245 の前に TPKT ヘッダーによりメッセージの長さを定義することが規定されています。 TPKT ヘッダーは H.225/H.245 メッセージと同じ TCP パケットで送信されるとは限らないので、メッセージを適切に処理およびデコードするには、セキュリティ アプライアンスで TPKT 長を保持しておく必要があります。 セキュリティ アプライアンスでは、接続ごとに、次に予測されるメッセージの TPKT 長が格納されたレコードを保持しています。

セキュリティ アプライアンスでメッセージ内の IP アドレスを NAT 変換する必要がある場合には、チェックサム、User-User Information Element（UUIE）、および TPKT（H.225 メッセージの

TCP パケットに含まれている場合）を変更する必要があります。 もし TPKT が別の TCP パケットで送信される場合には、セキュリティ アプライアンスは TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの TPKT を付加します。

SCCP

Cisco CallManager が、Cisco IP Phone より高いセキュリティ インターフェイス上に存在するトポロジで、Cisco CallManager IP アドレスの NAT が必要な場合、Cisco IP Phone では、Cisco CallManager IP アドレスを設定で明示的に指定する必要があるため、スタティックなマッピングを使用する必要があります。 アイデンティティ スタティック エントリによって、より高いセキュリティ インターフェイス上の Cisco CallManager で Cisco IP Phone からの登録を受け付けることができるようになります。

Cisco IP Phone では、Cisco CallManager サーバへの接続に必要な設定情報をダウンロードするために TFTP サーバにアクセスする必要があります。

Cisco IP Phone が TFTP サーバより低いセキュリティ インターフェイス上にある場合、保護された TFTP サーバに UDP ポート 69 で接続するには、アクセス リストを使用する必要があります。 TFTP サーバに対するスタティック エントリは必要ですが、これはアイデンティティ スタティック エントリである必要はありません。 NAT が使用されている場合、アイデンティティ スタティック エントリは同じ IP アドレスにマッピングされます。 PAT が使用されている場合、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager より高いセキュリティ インターフェイス上にある場合、Cisco IP Phone で接続を開始するのにアクセス リストもスタティック エントリも必要ありません。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

SIP のネットワーク ダイアグラム

このセクションでは、次のネットワーク設定を使用します。

SIP の設定例

この項では、次の設定例を使用しています。

セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズム機能によって、アプリケーション検査をサポートしています。 アダプティブ セキュリティ アルゴリズムで使用されるアプリケーションのステートフル インスペクションによって、セキュリティ アプライアンスは、ファイアウォールを通過する各コネクションをトラッキングし、これらのコネクションが有効であることを確認します。 また、ファイアウォールはステートフル インスペクションによってコネクションの状態も監視し、状態テーブルに情報を格納します。 管理者定義のルールに加えて状態テーブルを使用することで、フィルタリングの決定が、過去にファイアウォールを通過したパケットによって確立されたコンテキスト情報に基づいて行われるようになります。 アプリケーシ

ョン検査の実装は、次の処理で構成されています。

- トラフィックを識別する。
- トラフィックに検査を適用する。
- インターフェイス上での検査をアクティブ化する。

基本的な SIP 検査の設定

デフォルトでは、デフォルトのアプリケーション検査トラフィックをすべて照合する 1 つのポリシー（グローバル ポリシー）が設定に含まれており、これによりすべてのインターフェイス上のトラフィックに検査が適用されます。 デフォルトのアプリケーション検査トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。 適用できるグローバル ポリシーは 1 つだけです。 したがって、グローバル ポリシーを変更する場合、たとえば、非標準ポートに検査を適用したり、デフォルトでは有効でない検査を追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にして新しいポリシーを適用する必要があります。 すべてのデフォルトのポートのリストについては、『デフォルトの検査ポリシー』を参照してください。

1. **policy-map global_policy** コマンドを発行します。`ASA5510(config)#policy-map global_policy`
2. **class inspection_default** コマンドを発行します。`ASA5510(config-pmap)#class inspection_default`
3. **inspect sip** コマンドを実行します。`ASA5510(config-pmap-c)#inspect sip`

SIP の ASA 設定

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming SIP traffic. access-list 100 extended permit
tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq sip pager
lines 24 mtu inside 1500 mtu outside 1500 no failover
asdm image disk0:/asdm-522.bin no asdm history enable
arp timeout 14400 !--- Command to redirect the SIP
traffic received on outside interface to !--- inside
interface for the specified IP address. static
(inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1 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 h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp !--- Command to enable SIP
inspection. inspect sip inspect xdmcp inspect ftp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

MGCP、H.323、および SCCP のネットワーク ダイアグラム

このセクションでは、次のネットワーク設定を使用します。

MGCP の設定例

この項では、次の設定例を使用しています。

セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズム機能によって、アプリケーション検査をサポートしています。 アダプティブ セキュリティ アルゴリズムで使用されるアプリケーションのステートフル インスペクションによって、セキュリティ アプライアンスは、ファイアウォールを通過する各コネクションをトラッキングし、これらのコネクションが有効であることを確認します。 また、ファイアウォールはステートフル インスペクションによってコネクションの状態も監視し、状態テーブルに情報を格納します。 管理者定義のルールに加えて状態テーブルを使用することで、フィルタリングの決定が、過去にファイアウォールを通過したパケットによって確立されたコンテキスト情報に基づいて行われるようになります。 アプリケーション検査の実装は、次の処理で構成されています。

- トラフィックを識別する。
- トラフィックに検査を適用する。
- インターフェイス上での検査をアクティブ化する。

基本的な MGCP 検査の設定

デフォルトでは、デフォルトのアプリケーション検査トラフィックをすべて照合する 1 つのポリシー（グローバル ポリシー）が設定に含まれており、これによりすべてのインターフェイス上のトラフィックに検査が適用されます。 デフォルトのアプリケーション検査トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。 適用できるグローバル ポリシーは 1 つだけです。 したがって、グローバル ポリシーを変更する場合、たとえば、非標準ポートに検査を適用したり、デフォルトでは有効でない検査を追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にして新しいポリシーを適用する必要があります。 すべてのデフォルトのポートのリストについては、『デフォルトの検査ポリシー』を参照してください。

1. **policy-map global_policy** コマンドを発行します。`ASA5510(config)#policy-map global_policy`
2. **class inspection_default** コマンドを発行します。`ASA5510(config-pmap)#class inspection_default`
3. **inspect mgcp** コマンドを実行します。`ASA5510(config-pmap-c)#inspect mgcp`

追加検査の制御に対する MGCP 検査ポリシー マップの設定

セキュリティ アプライアンスがピンホールをオープンする必要のあるコール エージェントとゲートウェイがネットワーク上に複数存在する場合、MGCP マップを作成します。 これにより、MGCP 検査を有効にする際に、この MGCP マップを適用できます。 詳細は、『アプリケーション検査の設定』を参照してください。

```
!--- Permits inbound 2427 port traffic. ASA5510(config)#access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2427 !--- Permits inbound 2727 port traffic.
ASA5510(config)#access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq
2727 ASA5510(config)#class-map mgcp_port ASA5510(config-cmap)#match access-list 100
ASA5510(config-cmap)#exit !--- Command to create an MGCP inspection policy map.
ASA5510(config)#policy-map type inspect mgcp mgcpmap !--- Command to configure parameters that
affect the !--- inspection engine and enters into parameter configuration mode. ASA5510(config-
pmap)#parameters !--- Command to configure the call agents. ASA5510(config-pmap-p)#call-agent
10.1.1.10 101 !--- Command to configure the gateways. ASA5510(config-pmap-p)#gateway 10.2.2.5
101 !--- Command to change the maximum number of commands !--- allowed in the MGCP command
queue. ASA5510(config-pmap-p)#command-queue 150 ASA5510(config-pmap-p)# exit
ASA5510(config)#policy-map inbound_policy ASA5510(config-pmap)# class mgcp_port ASA5510(config-
pmap-c)#inspect mgcp mgcpmap ASA5510(config-pmap-c)# exit ASA5510(config)#service-policy
inbound_policy interface outside
```

MGCP の ASA 設定

```
ASA Version 7.2(1)24
!
hostname ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Permits inbound 2427 and 2727 port traffic. access-
list 100 extended permit udp 10.2.2.0 255.255.255.0 host
172.16.1.5 eq 2427 access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2727 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover no
asdm history enable arp timeout 14400 !--- Command to
redirect the MGCP traffic received on outside interface
to !--- inside interface for the specified IP address.
static (inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
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 mgcp_port match access-list 100 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 inspect mgcp policy-map type inspect
mgcp mgcpmap parameters call-agent 10.1.1.10 101 gateway
10.2.2.5 101 command-queue 150 policy-map inbound_policy
class mgcp_port inspect mgcp mgcpmap ! service-policy
global_policy global service-policy inbound_policy
interface outside prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

H.323 の設定例

この項では、次の設定例を使用しています。

セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズム機能によって、アプリケーション検査をサポートしています。 アダプティブ セキュリティ アルゴリズムで使用されるアプリケーションのステートフル インスペクションによって、セキュリティ アプライアンスは、ファイアウォールを通過する各コネクションをトラッキングし、これらのコネクションが有効であることを確認します。 また、ファイアウォールはステートフル インスペクションによってコネクションの状態も監視し、状態テーブルに情報を格納します。 管理者定義のルールに加えて状態テーブルを使用することで、フィルタリングの決定が、過去にファイアウォールを通過したパケットによって確立されたコンテキスト情報に基づいて行われるようになります。 アプリケーション検査の実装は、次の処理で構成されています。

- トラフィックを識別する。
- トラフィックに検査を適用する。
- インターフェイス上での検査をアクティブ化する。

基本的な H.323 検査の設定

デフォルトでは、デフォルトのアプリケーション検査トラフィックをすべて照合する 1 つのポリシー（グローバル ポリシー）が設定に含まれており、これによりすべてのインターフェイス上のトラフィックに検査が適用されます。 デフォルトのアプリケーション検査トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。 適用できるグローバル ポリシーは 1 つだけです。 したがって、グローバル ポリシーを変更する場合、たとえば、非標準ポートに検査を適用したり、デフォルトでは有効でない検査を追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にして新しいポリシーを適用する必要があります。 すべてのデフォルトのポートのリストについては、『デフォルトの検査ポリシー』を参照してください。

1. policy-map global_policy コマンドを発行します。`ASA5510(config)#policy-map global_policy`
2. class inspection_default コマンドを発行します。`ASA5510(config-pmap)#class inspection_default`
3. inspect h323 コマンドを実行します。`ASA5510(config-pmap-c)#inspect h323 h225`
   `ASA5510(config-pmap-c)#inspect h323 ras`

H.323 の ASA 設定

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
```

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming Gate Keeper Discovery UDP port traffic. access-
list 100 extended permit udp 10.2.2.0 255.255.255.0 host
172.16.1.5 eq 1718 !--- Command to allow the incoming
RAS UDP port. access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 1719 !---
Command to allow the incoming h323 protocol traffic.
access-list 100 extended permit tcp 10.2.2.0
255.255.255.0 host 172.16.1.5 eq h323 pager lines 24 mtu
inside 1500 mtu outside 1500 no failover asdm image
disk0:/asdm-522.bin no asdm history enable arp timeout
14400 !--- Command to redirect the h323 protocol traffic
received on outside interface to !--- inside interface
for the specified IP address. static (inside,outside)
172.16.1.5 10.1.1.10 netmask 255.255.255.255 access-
group 100 in interface outside route outside 0.0.0.0
0.0.0.0 172.16.1.1 1 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 !---
Command to enable H.323 inspection. 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 inspect
ftp ! !--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

SCCP の設定例

この項では、次の設定例を使用しています。

セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズム機能によって、アプリケーション検査をサポートしています。 アダプティブ セキュリティ アルゴリズムで使用されるアプリケーションのステートフル インスペクションによって、セキュリティ アプライアンスは、ファイアウォールを通過する各コネクションをトラッキングし、これらのコネクションが有効であることを確認します。 また、ファイアウォールはステートフル インスペクションによってコネクションの状態も監視し、状態テーブルに情報を格納します。 管理者定義のルールに加えて状態テーブルを使用することで、フィルタリングの決定が、過去にファイアウォールを通過したパケットによって確立されたコンテキスト情報に基づいて行われるようになります。 アプリケーション検査の実装は、次の処理で構成されています。

- トラフィックを識別する。

- トラフィックに検査を適用する。
- インターフェイス上での検査をアクティブ化する。

基本的な SCCP 検査の設定

デフォルトでは、デフォルトのアプリケーション検査トラフィックをすべて照合する 1 つのポリシー (グローバル ポリシー) が設定に含まれており、これによりすべてのインターフェイス上のトラフィックに検査が適用されます。 デフォルトのアプリケーション検査トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。 適用できるグローバル ポリシーは 1 つだけです。 したがって、グローバル ポリシーを変更する場合、たとえば、非標準ポートに検査を適用したり、デフォルトでは有効でない検査を追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にして新しいポリシーを適用する必要があります。 すべてのデフォルトのポートのリストについては、『デフォルトの検査ポリシー』を参照してください。

1. **policy-map global_policy** コマンドを発行します。`ASA5510(config)#policy-map global_policy`
2. **class inspection_default** コマンドを発行します。`ASA5510(config-pmap)#class inspection_default`
3. **inspect skinny** コマンドを実行します。`ASA5510(config-pmap-c)#inspect skinny`

SCCP の ASA 設定

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming SCCP traffic. access-list 100 extended permit
tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2000 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover
asdm image disk0:/asdm-522.bin no asdm history enable
arp timeout 14400 !--- Command to redirect the SIP
traffic received on outside interface to !--- inside
interface for the specified IP address. static
(inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1 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 h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp !---
Command to enable SCCP inspection. inspect skinny
inspect esmtp inspect sqlnet inspect sunrpc inspect tftp
inspect sip inspect xdmcp inspect ftp ! !--- This
command tells the device to !--- use the "global_policy"
policy-map on all interfaces. service-policy
global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

SIP：

設定が正常に行われたことを確認するには、**show service-policy** コマンドを使用し、**show service-policy inspect sip** コマンドを使用して出力を SIP 検査だけに制限します。

```
ASA5510#show service-policy inspect sip Global policy: Service-policy: global_policy Class-map:
inspection_default Inspect: sip, packet 0, drop 0, reset-drop 0 ASA5510#
```

MGCP：

```
ASA5510#show service-policy inspect mgcp Global policy: Service-policy: global_policy Class-map:
inspection_default Inspect: skinny, packet 0, drop 0, reset-drop 0
```

H.323：

```
ASA5510(config)#show service-policy inspect h323 h225 Global policy: Service-policy:
global_policy Class-map: inspection_default Inspect: h323 h225 _default_h323_map, packet 0, drop
0, reset-drop 0 h245-tunnel-block drops 0 connection ASA5510(config)#show service-policy inspect
h323 ras Global policy: Service-policy: global_policy Class-map: inspection_default Inspect:
h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0 h245-tunnel-block drops 0 connection
```

SCCP：

```
ASA5510(config)#show service-policy inspect skinny Global policy: Service-policy: global_policy
Class-map: inspection_default Inspect: skinny, packet 0, drop 0, reset-drop 0
```

トラブルシューティング

問題

オフィス伝達者はパススルー ASA できません、VPN トンネルに登録されている iPhone は接続が解除されます、または VPN トンネルを渡る IP フォンにオーディオがありません。

解決策

Office Communicator は標準 SIP を使用していないため、ASA では、デフォルトで Office Communicator をドロップします。 ASA のこの問題およびまた `clear xlate` および 解決するために SIP、Skinny および H323 インスペクションをディセーブルにして下さい。 同じソリューションは IPhone に適用されますも。

問題

ビデオ呼び出しは `%ASA-4-405102` と失敗しました： `laddr XX.XX.XX.XX/3239` エラーメッセージ `faddr XX.XX.XX.XX  H245` 。

解決策

ディセーブル H323 インスペクションこの問題を解決するため。

関連情報

- PIX/ASA 7.x： PIX/ASA 7.x：インターフェイス間通信の有効化および無効化
- PIX ファイアウォールでの VoIP トラフィックの処理
- Cisco Unified CallManager 5.0 における TCP ポートおよび UDP ポートの使用状況
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス製品のサポート
- Cisco PIX 500 シリーズ セキュリティ アプライアンス製品に関するサポート ページ
- メディア ゲートウェイ コントロール プロトコル（MGCP）テクノロジーに関するサポート
- Skinny Call Control Protocol（SCCP）テクノロジーに関するサポート
- H.323 テクノロジーに関するサポート
- テクニカルサポートとドキュメント - Cisco Systems