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

内容

概要

このドキュメントでは、ASA/PIX セキュリティ アプライアンスのインターフェイス間のさまざまな形式の通信の設定例を紹介します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- IP アドレスとデフォルト ゲートウェイの割り当て
- デバイス間の物理ネットワーク接続
- 実装するサービス用に特定された通信ポート番号

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン 7.x 以降のソフトウェアを実行する適応型セキュリティ アプライアンス
- Windows 2003 Server
- Windows XP ワークステーション

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、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。

- 7.x 以降を実行する PIX 500 シリーズ ファイアウォール

表記法

ドキュメント表記の詳細については、『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

このドキュメントは、異なるインターフェイス間の通信フローを確立するために必要な手順についてまとめたものです。次のような通信形式を取り上げています。

1. DMZ にあるリソースへのアクセスが必要な、外部に設置されているホストからの通信
2. DMZ にあるリソースへのアクセスが必要な、内部ネットワークに設置されているホストからの通信
3. 外部にあるリソースへのアクセスが必要な、内部および DMZ ネットワークに設置されているホストからの通信

NAT

この例では、設定でネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）を使用します。アドレス変換は、パケット内の実際のアドレス（ローカル）を、宛先ネットワーク上でルーティング可能なマッピングされたアドレス（グローバル）に置き換えます。NAT は、実際のアドレスがマッピングされたアドレスに変換されるプロセスと、戻りのトラフィック用に変換を元に戻すプロセスの 2 つの手順から構成されています。この設定ガイドでは、スタティックとダイナミックの 2 つの形式のアドレス変換を使用します。

ダイナミック変換によって、各ホストは後続の各変換用に、異なるアドレスやポートを使用できるようになります。ダイナミック変換は、ローカル ホストが 1 つ以上の共通グローバル アドレスを共有したり、非表示にしたりする際に使用できます。このモードでは、1 つのローカル アドレスで変換用のグローバル アドレスを永続的に予約することはできません。代わりに、多対一または多対多のアドレス変換が行われ、必要な場合にのみ変換エントリが作成されます。変換エントリは使用されなくなると削除されて、他のローカル ホストで使用可能になります。このタイプの変換は、接続時にのみダイナミック アドレスやポート番号が割り当てられる、内部ホストのアウトバウンド接続に最適です。ダイナミック アドレス変換には、次の 2 つの形式があります。

- ダイナミック NAT：ローカル アドレスが、次に使用可能なプールのグローバル アドレスに変換されます。変換は一対一で行われるため、多数のローカル ホストで同一時間に変換する必要がある場合は、グローバル アドレスのプールが枯渇する可能性があります。
- NAT オーバーロード（PAT）：ローカル アドレスが 1 つのグローバル アドレスに変換されます。各接続は、グローバル アドレスの次に使用可能な上位ポート番号が接続元として割り当てられた場合に、一意で実行されます。多数のローカル ホストが 1 つの共通グローバル アドレスを共有しているため、変換は多対一で行われます。

スタティック変換では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。スタティック NAT 設定では、ホストによって各接続に同じアドレスがマッピングされるため、永続的な変換ルールとなります。スタティック アドレス変換は、内部またはローカルのホストで全接続に同じグローバル アドレスが必要な場合に使用されます。アドレス変換は一対一で行われます。スタティック変換は、単一ホストに、または IP サブネットに含まれるすべてのアドレスに定義できます。

ダイナミック NAT と、スタティック NAT のアドレス範囲との主な違いは、スタティック NAT では、変換されたホストへの接続をリモート ホストが開始できるが（それを許可するアクセス リストがある場合）、ダイナミック NAT ではできないことです。また、スタティック NAT では、同じ数のマップ アドレスが必要です。

セキュリティ アプライアンスは、NAT ルールがトラフィックに一致すると、アドレスを変換します。NAT ルールが一致しなかった場合、パケットの処理が続行されます。ただし、NAT 制御を有効にしている場合は例外です。NAT コントロールを有効にした場合、セキュリティの高いインターフェイス（inside）から低いセキュリティ レベル（outside）に移動するパケットは NAT ルールに一致する必要があり、一致しないとそのパケットの処理は停止します。一般的な設定情報を表示するには、『PIX/ASA 7.x NATおよびPAT』を参照してくださいい。NAT の動作の詳細を理解するには、『NAT の動作の仕組み』を参照してください。

ヒント：NAT設定を変更する場合は、常に現在のNAT変換をクリアすることをお勧めします。変換テーブルのクリアは、**clear xlate** コマンドを使用して実行できます。**ただし、これを実行する場合は注意が必要です。**なぜなら、変換テーブルをクリアすると、変換を使用する現在の接続がすべて切断されるからです。変換テーブルをクリアする代わりに、現在の変換がタイムアウトされるのを待機する方法がありますが、これは推奨できません。新たなルールで新しい接続が作成されると、予期せぬ動作が引きこされる可能性があります。

セキュリティ レベル

セキュリティ レベル値は、さまざまなインターフェイスのホストやデバイスの相互通信方法を制御します。デフォルトでは、インターフェイスに接続されたセキュリティ レベルの高いホストやデバイスから、セキュリティ レベルの低いホストやデバイスに接続し、通信できるようになっています。セキュリティ レベルの低いインターフェイスに接続されたホストやデバイスからは、アクセス リストの許可がないかぎり、セキュリティ レベルの高いインターフェイスに接続されたホストやデバイスへ接続できません。

security-level コマンドは、バージョン 7.0 で初めて採用され、インターフェイスのセキュリティ レベルに割り当てられた **nameif** コマンドの一部を代替します。「inside」と「outside」の 2 つのインターフェイスには、デフォルトのセキュリティ レベルが割り当てられていますが、それらは **security-level** コマンドで上書きできます。インターフェイス名を「inside」にすると、デフォルトのセキュリティ レベルは 100 となります。「outside」という名前のインターフェイスには、デフォルトのセキュリティレベル0が割り当てられます。新しく追加されたインターフェイスには、すべてデフォルトのセキュリティレベル0が割り当てられます。新しいセキュリティレベルをインターフェイスに割り当てるには、インターフェイスコマンドモードで**security-levelコマンドを**

使用します。セキュリティ レベルの範囲は 1 ~ 100 です。

注：セキュリティレベルは、ファイアウォールがトラフィックを検査および処理する方法を決定するためにのみ使用されます。たとえば、セキュリティ レベルの高いインターフェイスから低いインターフェイスへと渡されたトラフィックは、セキュリティ レベルの低いインターフェイスから高いインターフェイスへ渡されるトラフィックよりも厳しくないデフォルト ポリシーで転送されます。セキュリティ レベルの詳細については、『ASA/PIX 7.x コマンド リファレンス ガイド』を参照してください。

ASA/PIX 7.x では、同じセキュリティ レベルで複数のインターフェイスを設定できます。たとえば、パートナーや他のDMZに接続された複数のインターフェイスすべてにセキュリティレベル50を設定できます。デフォルトでは、これらの同じセキュリティインターフェイスは相互に通信できません。この問題を解決するため、**same-security-traffic permit inter-interface** コマンドが導入されています。このコマンドを使用すると、同じセキュリティ レベルのインターフェイス間の通信が可能になります。同じセキュリティ レベルのインターフェイスの詳細については、『コマンド リファレンス ガイド』の「インターフェイス パラメータの設定」とこちらの例を参照してください。

ACL

アクセス コントロール リストは、通常、リンクされたリストのセキュリティ アプライアンスによって内部構成される複数のアクセス コントロール エントリ (ACE) から構成されています。ACE は、ホストやネットワークからの一連のトラフィックについて説明し、そのトラフィックに適用するアクション (通常は許可や拒否) のリストを作成します。パケットがアクセス リストの制御を受ける場合は、Cisco セキュリティ アプライアンスが ACE にリンクされたリストを検索し、パケットに一致するものを見つけ出します。**セキュリティ アプライアンスに一致する最初の ACE は、パケットに適用される ACE です。**一致する ACE が見つかると、その ACE のアクション (許可や拒否) がパケットに適用されます。

インターフェイスや方向ごとに 1 つのアクセス リストしか許可されません。つまり、インターフェイスのインバウンド トラフィックに適用されるのは 1 つのアクセス リストのみで、インターフェイスのアウトバウンド トラフィックに適用されるのは 1 つのアクセス リストのみです。インターフェイスに適用されない NAT ACL などのアクセス リストは、無制限となります。

注：デフォルトでは、すべてのアクセスリストには、すべてのトラフィックを拒否する暗黙的なACEが存在するため、アクセスリストに入力したACEに一致しないすべてのトラフィックは、最後に暗黙的なdenyに一致し、廃棄されます。インターフェイス アクセス リストでは、トラフィックのフローを実現するため、1 つ以上の許可ステートメントを設定する必要があります。許可ステートメントがないと全トラフィックが拒否されます。

注：アクセスリストは、**access-listコマンドと**access-group**コマンドで実装**されます。これらのコマンドは、PIX Firewall ソフトウェアの以前のバージョンで使用されていた、**conduit** コマンドおよび **outbound** コマンドの代わりに使用されます。ACL の詳細については、『IP アクセス リストの設定』を参照してください。

設定

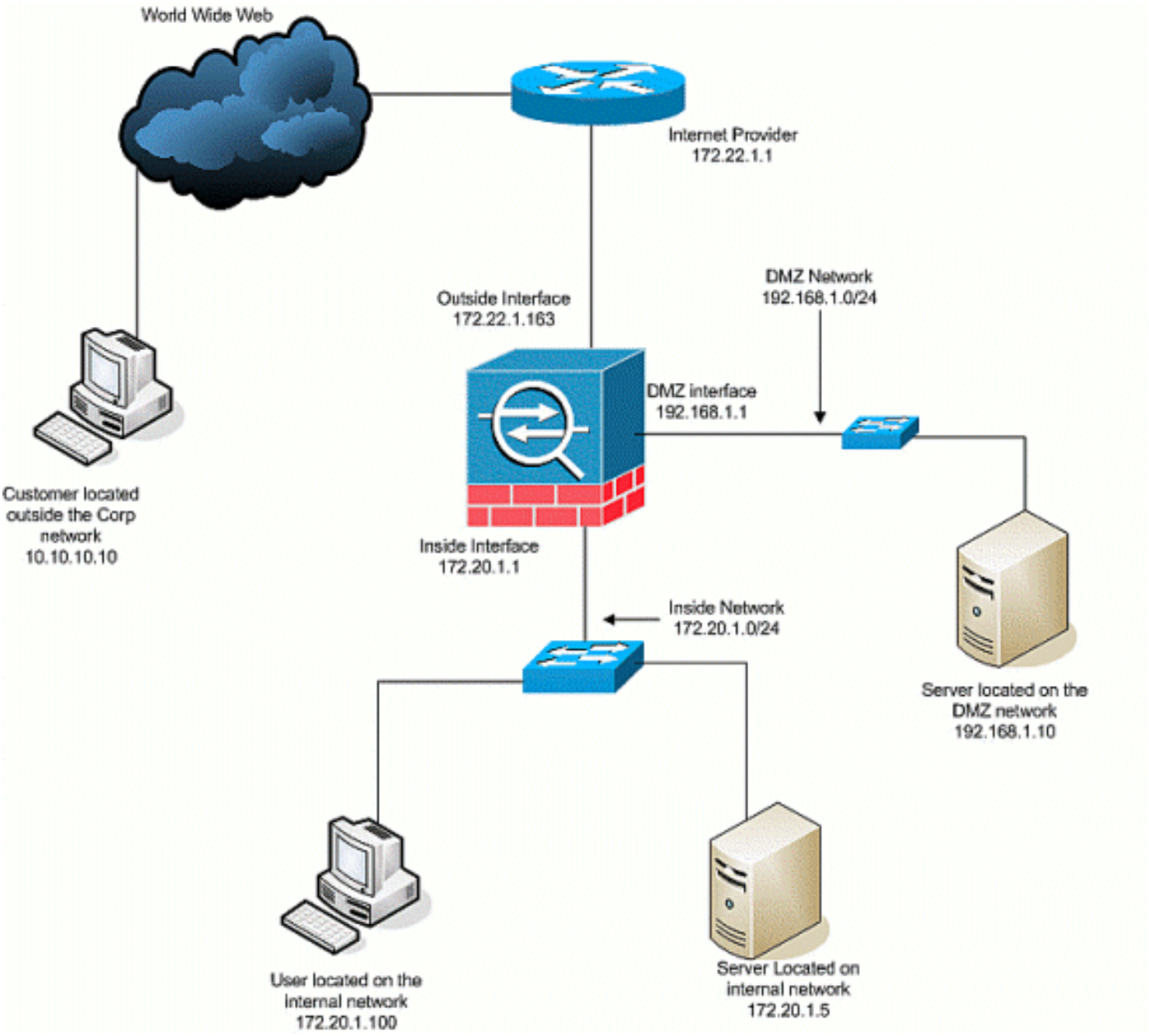
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



初期設定

このドキュメントでは、次の構成を使用します。

- この基本ファイアウォール設定では、現在、NAT/STATIC ステートメントはありません。
- 適用されている ACL がないため、deny any any の暗黙的 ACE が使用されています。

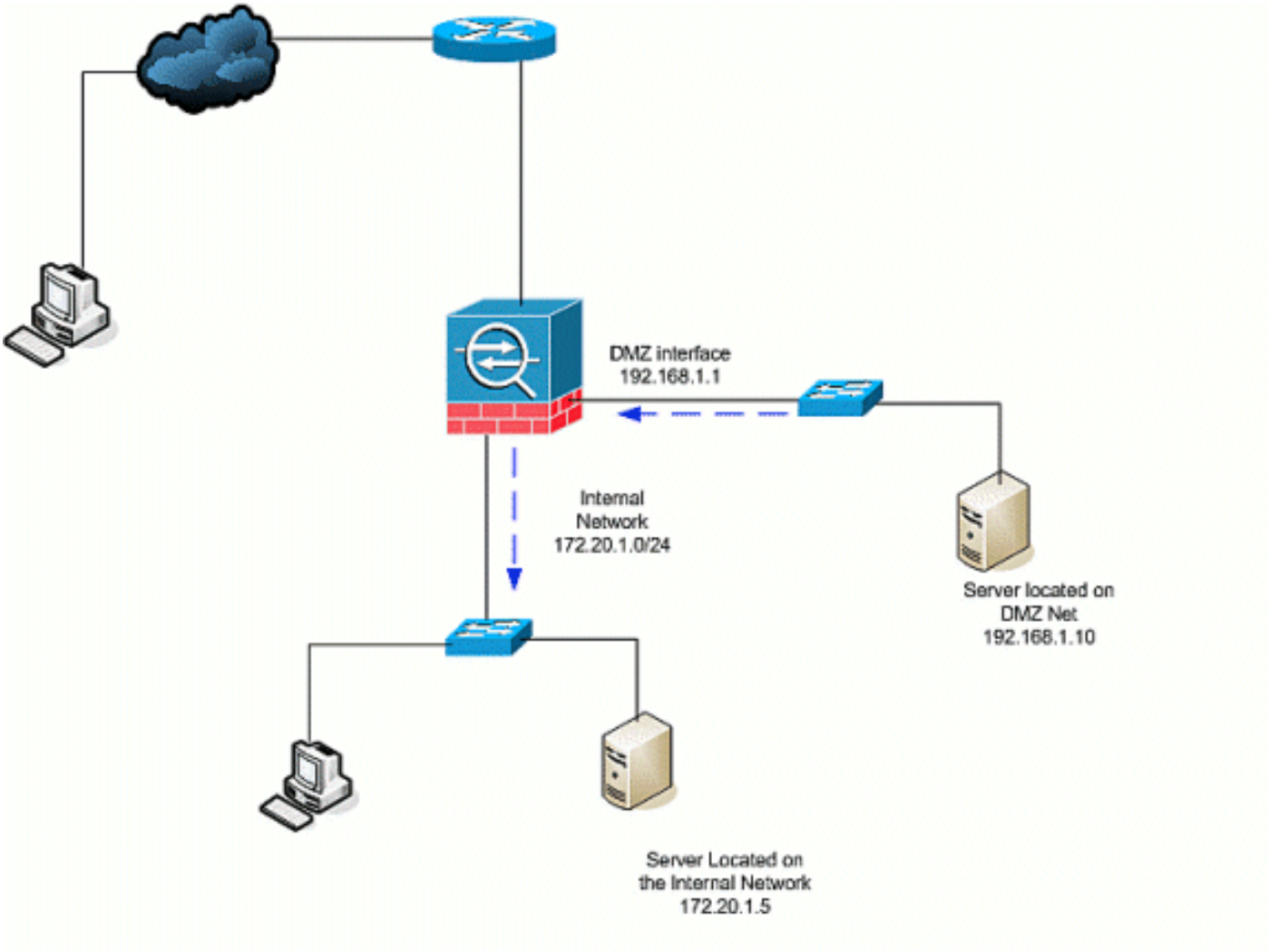
デバイス名 1
ASA-AIP-CLI(config)#**show running-config**

```
 ASA Version 7.2(2)
!
hostname ASA-AIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 172.22.1.163 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.20.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/3
 nameif DMZ-2-testing
 security-level 50
 ip address 192.168.10.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu inside 1500
mtu Outside 1500
mtu DMZ 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat-control
route Outside 0.0.0.0 0.0.0.0 172.22.1.1 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 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:4b2f54134e685d11b274ee159e5ed009
: end
ASA-AIP-CLI(config)#
```

DMZ から内部へ

DMZ から内部ネットワーク ホストへの通信を可能にするには、次のコマンドを使用します。この例では、DMZ の Web サーバで内部の AD および DNS サーバにアクセスする必要があります。



1. DMZ 上の AD および DNS サーバに、スタティック NAT エントリを作成します。スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピングされたこのアドレスは、DMZ ホストがサーバの実際のアドレスを知らなくても内部のサーバに対するアクセスに使用できるアドレスです。このコマンドは、DMZ アドレス 192.168.2.20 から実際の内部アドレス 172.20.1.5 にマッピングします。`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. ACL は、セキュリティ レベルの低いインターフェイスから、セキュリティ レベルの高いインターフェイスにアクセスするために必要です。この例では、DMZ 上にある Web サーバ（セキュリティ 50）から、内部にある AD/DNS サーバ（セキュリティ 100）に、特定のサービス ポート（DNS、Kerberos、LDAP）を使用してアクセスしています。`ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq domainASA-AIP-CLI(config)# access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq 389`**注：ACLは**、実際の内部アドレスではなく、この例で作成したAD/DNSサーバのマッピングされたアドレスへのアクセスを許可します。
3. この手順では、次のコマンドを使用して、ACL をインバウンド方向の DMZ インターフェイスに適用しています。`ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ`**注：ポート**88をブロックまたは無効にする場合、たとえばDMZから内部へのトラフィックは次のように使用します。

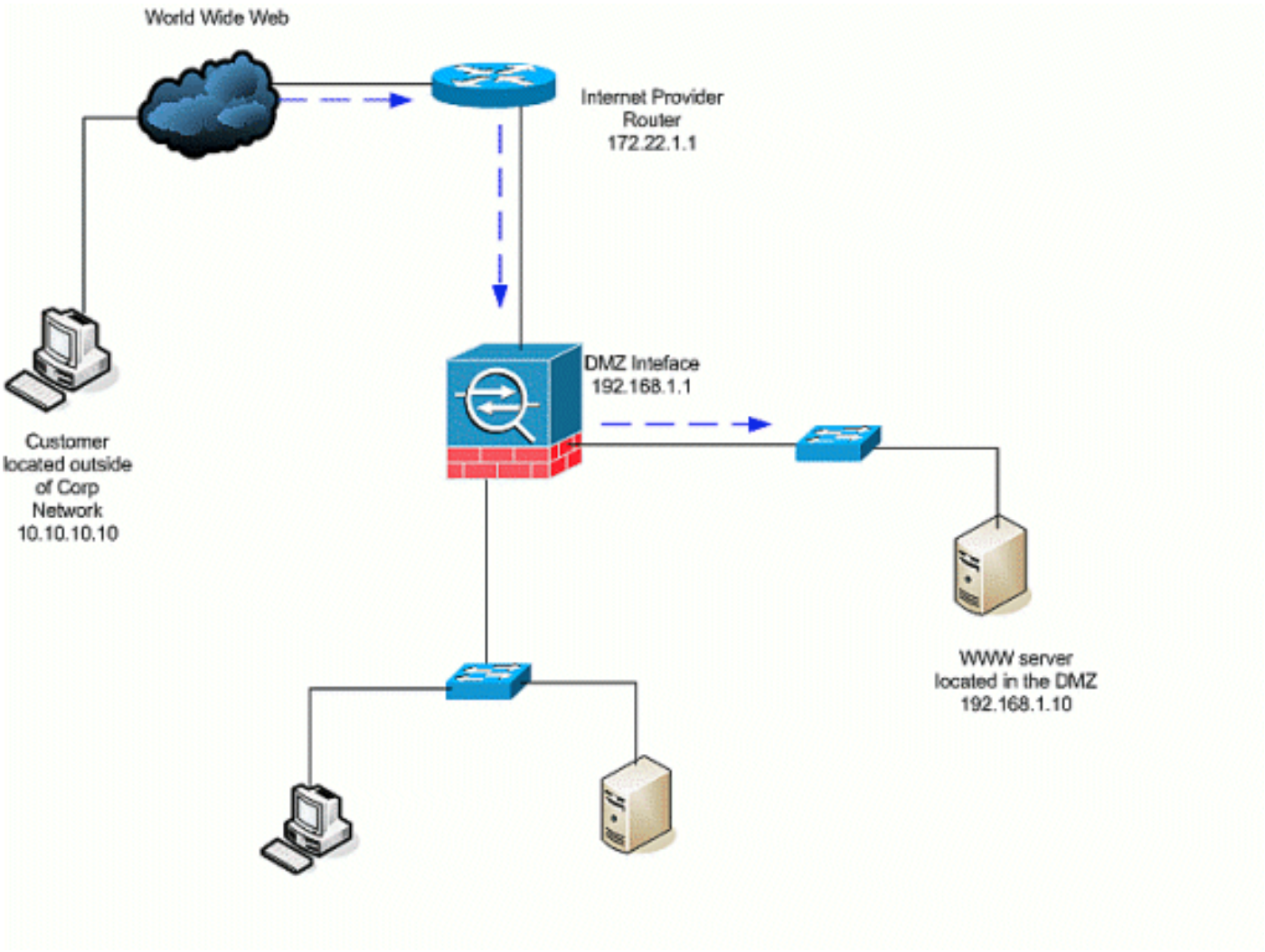
   ```
   ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
   tcp host 192.168.1.10 host 192.168.2.20 eq 88
   ```

   ヒント：NAT設定を変更する場合は、常に現在のNAT変換をクリアすることをお勧めします。変換テーブルのクリアは、**clear xlate** コマンドを使用して実行できます。**ただし、これを**

実行する場合は注意が必要です。なぜなら、変換テーブルをクリアすると、変換を使用する現在の接続がすべて切断されるからです。変換テーブルをクリアする代わりに、現在の変換がタイムアウトされるのを待機する方法がありますが、これは推奨できません。新たなルールで新しい接続が作成されると、予期せぬ動作が引きこされる可能性があります。その他の共通設定には、次のようなものがあります。DMZ のメール サーバ内部および外部の SSH アクセスPIX/ASA デバイス経由の許可されたリモート デスクトップDMZ で使用されるその他の DNS ソリューション

インターネットから DMZ へ

インターネット上のユーザや外部インターフェイス（セキュリティ 0）から DMZ にある Web サーバ（セキュリティ 50）への通信を可能にするには、次のコマンドを使用します。



1. DMZ の Web サーバから外部へのスタティック変換を作成します。スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピングされたこのアドレスは、インターネット上のホストがサーバの実際のアドレスを知らなくても DMZ 上の Web サーバに対するアクセスに使用できるアドレスです。このコマンドは、外部アドレスの 172.22.1.25 を実際の DMZ アドレス 192.168.1.10 にマッピングします。`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. ユーザがマッピング アドレスを通じて外部から Web サーバにアクセスできる ACL を作成します。Web サーバもまた、FTP をホストしている点に注意してください。`ASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`

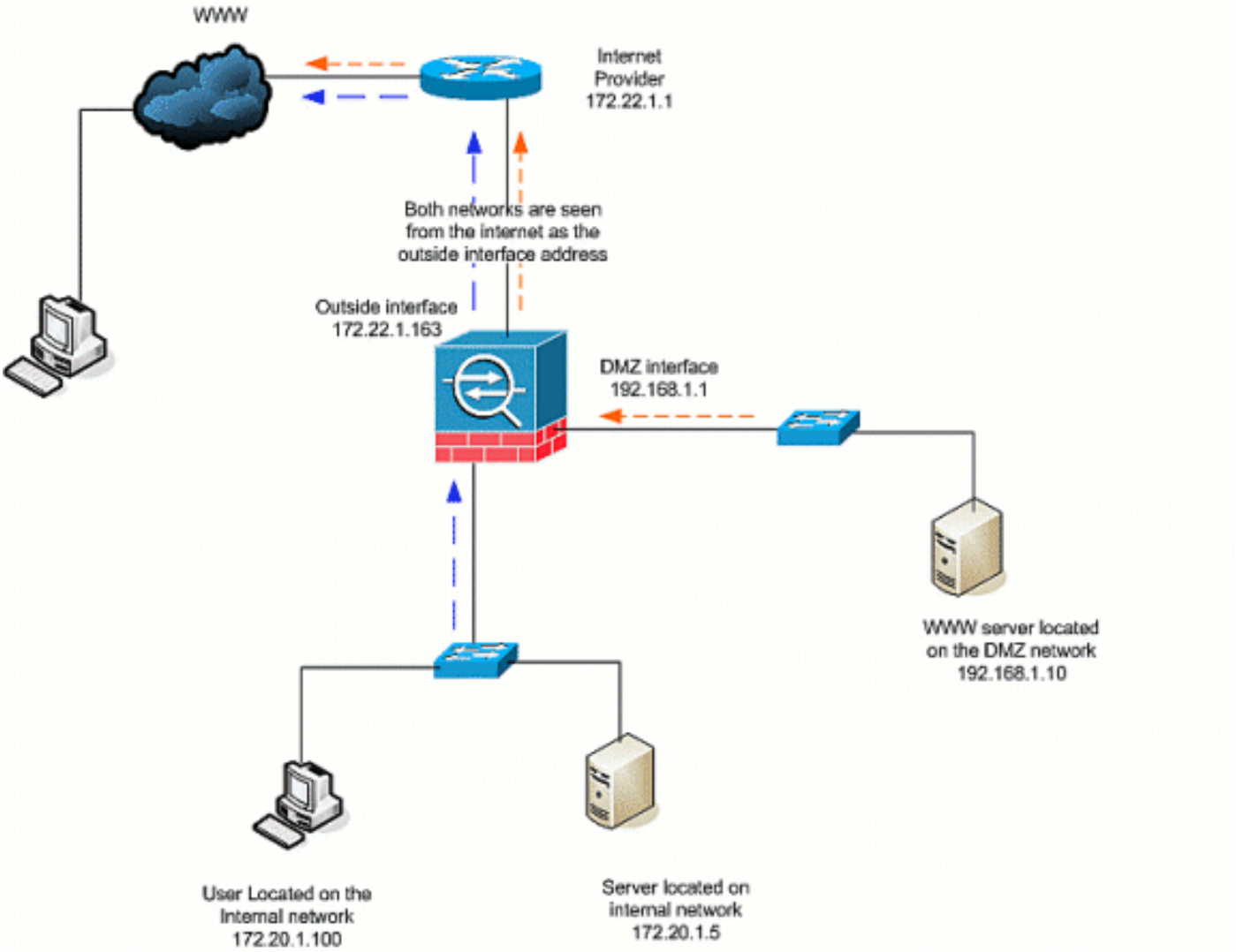
3. この設定の最後の手順は、ACL を外部インターフェイスに適用して、インバウンド方向のトラフィックを実現することです。`ASA-AIP-CLI(config)# access-group OutsidetoDMZ in interface Outside`**注：インターフェイス**ごとに、方向ごとに1つのアクセスリストしか適用できないことに注意してください。外部インターフェイスにすでにインバウンド ACL を設定している場合は、この例の ACL を適用できません。代わりに、インターフェイスに適用されている現在の ACL に、この例の ACE を追加してください。**注：インター**ネットからDMZへのFTPトラフィックをブロックまたは無効にする場合、たとえば次のコマンドを使用します。

```
ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
tcp any host 172.22.1.25 eq ftp
```

ヒント：NAT設定を変更する場合は、常に現在のNAT変換をクリアすることをお勧めします。変換テーブルのクリアは、**clear xlate** コマンドを使用して実行できます。**ただし、これを実行する場合は注意が必要です。**なぜなら、変換テーブルをクリアすると、変換を使用する現在の接続がすべて切断されるからです。変換テーブルをクリアする代わりに、現在の変換がタイムアウトされるのを待機する方法がありますが、これは推奨できません。新たなルールで新しい接続が作成されると、予期せぬ動作が引きこされる可能性があります。

内部/DMZ からインターネットへ

このシナリオでは、セキュリティ アプライアンスの内部インターフェイス (セキュリティ 100) にあるホストに対し、外部インターフェイス (セキュリティ 0) にあるインターネットへのアクセスが提供されます。 これは、PAT、NAT オーバーロード、ダイナミック NAT の形式で実現されます。他のシナリオとは異なり、ACL はこのケースでは不要です。なぜなら、セキュリティ レベルの高いインターフェイスのホストから、セキュリティ レベルの低いインターフェイスのホストにアクセスするためです。



1. 変換が必要なトラフィックのソースを指定します。ここで NAT ルール番号 1 が定義され、内部からの全トラフィックと DMZ ホストが許可されます。`ASA-AIP-CLI(config)# nat (inside) 1 172.20.1.0 255.255.255.0ASA-AIP-CLI(config)# nat (inside) 1 192.168.1.0 255.255.255.0`
2. NAT トラフィックが外部インターフェイスへのアクセス時に使用するアドレス、アドレス プール、インターフェイスを指定します。このケースでは、PAT が外部インターフェイス アドレスで実行されています。これは、DHCP 設定など、外部インターフェイス アドレスがあらかじめ分からない場合に特に便利です。ここでは、グローバル コマンドが同じ NAT ID の 1 で発行され、同一 ID の NAT ルールと結び付けられます。`ASA-AIP-CLI(config)# global (Outside) 1 interface`

ヒント：NAT設定を変更する場合は、常に現在のNAT変換をクリアすることをお勧めします。変換テーブルのクリアは、**clear xlate** コマンドを使用して実行できます。**ただし、これを実行する場合は注意が必要です。**なぜなら、変換テーブルをクリアすると、変換を使用する現在の接続がすべて切断されるからです。変換テーブルをクリアする代わりに、現在の変換がタイムアウトされるのを待機する方法がありますが、これは推奨できません。新たなルールで新しい接続が作成されると、予期せぬ動作が引きこされる可能性があります。

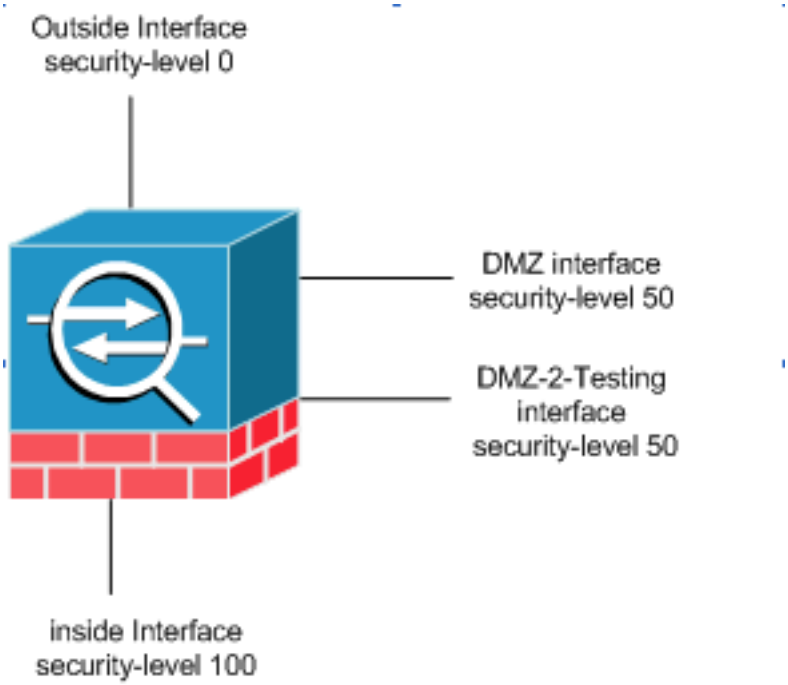
注：高いセキュリティゾーン（内部）から低いセキュリティゾーン（インターネット/DMZ）へのトラフィックをブロックする場合は、ACLを作成し、インバウンドとしてPIX/ASAの内部インターフェイスに適用します。

注： 例：インサイド ネットワークのホスト 172.20.1.100 からインターネットへのポート 80 トラフィックをブロックするには、次のコマンドを使用します。

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

同じセキュリティ レベルの通信

初期設定では、インターフェイスの「DMZ」と「DMZ-2-testing」が、セキュリティ レベル 50 に設定されています。デフォルトでは、この 2 つのインターフェイスは通信できません。このインターフェイスを通信できるようにするには、次のコマンドを使用します。




```
ASA-AIP-CLI(config)# same-security-traffic permit inter-interface
```

注：「same-security traffic permit inter-interface」が同じセキュリティレベルインターフェイス（「DMZ」と「DMZ-2-testing」）に設定されている場合でも、これらのインターフェイスに配置されたリソースにアクセスするには変換ルール（スタティック/ダイナミック）が必要です。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- PIX および ASA を経由した接続のトラブルシューティング
- NAT の検証とトラブルシューティングに関する NAT 設定

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
- テクニカル サポートとドキュメント – Cisco Systems