H3C SecPathファイアウォール製品

Comware 7トラブルシューティングガイド

文書バージョン:6W402-20220223

内容

適用可能なデバイスモデルおよびソフトウェアバージョン 6
序論 7
一般的なガイドライン 7
ログおよび動作情報の収集 8
一般的なログメッセージの収集 9
診断ログメッセージの収集 9
動作統計の収集 9
トラブルシューティング方法 10
トラブルシューティングフローチャート 10
障害タイプ 11
一般的なサービスリカバリーおよび障害除去方法 12
ハードウェアのトラブルシューティング 13
シャーシの障害 13
症状 13
ソリューション 13
ファントレイの障害 14
症状 14
ソリューション 14
温度アラーム 14
症状 14
ソリューション 14
関連コマンド 15
ソリューション 17
インターフェースが起動しない 18
症状 18
ソリューション 18
インターフェースがダウンした場合 19
症状 19
ソリューション 19
インターフェースステートフラッピング 20
症状 20
ソリューション 20
トランシーバーモジュール障害 20
症状 20
ソリューション 20
関連コマンド 23
パケット転送障害のトラブルシューティング 23
直接接続されたPCからのデバイスping障害 23
症状 23
ソリューション 23
デバイスを介して接続された2台のPC間の接続障害 24
症状 24
ソリューション 24
同じセキュリティゾーン内のデバイスを介して接続されているPC間の接続障害 25
症状 25
ソリューション 26
pingまたはtracert操作の失敗 26
症状 26
ソリューション 27
NATを介したping動作の失敗 28
症状 28
ソリューション 28

パケット損失 29
症状 29
ソリューション 29
関連コマンド 30
IRFのトラブルシューティング 31
IRFファブリック確立失敗 31
症状 31
ソリューション 31
IRF分割 33
症状 33
ソリューション 33
関連コマンド 34
ソリューション 35
RBMシステム分割 38
症状 38
ソリューション 38
ホットバックアップのトラブルシューティング 39
冗長グループに割り当てられていない場合、Rethインターフェースにpingできません。 39
症状 39
ソリューション 39
ポリシーNATのトラブルシューティング 41
内部ユーザーから外部ネットワークにアクセスできない 41
症状 41
ソリューション(セキュリティポリシー) 41
ソリューション(ポリシーベースNAT) 42
送信元アドレス変換エラー 42
症状 42
ソリューション(セキュリティポリシー) 43
ソリューション(ポリシーベースNAT) 43
宛先アドレス変換失敗 44
症状 44
ソリューション(セキュリティポリシー) 44
ソリューション(ポリシーベースNAT) 45
宛先アドレス変換失敗(宛先アドレス変換と統合されたソースアドレス変換) 45
症状 45
ソリューション(セキュリティポリシー) 45
ソリューション(ポリシーベースNAT) 46
IP Sec設定の失敗(IPsecと統合されたNAT) 46
症状 46
ソリューション 47
ポリシーベースNATで設定されたゲートウェイデバイスへの内部ユーザーからのアクセスの失敗 47
症状 47
ソリューション(セキュリティポリシー) 47
ソリューション(ポリシーベースNAT) 48
発信元アドレス変換が設定されたゲートウェイデバイスに外部ユーザーからアクセスできない 48
症状 48
ソリューション(セキュリティポリシー) 49
ソリューション(ポリシーベースNAT) 49
外部ユーザーから宛先アドレス変換が設定されたゲートウェイデバイスへのアクセスの失敗 49
症状 49
ソリューション(セキュリティポリシー) 50
ソリューション(ポリシーベースNAT) 50
インターフェースNATのトラブルシューティング 51
内部ユーザーから外部ネットワークにアクセスできない 51
症状 51

ソリューション(セキュリティポリシー)....51
ソリューション(インターフェースNAT)....52
送信元アドレス変換エラー....52
症状....52
ソリューション(セキュリティポリシー)....52
ソリューション(インターフェースNAT)....53
宛先アドレス変換エラー....53
症状....53
ソリューション(セキュリティポリシー)....54
ソリューション(インターフェースNAT)....54
宛先アドレス変換失敗(宛先アドレス変換と統合されたソースアドレス変換)....55
症状....55
ソリューション(セキュリティポリシー)....55
ソリューション(インターフェースNAT)....56
IP Sec設定の失敗(IPsecと統合されたNAT)....56
症状....56
ソリューション....56
発信元アドレス変換が設定されたゲートウェイデバイスに外部ユーザーからアクセスできない....57
症状....57
ソリューション(セキュリティポリシー)....57
ソリューション(ポリシーベースNAT)....57
外部ユーザーから宛先アドレス変換が設定されたゲートウェイデバイスへのアクセスの失敗....58
症状....58
ソリューション(セキュリティポリシー)....58
ソリューション(インターフェースNAT)....59
ダイナミックNATエラー....59
症状....59
ソリューション....59
NATは失敗するが、発信インターフェースは外部ネットワークから正常にpingを実行できる....60
症状....60
ソリューション....61
関連コマンド....61
IPsecとIKEのトラブルシューティング....62
IPsec SAは正常に確立されましたが、IPsecで保護されたトラフィックを転送できません....62
症状....62
ソリューション....62
IKE SAは正常に確立されましたが、IPsec SAを確立できません。....63
症状....63
ソリューション....63
関連コマンド....64
IKE SAを確立できない....64
症状....64
ソリューション....64
IP Secスマートリンクがリンク品質を検出しない....65
症状....65
ソリューション....67
IP Secトンネルインターフェースベースの IPsecトンネルを確立できない....68
症状....68
ソリューション....69
関連コマンド....69
ソリューション....70
不均等なロードバランシング....70
症状....70
ソリューション....70
システム管理のトラブルシューティング....71
CPU使用率が高い....71

症状 71
ソリューション 72
メモリ使用率が高い 74
症状 74
ソリューション 75
SSL VPNのトラブルシューティング 77
SSL VPN Webインターフェースへのログインの失敗 77
症状 77
ソリューション 77
ブラウザからSSL VPNゲートウェイへのログインの失敗 78
症状 78
ソリューション 78
ブラウザから内部リソースにアクセスできない 80
症状 80
ソリューション 80
INodeクライアントからSSL VPNゲートウェイ情報を取得できない 82
症状 82
ソリューション 82
INodeクライアントからSSL VPNゲートウェイにログインできない 84
症状 84
ソリューション 84
INodeクライアントから内部リソースにアクセスできない 86
症状 86
ソリューション 86
INodeクライアントユーザーのアイドルSSL VPNセッションの終了に失敗する 87
症状 87
ソリューション 87
ユーザーのフィルター、モニター、およびIPバインド設定が有効にならない 88
症状 88
ソリューション 88
SSL VPNゲートウェイへの再ログインの失敗 88
症状 88
ソリューション 88
WeChat Work(またはWeCom)認証の設定の失敗 89
症状 89
ソリューション 89
DPIのトラブルシューティング 90
IPSまたはアンチウイルスが誤って合法的なトラフィックを傍受 90
症状 90
ソリューション 91
IPSまたはWAFが攻撃トラフィックの捕捉や攻撃ログの生成に失敗する 92
症状 92
ソリューション 93
アプリケーションレート制限が有効にならない 97
症状 97
ソリューション 98
ファイルフィルタリングまたはデータフィルタリングが有効にならない 100
症状 100
ソリューション 101
関連コマンド 104
SSL復号化が有効にならない 104
症状 104
ソリューション 105
関連コマンド 110
アプリケーションの監査と管理が有効にならない 110
症状 110

ソリューション....111
関連コマンド....112
URLフィルタリングが有効にならない....112
症状....112
ソリューション....114
関連コマンド....115
サーバー接続検出が有効にならない....116
症状....116
ソリューション....116
関連コマンド....117
IPレピュテーションが有効にならない....117
症状....117
ソリューション....118
関連コマンド....119
データ分析センターがログの表示または更新に失敗する....119
症状....119
ソリューション....120
関連コマンド....121

適用可能なデバイスモデルおよびソフトウェアバージョン

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。このドキュメントに記載されている手順および情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

表1に、該当するデバイスモデルとソフトウェアバージョンを示します。

表1 該当するデバイスモデルおよびソフトウェアバージョン

デバイスモデル	ソフトウェアのバージョン
F5030-D、F5060-D、F5080-D、F5000-AK515、F5000-AK525	R9620
F5030、F5030-6GW、F5060、F5080、F5000-AI-40、F5000-V30、F5000-M、F5000-A、F5000-AI-20	R9628
F5010、F5020-GM、F5020、F5040、F5000-C、F5000-S	R9342
F1000-AI-20、F1000-AI-30、F1000-AI-50	R9345
F1000-AI-60、F1000-AI-70、F1000-AI-80、F1000-AI-90	R8601
F1005、F1010、F1003-L、F1005-L、F1010-L	R9536
F1020、F1020-GM、F1030、F1030-GM、F1070-GM-L、F1080、F1000-V70、F1050、F1060、F1070、F1070-GM	R9345
F1090、F1000-V90	R8601
F1000-AK1010、F1000-AK1020、F1000-AK1030	R9536
F1000-AK1110、F1000-AK1120、F1000-AK1130、F1000-AK1140	R9536
F1000-AK1212、F1000-AK1222、F1000-AK1232、F1000-AK1312、F1000-AK1322、F1000-AK1332	R9345
F1000-AK1414、F1000-AK1424、F1000-AK1434、F1000-AK1514、F1000-AK1524、F1000-AK1534、F1000-AK1614	R8601
F1000-AK108、F1000-AK109、F1000-AK110、F1000-AK115、F1000-AK120、F1000-AK125、F1000-AK710	R9536
F1000-AK130、F1000-AK135、F1000-AK140、F1000-AK145、F1000-AK150、F1000-AK155、F1000-AK160、F1000-AK165、F1000-AK170、F1000-AK175、F1000-AK180、F1000-AK185、F1000-AK711、F1000-GM-AK370、F1000-GM-AK380	R9345
F1000-E-G5、F1000-H-G5	R8601
F100-C-G5、F100-M-G5、F100-S-G5	R9345
F1000-A-G3、F1000-C-G3、F1000-E-G3、F1000-S-G3	R8601
F1000-9390-AI、F1000-9385-AI	R8601
F1000-990-AI、F1000-980-AI、F1000-970-AI、F1000-960-AI、F1000-950-AI、F1000-930-AI、F1000-920-AI	R9345
F1000-910-AI、F1000-905-AI	R9536
F1000-720-HI、F1000-710-HI	R9536

デバイスモデル	ソフトウェアのバージョン
F100-C-XI、F100-S-XI	R9536
F1000-E-G2、F1000-A-G2、F1000-S-G2、F1000-C-G2、F100-A-G2、F100-E-G2、F100-E-G2、F100-A-G3、F100-E-G3	R9345
F1000-C8180、F1000-C8170、F1000-C8160、F1000-E-VG	R9345
F1000-C-EI、F1000-C-HI、F100-A80-WiNet、F100-A-EI、F100-E-EI、F 100-A-HI、F100-A-SI	R9345
F1000-C8150、F1000-C8130、F1000-C8120、F1000-C8110、F1000-S-VG	R9536
F1000-C8395	R8601
F100-C-A6、F100-C-A5、F100-C-A3、F100-C-G3、F100-S-G3、F100-M-G3、F100-M-G2、F100-S-G2、F100-C-G2、F100-C-EI、F100-C-HI、F100-S-HI	R9536
F100-C80-WiNet、F100-C60-WiNet、F100-C50-WiNet、F100-S80-WiNet	R9536
F100-C-A6-WL、F100-C-A5-W、F100-C-A3-W	R9602
LSU3FWCEA0、LSUM1FWCEAB0、LSX1FWCEA1	R8239
LSPM6FWD	R8533
LSXM1FWDF1、LSUM1FWDEC0、IM-NGFWX-IV、LSQM1FWDSC0、LSWM1FWD0、LSQM2FWDSC0	R8534
LSPM6FWD8	R8535
LSQM2FWDSC8	R8520

序論

この文書では、ファイアウォールに関する一般的なソフトウェアおよびハードウェアの問題のトラブルシューティングについて説明します。

一般的なガイドライン

重要:

問題によって構成が失われないようにするには、システムが正常に動作しているときに機能の構成を終了するたびに構成を保存します。構成を回復するには、定期的に構成をリモートのサーバーにバックアップします。

ファイアウォールをトラブルシューティングする場合は、次の一般的なガイドラインに従ってください。

- 安全を確保するために、ハードウェアコンポーネントを交換または保守するときは、静電気防止用リストストラップを着用してください。
- 問題の原因を特定するために、次のようなシステムおよび構成情報を収集します。
  - 現象、障害発生時刻、および設定。
  - ネットワーク図、ポート接続、障害点などのネットワークトポロジ情報。
  - 構成変更の内容、ケーブル交換、リブートなどの手順を実行したときの動作を記録。
  - トラブルシューティングプロセス中に実行されたコマンドの出力。
  - ログメッセージと診断情報。

    - キャプチャされたパケットに関する情報、デバッグ情報、MPUまたはスイッチングファブリックモジュールの再起動の繰り返しに関する情報。
    - 故障の物理的証拠:
        - ハードウェアの写真。
        - カード、電源、およびファントレイのステータスLEDのステータス。
- トラブルシューティングプロセスでは、各設定または操作の影響を明確にし、設定または操作によって発生した問題が修正可能で、重大な結果を引き起こさないことを確認します。
- 各動作後、一定時間待って動作効果を確認してください。
- 設定の損失を防止するため、特にIRFスプリットが発生した場合は、トラブルシューティングプロセスで設定を保存しないでください。

ログおよび動作情報の収集

重要:

インフォメーションセンターはデフォルトで有効になっています。この機能が無効になっている場合はinfo-center enableコマンドを使用して、ログメッセージを収集する機能をイネーブルにします。

デバイスは、動作プロセス中に共通および診断ログメッセージと動作統計情報を生成します。

共通ログメッセージは、ログファイルに保存される前にログバッファに保存されます。システムは、指定された頻度でログファイルバッファの内容をログファイルに保存します。任意のビューでlogfile saveコマンドを実行して、ログファイルバッファの内容をただちにログファイルに保存することもできます。

これらのログファイルは、デバイスのフラッシュまたはCFカードに保存されます。これらのファイルは、FTPまたはTFTPを使用してエクスポートできます。

表2 ログおよび動作情報

カテゴリ	ファイル名の形式	内容
共通ログ	**logfile**X.**log**	コマンド実行、トラップ、および操作ログメッセージ。
診断ログ	**diagfile**X.**log**	デバイスオペレーションに関する診断ログメッセージ。次の項目が含まれます。 • エラー発生時に有効なパラメータ設定です。 • カード起動エラーに関する情報。 • 通信異常時のMPUとインターフェースカード間のハンドシェイク情報
動作統計	*basename.**gz**ファイル*	デバイスステータス、CPUステータス、メモリステータス、コンフィギュレーション、ソフトウェアエントリ、およびハードウェアエントリ

一般的なログメッセージの収集

1. 共通ログメッセージをログバッファからログファイルに保存するには、logfile saveコマンドを使用します。

   [H3C] logfile save

   ログファイルバッファの内容は、flash:/logfile/logfile.logファイルに保存されています。

2. ログファイルに関する情報を確認します。

   <H3C> dir flash:/logfile/

   Directory of flash:/logfile

   0 -rw- 10483632 Jul 08 2014 15:05:22 logfile.log

   253156 KB total (77596 KB free)

診断ログメッセージの収集

1. diagnostic-logfile saveコマンドを使用して、診断ログバッファから診断ログファイルに診断ログメッセージを保存します。

   <H3C>diagnostic-logfile save

   The contents in the diagnostic log file buffer have been saved to the file flash:/diagfile/diagfile.log.

2. 診断ログファイルに関する情報を確認します。

   <H3C>dir flash:/diagfile/

   Directory of flash:/diagfile

   0 -rw- 10485740 Nov 04 2020 17:51:52 diagfile.log

   7456492 KB total (6624504 KB free)

動作統計の収集

診断情報を表示または保存するには、display diagnostic-informationコマンドを使用します。

#オペレーティング統計を保存するには、display diagnostic-informationコマンドを実行し、診断情報を保存または表示するように指示されたときにYを入力して診断情報を保存します。診断情報を表示するためにNを入力すると、情報が完全に収集されない場合があります。

<H3C> display diagnostic-information

Save or display diagnostic information (Y=save, N=display)? [Y/N]:y

Please input the file name(*.gz) [flash:/diag.gz] :flash:/diag.gz

Diagnostic information is outputting to flash:/diag.gz.

Save successfully.

<H3C> dir flash:/

Directory of flash:

.....

6 -rw- 898180 Jun 26 2013 09:23:51 diag.gz

1021808 KB total (259072 KB free)

診断情報を表示するには、display diagnostic-information コマンドを実行する前に、screen-length disable コマンドを実行して、出力の画面間の一時停止を無効にします。

```
<H3C> screen-length disable
% Screen-length configuration is disabled for current user.
<H3C> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:N
================================================================
  ===============display cpu===============
Slot 1 CPU 0 CPU usage:
          6% in   last    5  seconds
          6% in   last    1  minute
          6% in   last    5  minutes

============================================================
================================================================
  ===============display cpu-usage history slot 1 =============== 100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|############################################################
    ------------------------------------------------------------------------------------------------------------------------
                  10          20          30          40          50          60   (minutes)
                                cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
……
```

トラブルシューティング方法

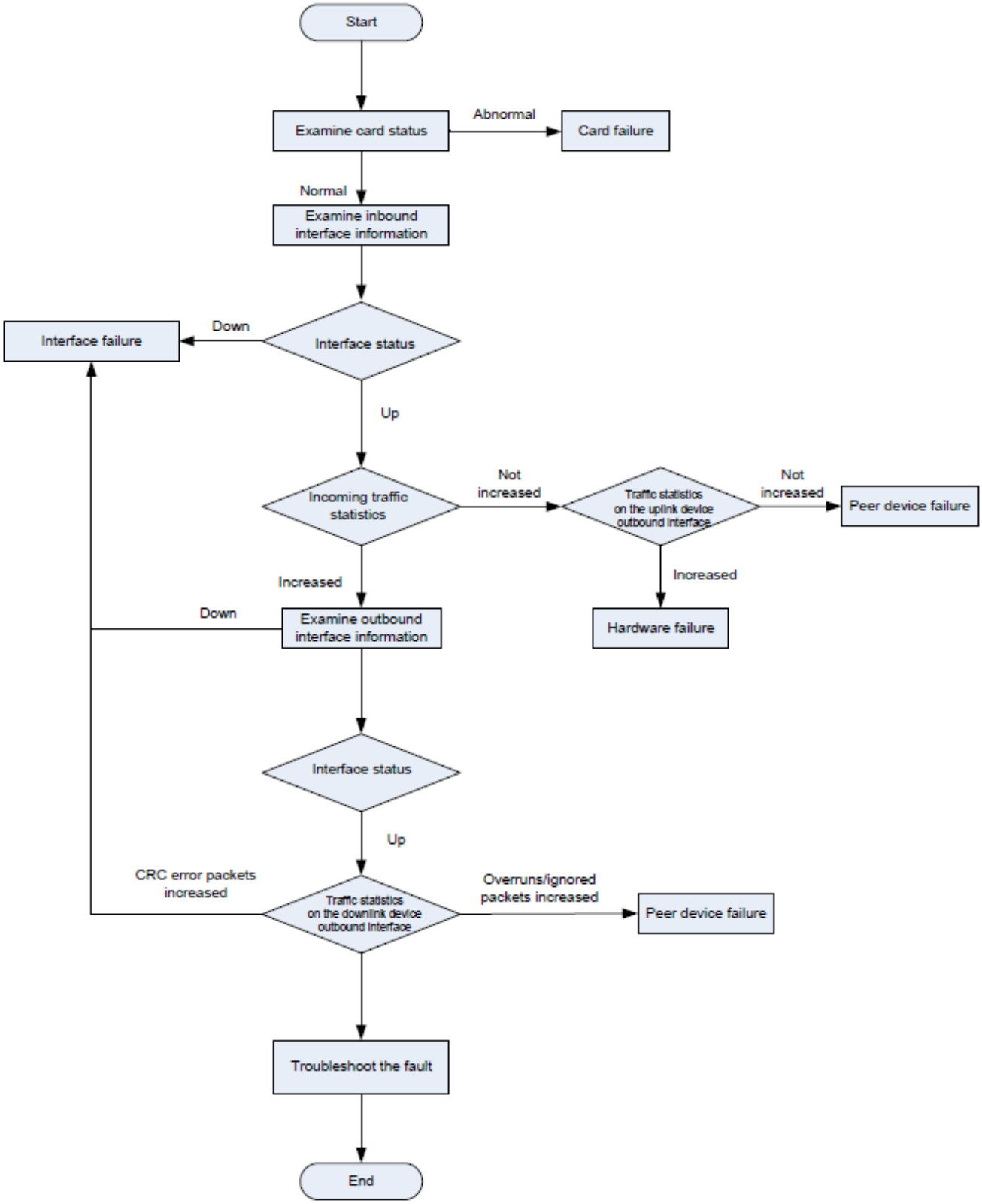
障害が発生した場合は、まず関連するシステム、構成、動作情報を収集して障害タイプを特定し、その障害タイプのトラブルシューティング方法に従って障害を解決します。

障害を特定できない場合は、収集した情報とともに障害の説明をテクニカルサポートに提供して分析を依頼します。

トラブルシューティングフローチャート

図1は、障害タイプを特定するための一般的なトラブルシューティングプロセスを示しています。

図1 トラブルシューティングのフローチャート



障害タイプ

デバイスでは、次のタイプの障害が発生する可能性があります。

- **シャーシ障害**: 予期しない再起動、異常な状態、起動の失敗、または再起動の繰り返し。トラブル

シューティング手順については、「ハードウェアのトラブルシューティング」の「シャーシの障害」を参照してください。

- **温度アラーム**: トラブルシューティング手順については、「ハードウェアのトラブルシューティング」の「温度アラーム」を参照してください。
- **インターフェース障害**: インターフェースがアップに失敗した場合、アップステートとダウンステートの間でフラップが発生した場合、またはエラーパケットが発生した場合は、トラブルシューティング手順について「インターフェースのトラブルシューティング」を参照してください。
- **IRF障害**: デバイスがIRFを形成できない場合、またはIRFスプリットが発生した場合のトラブルシューティング手順については、「IRFのトラブルシューティング」を参照してください。
- **ホットバックアップ障害**: マスター/下位スイッチオーバー、冗長ポート経由の転送、または冗長ポートへのサービススイッチング中に例外が発生した場合は、トラブルシューティング手順について「ホットバックアップのトラブルシューティング」を参照してください。
- **ロードバランシングの失敗**: トラブルシューティング手順については、「ロードバランシングのトラブルシューティング」を参照してください。
- **高CPU使用率**: トラブルシューティング手順については、「システム管理のトラブルシューティング」の「CPU高使用率」を参照してください。
- **メモリ使用率が高い**: トラブルシューティング手順については、「システム管理のトラブルシューティング」の「メモリ使用率が高い」を参照してください。

一般的なサービスリカバリーおよび障害除去方法

表3一般的な電力および空調設備の方法

障害カテゴリ	サービスの回復方法	障害の除去方法
ハードウェア	• 問題のあるカードを特定します。 • トラフィック転送パスを調整して、障害のあるデバイスを特定します。たとえば、トラフィックが他のパスに切り替えられるようにルートのプリファレンスを変更します。	バックアップハードウェアで必要なテストを完了し、障害が発生したハードウェアを交換します。
ソフトウェア	• 障害のあるデバイスでプロトコルを再度イネーブルにします。 • トラフィック転送パスを調整して、障害のあるデバイスを特定します。	ソフトウェアバージョン(パッチバージョンを含む)をアップグレードします。 ネットワークトポロジを調整するか、設定を変更して障害を除去します。
リンク	トラフィック転送パスを調整して、障害のあるリンクを分離します。	障害のあるケーブルを交換します。
その他	• 設定エラーを修正します。 • デバイスのポートを正しく接続してください。 • トラフィック転送パスを調整して、障害のあるリンクを分離します。	• 正しくない設定を修正してください。 • デバイスポートを正しく接続してください。 • デバイスの電源およびエアコンシステムを修理します。

ハードウェアのトラブルシューティング

シャーシの障害

症状

シャーシが予期せずリブートする。

ソリューション

この問題を解決するには、次の手順に従います

display versionコマンドを実行し、最後のreboot reasonフィールドをチェックして、シャーシのリブートの原因を特定します。

シャーシの再起動の原因がソフトウェアの異常である場合は、診断情報を収集してH3Cサポートに送信します。

<H3C>display version
H3C Comware Software, Version 7.1.064, Ess 8601P08
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved. H3C SecPath F1090
uptime is 0 weeks, 0 days, 0 hours, 5 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-E8601P08.bin Boot
image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-E8601P08.bin System
image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00

SLOT 1
CPU type: Multi-core CPU
DDR4 SDRAM Memory: 8192M
bytes FLASH: 7296M bytes
CPLD_A Version: 1.0
CPLD_B Version: 1.0
Release Version:SecPath F1090-8601P08
Basic BootWare Version:0.30
Extend BootWare Version:1.01
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.A
HD_BackBoard Version:Ver.D Pcb
Version:Ver.A
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.A, (Driver)1.0, (Cpld)1.0
Boot Type: Warm

ファントレイの障害

症状

ファントレイステータスLEDは、異常な状態が存在することを示します。デバイスは、ファントレイの障害に関するメッセージを次のように出力します。

%May 06 10:12:24:805 2017 H3C DEV/3/FAN_ABSENT: -MDC=1; Slot 2 Fan 2 is absent.

%May0610:12:32:8052017H3CDEVD/2/DRV_DEV_FAN_CHANGE:-MDC=1; Slot2:Fancommunication state changed: Fan 1 changed to fault.

%May 06 10:12:42:405 2017 H3C DEV/2/FAN_FAILED: -MDC=1; Slot 2 Fan 1 failed.

ソリューション

この問題を解決するには、次の手順に従います

1. ファントレイがスロットにある場合は、デバイスの排気口に手を置いて、デバイスから風が吹き出していることを確認します。

   デバイスから風が吹き出していない場合は、ファントレイに障害があります。
2. 吸気口と排気口がふさがれていないこと、および吸気口と排気口に大量のほこりが堆積していないことを確認します。
3. ファントレイが、正常な動作状態および正常なファン速度でスロットに取り付けられていることを確認します。

   ファントレイの動作ステータス情報を表示するには、display fanコマンドを実行します。ファンのステータスが正常でない場合、または表示されるファン速度が正常なファン速度の半分未満の場合は、ファントレイを取り外して再取り付けするか、ファントレイを別のファントレイとスワップして、障害の理由を確認できます。

   SLOT 1 Fan 0 Status: Normal Speed:9500 SLOT 1

   Fan 1 Status: Normal Speed:9500 SLOT 1 Fan 2

   Status: Normal Speed:9500
4. 問題が解決しない場合は、ファントレイを交換してください。

   ファントレイがない場合は、デバイスの電源をオフにして、高温によるモジュールの損傷を防止します。デバイスの動作温度を50°C(122°F)未満に保つための冷却手段を使用できる場合は、デバイスの使用を継続できます。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

温度アラーム

症状

デバイスは、次のような高温または低温アラームメッセージを出力します。

%Mar 18 04:22:05:893 2017 H3C DEV/4/TEMPERATURE_WARNING: -Context=1; Temperature is greater than the high-temperature warning threshold on slot 2 sensor inflow 1. Current temperature is 43 degrees centigrade.

ソリューション

この問題を解決するには、次の手順に従います

1. 周囲温度が正常であることを確認します。

   周囲温度が高い場合は、機器室の換気不良やエアコンの故障など、高温の原因を確認してください。

2. デバイスの温度が警告またはアラームのしきい値の上限または下限を超えていないことを確認します。

   表示環境コマンドを実行して、モジュール温度を確認したり、手でモジュールに触れることができます。モジュール温度が高い場合は、モジュールの長時間の高温によるモジュール損傷を防止するため、高温の原因を早急に調査してください。

   温度フィールドにエラーまたは通常と異なる値が表示される場合、スイッチはI2Cバスを介してカード温度センサーにアクセスできない可能性があります。スイッチは同じI2Cバスを介してトランシーバーモジュールにアクセスします。トランシーバーモジュール情報が正しく表示されているかどうかを確認できます。スイッチがトランシーバーモジュールにアクセスできる場合はtemperature-limitコマンドを使用して温度しきい値を再設定します。次にdisplay environmentコマンドを使用して、設定が有効かどうかを確認します。

   [H3C] temperature-limit slot 1 inflow 1 -5 65 76

   [H3C] display environment

Slot	Sensor	Temperature	LowerLimit	WarningLimit	AlarmLimit
0/1	Inflow 1	30	10	65	76
0/1	Outflow 1	33	-5	66	76
0/1	Outflow 2	37	-5	66	76
0/1	Hotspot 1	39	-5	66	76
0/1	Hotspot 2	42	-5	66	76
0/1	Hotspot 3	44	-5	66	76

   それでも温度アラームの原因を見つけることができない場合は、温度アラームログと温度情報を入手し、それらをH3Cサポートに送ってヘルプを求めてください。

関連コマンド

コマンド	説明
Display device	デバイス情報を表示します。
Display environment	温度情報を表示します。
Display power	次のような電源情報を表示します。 • パワーサプライのステータス。 • 電源タイプ、定格入力電圧、定格出力電圧です。 • 使用可能なパワーサプライの数、パワーサプライの使用可能な合計電力、使用電力の合計、および冗長電源。 • 取り付けられているパワーサプライのステータス。 • カードの電源ステータス。
Display version	システムバージョン情報、モジュールのアップタイム、および最後のリブート理由を表示します。
save	現在のコンフィグをコンフィグファイルに保存します。
temperature-limit	温度アラームしきい値を設定します。

インターフェースのトラブルシューティング

インターフェース上のエラーパケット

症状

display interfaceコマンドの出力は、インターフェースにエラーパケットが存在することを示しています。

<H3C>display interface GigabitEthernet 1/0/2

GigabitEthernet1/0/2
Current state: DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/2 Interface Maximum
transmission unit: 1500
Internet address: 192.168.2.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 50da-00dd-1327 IPv6 packet frame
type: Ethernet II, hardware address: 50da-00dd-1327 Media type is twisted pair, loopback
not set, promiscuous mode not set Speed Negotiation, Duplex Negotiation, link type is
autonegotiation Output flow-control is disabled, input flow-control is disabled
Last link flapping: Never
Last clearing of counters: Never
Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
Last 300 second input: 0 packets/sec 0 bytes/sec -%
Last 300 second output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses Input (normal): 0
packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses Input: 0 input
errors, 0 runts, 0 giants, - throttles
0 CRC, 0 frame, 0 overruns, 0 aborts
0 ignored, - parity errors Output
(total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses Output (normal): 0
packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses Output: 0 output
errors, 0 underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lost carrier, 0 no carrier

着信エラーパケット用のフィールド

- **input errors**: 着信エラーパケットの総数。
- **runts**: 次の条件を満たす着信フレームの数。
  - 64バイトより短い。

    - 正しい形式で。
    - 有効なCRCを含む。
- **giants**: 受信したジャンボフレームの数。ジャンボフレームとは、インターフェースでサポートされている最大フレーム長より大きいフレームを指します。ジャンボフレームを許可しないイーサネットインターフェースの場合、最大フレーム長は1518バイト(VLANタグなし)または1522バイト(VLANタグあり)です。ジャンボフレームを許可するイーサネットインターフェースの場合、インターフェースでジャンボフレームサポートを設定すると、イーサネットフレームの最大長が設定されます。
- **throttles**: バイト数が整数以外の着信フレームの数。
- **CRC**: 長さは正常であったがCRCエラーが含まれていた着信フレームの総数。
- **frame**: CRCエラーおよび非整数バイトを含む着信フレームの合計数。
- **overruns**: ポートの入力レートがキューイング機能を超えたためにドロップされたパケットの数。
- **aborts**: 不正な着信パケットの総数(フラグメントフレーム、ジャバーフレーム、シンボルエラーフレーム、未知の演算コードフレーム、長さエラーフレームなど)。
- **ignored**: ポートの受信バッファが不足したためにドロップされた着信フレームの数。
- **parity errors**: パリティエラーが発生したフレームの合計数。

発信エラーパケット用のフィールド

- **output errors**: エラーのある発信パケットの合計数。
- **underruns**: インターフェースの出力レートが出力キューイング機能を超えたためにドロップされたパケットの数。これは、可能性の低いハードウェアの異常です。
- **buffer failures**: インターフェースの送信バッファが不足したためにドロップされたパケットの数。
- **aborts**: 送信に失敗したパケットの数。これらのパケットの送信は開始されましたが、さまざまな理由(衝突など)により失敗しました。
- **deferred**: 衝突が検出されたためにインターフェースが送信を延期したフレームの数。
- **collisions**: 送信中にコリジョンが検出されたために、インターフェースが送信を停止したフレーム数。
- **late collisions**: 検出されたコリジョンのために、最初の512ビットを送信した後、インターフェースが送信を延期したフレームの数。
- **lost carrier**: 伝送中に失われたキャリア数。このカウンタは、キャリアが失われると1増加し、シリアルWANインターフェースに適用されます。
- **no carrier**: ポートがフレームの送信時にキャリアの検出に失敗した回数。このカウンタは、ポートがキャリアの検出に失敗した場合に1ずつ増加し、シリアルWANインターフェースに適用されます。

ソリューション

この問題を解決するには、現象に応じて次のいずれかの解決策を選択します。

- インバウンド方向のCRC、フレーム、およびスロットルエラーを増加させるソリューション
- インバウンド方向のジャンボフレームを通すためのソリューション
- アウトバウンド方向でエラーパケットが増加しているときの解決策

インバウンド方向のCRC、フレーム、およびスロットルエラーを増加させるソリューション

1. リンクのパフォーマンスをテストします。リンクの品質が低いか、光信号が大幅に減衰している場合は、ケーブルまたは光ファイバを交換してください。
2. インターフェースにトランシーバーモジュールが取り付けられている場合は、「トランシーバーモジュールの障害」の説明に従って、問題の原因がトランシーバーモジュールの障害であるかどうか

を確認します。

3. ケーブル、光ファイバ、またはトランシーバーモジュールを、正常に動作しているインターフェースのモジュールとスワップしてから、スワップします。
   - 問題が元のインターフェースでは同じままで、新しいインターフェースでは発生しない場合は、元のインターフェースが障害の原因である可能性があります。正しく動作するインターフェースを使用してサービスを提供し、障害情報を分析のためにH3Cサポートに送信してください。
   - 問題が元のインターフェースではなく、新しいインターフェースで発生する場合は、ピアデバイスと中間デバイスおよびリンクが正しく動作していることを確認します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

インバウンド方向のジャンボフレームを通すためのソリューション

1. 両端のインターフェースに対するjumboframe enableコマンドの次の設定を確認します。
   - ジャンボフレーム機能が両方のインターフェースでイネーブルになっていることを確認します。
   - コマンドのデフォルト設定が同じであることを確認します。
   - コマンドの現在の設定が同じであることを確認します。
2. 問題が解決しない場合は、H3Cサポートに連絡してください。

アウトバウンド方向でエラーパケットを増加させるための解決策

1. インターフェースが全二重モードで動作していることを確認します。
2. 問題が解決しない場合は、H3Cサポートに連絡してください。

インターフェースが起動しない

症状

インターフェースがアップ状態にならない。

ソリューション

この問題を解決するには、次の手順に従います

1. インターフェースおよびそのピアインターフェースに接続されているケーブルまたは光ファイバが正しく確実に接続されていることを確認します。
2. 問題が解決しない場合は、ケーブルまたは光ファイバを正常に動作するケーブルまたは光ファイバと交換して、中間リンクが正常に動作していることを確認します。
3. アップ/ダウン状態、デュプレックスモード、速度、自動ネゴシエーションモード、MDIなどのインターフェースの設定を調べます。インターフェースが正しく設定されていることを確認します。

表4 デュプレックスモードのサポート

速度 デュプレックス	10G	1000M	100M	10M
Full	サポートされていません	サポート対象	サポート対象	サポート対象
half	サポートされていません	サポートされていません	サポート対象	サポート対象

4. インターフェースにトランシーバーモジュールが搭載されている場合は、トランシーバーモジュールが同じタイプ(速度、波長、シングルモード、マルチモードなど)であることを確認します。
5. 問題が解決しない場合は、疑わしいトランシーバーモジュールを正常に動作するトランシーバーモジュールとスワップします。「トランシーバーモジュールの障害」の説明に従って、問題の原因がトランシーバーモジュールの障害であるかどうかを確認します。

```
<H3C> display transceiver interface GigabitEthernet 1/0/17

GigabitEthernet1/0/17 transceiver information:
Transceiver Type                 : 1000_BASE_SX_SFP
Connector Type                   : LC
Wavelength(nm)                   : 850
Transfer Distance(m)             :550(OM2),270(OM1)
Digital Diagnostic Monitoring    : YES
Vendor Name                      : JDSU
```

6. トランシーバーモジュールが故障している場合は、トランシーバーモジュールを交換し、H3Cサポートに連絡してください。

インターフェースがダウンした場合

症状

インターフェースがダウンした。

ソリューション

この問題を解決するには、次の手順に従います

1. ローカルデバイスおよびピアデバイスのログメッセージを確認します。インターフェースが手動でシャットダウンされたかどうかを確認します。
2. インターフェースステータス情報を表示します。インターフェースにプロトコルの問題があるかどうか、またはエラーのために診断モジュールによってシャットダウンされたかどうかを識別します。問題がある場合は、H3Cサポートに連絡してください。

```
<H3C> display interface GigabitEthernet 1/0/2

GigabitEthernet1/0/2
Current state: DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/4/0/1 Interface Bandwidth:
1000000kbps
Maximum Transmit Unit: 1500
Internet protocol processing: disabled
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0004-5601 IPv6 Packet
Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0004-5601 Media type is not
sure,Port hardware type is No connector
Last clearing of counters: 16:45:01 Wed 12/11/2013
Peak value of input: 0 bytes/sec, at 2013-12-11 16:45:03
Peak value of output: 0 bytes/sec, at 2013-12-11 16:45:03
Last 300 second input:  0 packets/sec 0 bytes/sec
Last 300 second output:  0 packets/sec 0 bytes/sec
```

3. 「インターフェースが起動しない」で説明されているように、インターフェースが正しく設定され、ケーブル、トランシーバーモジュール、および光ファイバが正しく動作していることを確認します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

インターフェースステートフラッピング

症状

インターフェースはアップステートとダウンステートの間でフラップします。

ソリューション

この問題を解決するには、次の手順に従います

1. インターフェースがファイバポートの場合は、「トランシーバーモジュールの障害」の説明に従って、両端のトランシーバーモジュールが正常に動作していることを確認します。
2. インターフェースが銅線ポートの場合は、速度とデュプレックスモードを設定します。状態フラッピングの問題は通常、自動ネゴシエーションモードで発生します。自動ネゴシエーションモードをディセーブルにして、両端の両方のインターフェースに同じ速度とデュプレックスモードを設定します。
3. 問題が解決しない場合は、H3Cサポートに連絡してください。

トランシーバーモジュール障害

症状

トランシーバーモジュールが取り付けられているファイバポートが正しく動作しません。

ソリューション

この問題を解決するには、次の手順に従います

1. インターフェースが10-GEファイバポートの場合は、ファイバポートでサポートされていないギガビットトランシーバーモジュールがファイバポートに取り付けられているかどうかを確認します。取り付けられている場合は、トランシーバーモジュールをサポートされているモデルのいずれかに交換します。
2. display transceiver alarm interfaceコマンドを実行して、トランシーバーモジュールに存在するアラームを調べます。
   - 入力エラーが発生した場合は、ピアポート、ファイバ、および中継デバイスが正しく動作していることを確認します。
   - 出力エラー、電流エラー、または電圧エラーが発生した場合は、ローカルポートが正しく動作していることを確認します。

   <H3C> display transceiver alarm interface Ten-GigabitEthernet 1/0/25

   Ten-GigabitEthernet1/0/25 transceiver current alarm information:

   RX signal loss

表5 トランシーバーモジュールのアラーム

フィールド	説明
SFP/SFP+	
RX loss of signal	着信(Rx)信号が失われた。
RX power high	受信(Rx)電力が高い。
RX power low	受信(Rx)電力が低い。
TX fault	送信障害。
TX bias high	Txバイアス電流は大きい。
TX bias low	Txバイアス電流は低い。
TX power high	Txパワーが高い。
TX power low	Tx電力が低い。
Temp high	温度が高い。
Temp low	温度が低い。
Voltage high	電圧が高い。
Voltage low	電圧が低い。
Transceiver info I/O error	トランシーバー情報の読み取りおよび書き込みエラーです。
Transceiver info checksum error	トランシーバー情報チェックサムエラーです。
Transceiver type and port configuration mismatch	トランシーバータイプがポート設定と一致しません。
Transceiver type not supported by port hardware	ポートはトランシーバー タイプをサポートしていません。
XFP	
RX loss of signal	着信(Rx)信号が失われた。
RX not ready	受信機の準備ができていません。
RX CDR loss of lock	Rxクロックを回復できません。
RX power high	Rxパワーが高い。
RX power low	Rxパワーが低い。
TX not ready	Txの準備ができていません。
TX fault	Tx障害。
TX CDR loss of lock	Txクロックを回復できません。
TX bias high	Txバイアス電流は大きい。
TX bias low	Txバイアス電流は低い。
TX power high	Txパワーが高い。
TX power low	Tx電力が低い。
Module not ready	モジュールの準備ができていません。
APD supply fault	APD電源障害。
TEC fault	TEC障害。
Wavelength unlocked	光信号の波長がメーカーの許容範囲を超えています。
Temp high	温度が高い。
Temp low	温度が低い。
Voltage high	電圧が高い。
Voltage low	電圧が低い。

Transceiver info I/O error	トランシーバー情報の読み取りおよび書き込みエラー。
Transceiver info checksum error	トランシーバー情報のチェックサム エラー。
Transceiver type and port configuration mismatch	トランシーバーのタイプがポート構成と一致しません。
Transceiver type not supported by port hardware	トランシーバー タイプがポートでサポートされていません。

3. 問題のあるトランシーバーモジュールと正常に動作するトランシーバーモジュールをスワップし、インターフェースをスワップします。
4. トランシーバーモジュールに障害が発生していることが確実な場合は、display transceiver diagnosisコマンドを実行して、トランシーバーモジュールのデジタル診断パラメータの現在の値を収集し、H3Cサポートに送信します。display transceiver diagnosisコマンドはH3Cトランシーバーモジュールに適用されるため、非H3Cトランシーバーモジュールに関する情報を表示できない場合があります。

   <H3C>display transceiver diagnosis interface GigabitEthernet 1/0/17

   GigabitEthernet1/0/17 transceiver diagnostic information:

   Current diagnostic parameters:

   Temp.(°C) Voltage(V) Bias(mA) RX power(dBm) TX power(dBm) 54 3.35

   5.39 -5.91 -5.29

   Alarm thresholds:

   Temp.(°C) Voltage(V) Bias(mA) RX power(dBm) TX power(dBm) High 73 3.80

   11.00 0.00 0.00

   Low -3 2.81 1.00 -16.99 -12.52

   <H3C>
5. トランシーバー モジュールの電子ラベル情報を表示します。**Vendor Name** フィールドには、H3C トランシーバー モジュールの **H3C** が表示されます。ベスト プラクティスとして、H3C トランシーバー モジュールのみを使用してください。

   <H3C>display transceiver manuinfo interface GigabitEthernet1/0/16

   transceiver manufacture information: The transceiver is absent.

   GigabitEthernet1/0/17 transceiver manufacture information: The transceiver does not support this function.

   GigabitEthernet1/0/18 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet1/0/19 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet1/0/20 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet1/0/21 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet1/0/22 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet1/0/23 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/16 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/17 transceiver manufacture information: The transceiver does not support this function.

   GigabitEthernet2/0/18 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/19 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/20 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/21 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/22 transceiver manufacture information: The transceiver is absent.

   GigabitEthernet2/0/23 transceiver manufacture information: The transceiver is absent.
6. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

ここでは、インターフェースのトラブルシューティングに使用できるコマンドを示します。

コマンド	説明
display current-configuration	実行コンフィギュレーションを表示します。特定のインターフェースの実行コンフィギュレーションを表示できます。
display interface	インターフェースステータス、着信および発信トラフィック統計情報などのインターフェース情報を表示します。
display transceiver alarm	トランシーバーラームを表示します。
Display transceiver diagnosis	トランシーバーモジュールのデジタル診断パラメータの現在の値(温度、電圧、バイアス電流、入力電力、出力電力など)を表示します。
display transceiver interface	トランシーバーモジュールの主要なパラメータを表示します。
display transceiver manuinfo	トランシーバーモジュールの電子ラベル情報を表示して、トランシーバーモジュールのベンダーを識別します。

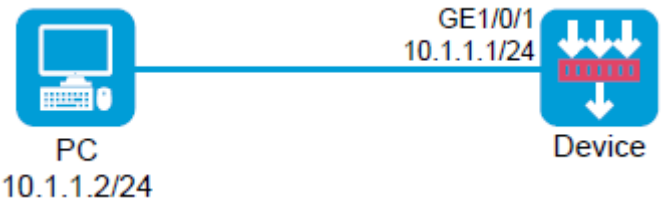
パケット転送障害のトラブルシューティング

直接接続されたPCからのデバイスping障害

症状

PCは、ネットワークケーブルを介してデバイスのサービスインターフェースに接続され、デバイスと同じサブネット内にあります。ただし、PCからデバイスへのpingは成功しません。

図2ネットワーク図



ソリューション

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Network > Security Zones** ページにアクセスします。
3. ターゲットセキュリティゾーンの**Edit**アイコンをクリックします。
4. デバイスをPCに接続するインターフェースをメンバーインターフェースとして追加します。
5. **OK**をクリックします。
6. **Policies > Security Policies**ページにアクセスします。

7. **Security Policies**タブで、**Create**をクリックし、**Create a Policy**をクリックします。
8. 必要に応じて、ポリシーパラメータを設定します。
   - **Source zone**: インターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Name**: ポリシー名を指定します。この例では、名前は**trust-local**です。
   - **Destination Zone**: Destination ZoneとしてLocalを選択します。
   - **Action**: アクションとして**Permit**を選択します。
   - **Source IPv4 address**: 送信元IPとしてPCのIPアドレスを指定します。この例では、アドレスは10.1.1.2です。
   - **Destination IPv4 address**: 宛先IPとしてデバイスのIPアドレスを指定します。この例では、アドレスは10.1.1.1です。

デバイスからPCにアクセスするには、デバイスからPCへのパケットを許可するセキュリティポリシーを作成します。

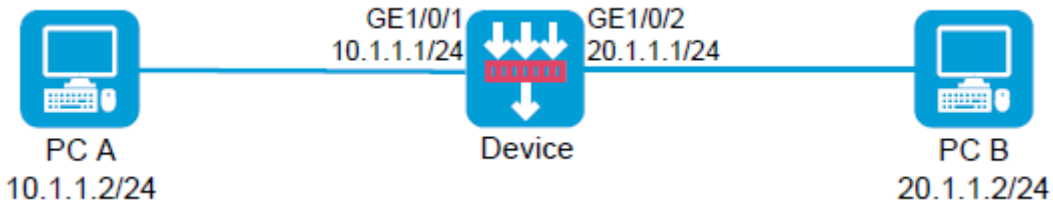
   - **Name**: ポリシー名を指定します。この例では、名前は**local-trust**です。
   - **Source Zone**: Source Zoneとして**Local**を選択します。
   - **Destination Zone**: Destination Zoneとしてインターフェースが属するゾーンを選択します。この例では、Destination Zoneは**trust**です。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてデバイスのIPアドレスを指定します。この例では、アドレスは10.1.1.1です。
   - **Destination IPv4 address**: 宛先IPとしてPCのIPアドレスを指定します。この例では、アドレスは10.1.1.2です。
9. **OK**をクリックします。

デバイスを介して接続された2台のPC間の接続障害

症状

2台のパソコン台のPCが接続され、IPとルートの設定が正しく設定されていますが、2台のPCが互いに通信できません。

図3ネットワーク図



ソリューション

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Network > Security Zones**ページにアクセスします。
3. ターゲットセキュリティゾーンの**Edit**アイコンをクリックします。

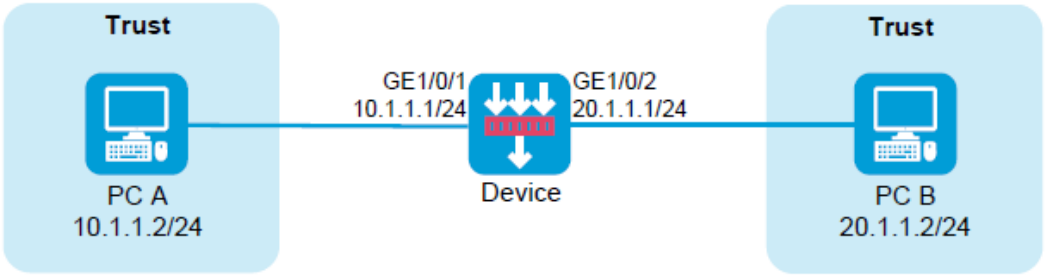
4. デバイスをPCに接続するインターフェースをメンバーインターフェースとして追加します。
5. **OK**をクリックします。
6. 前の手順を繰り返して、他のPCに対するデバイスのインターフェースを別のセキュリティゾーンに追加します。
7. **Policies > Security Policies**ページにアクセスします。
8. **Security Policies**タブで、**Create**、**Create a Policy**の順にクリックします。PC AからPC Bへのパケットを許可するセキュリティポリシーを作成します。
9. 必要に応じてポリシーパラメータを構成します。ベスト・プラクティスとして、正確な一致基準を指定します。
   - **Name**: ポリシー名を指定します。この例では、名前はtrust-untrustです。
   - **Source Zone**: PC Aに接続するインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Destination Zone**: PC Bを接続するインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはUntrustです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アドレスは10.1.1.2です。
   - **Destination IPv4 address**: PC BのIPアドレスを宛先IPとして指定します。この例では、アドレスは20.1.1.1です。
10. デバイスからPCにアクセスするには、デバイスからPCへのパケットを許可するセキュリティポリシーを作成します。
    - **Name**: ポリシー名を指定します。この例では、名前はuntrust-trustです。
    - **Source Zone**: PC Bに接続しているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
    - **Destination Zone**: PC Aを接続するインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはTrustです。
    - **Action**: アクションとしてPermitを選択します。
    - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは20.1.1.2です。
    - **Destination IPv4 address**: 宛先IPとしてPC AのIPアドレスを指定します。この例では、アドレスは10.1.1.1です。
11. **OK**をクリックします。

同じセキュリティゾーン内のデバイスを介して接続されているPC間の接続障害

症状

2台のPCが接続され、IPとルートの設定が正しく設定されています。PCは同じセキュリティゾーンにありますが、互いに到達できません。

図4ネットワーク図



ソリューション

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies**ページにアクセスします。
3. **Security Policies**タブで、**Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はtrust-trustです。
   - **Source Zone**: PCが属するゾーンをSource Zoneとして選択します。この例では、Source Zoneはtrustです。
   - **Destination Zone**: Destination Zoneと同じゾーンを選択します。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AとPC BのIPアドレスを指定します。この例では、PC AとPC Bのアドレスはそれぞれ10.1.1.2と20.1.1.2です。
   - **Destination IPv4 address**: PC BとPC AのIPアドレスを宛先IPとして指定します。この例では、PC BとPC Aのアドレスはそれぞれ20.1.1.2と10.1.1.2です。
5. **OK**をクリックします。

pingまたはtracert操作の失敗

症状

デバイスが宛先へのpingまたはトレースルートに失敗しました。

たとえば、デバイス192.168.20.14からpingデバイス10.0.0.5に送信されたすべてのICMPエコー要求がタイムアウトし、応答が受信されませんでした。

<H3C> ping 10.0.0.5

PING 10.0.0.5 (10.0.0.5): 56 data bytes, press CTRL_C to break Request time out

Request time out

Request time out

Request time out

Request time out

--- 10.0.0.5 ping statistics ---

5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

ソリューション

この問題を解決するには、次の手順に従います

1. display security-zoneコマンドを実行して、パケット転送に関係する入出力インターフェースがセキュリティゾーンに追加されたことを確認します。

```
<H3C>display security-zone
Name: Local
Members: None

Name: Trust
Members:
  GigabitEthernet1/0/8

Name:DMZ
Members:
  None

Name: Untrust
Members:
  GigabitEthernet1/0/10

Name: Management
Members:
  GigabitEthernet1/0/
```

2. display security-policyコマンドを実行して、セキュリティポリシーが設定されていることを確認します。

```
<H3C>display security-policy ip
Security-policy ip
rule 0 name 1 action
pass
<H3C>display security-policy ipv6
Security-policy ipv6
rule 0 name IPv6
action pass
```

3. パケット転送パスを特定し、パス上でICMPパケットが失われた場所を特定します。

   ノードの入出力インターフェースから収集されたICMPパケット統計情報を比較して、パケット損失を特定できます。インターフェースの履歴統計情報をクリアするには、reset counters interfaceコマンドを実行します。

   a. 入力インターフェースでICMPパケットが受信されない場合は、隣接するアップストリームデバイスに障害がないかどうかを調べます。
   b. 入力ICMPパケット数が出力ICMPパケット数と一致する場合は、隣接するダウンストリームデバイスに障害がないかどうかを調べます。
   c. 出力インターフェースでICMPパケットが転送されない場合は、次のステップに進みます。

4. debugging aspf packet aclコマンドおよびdebugging aspf eventコマンドを実行して、ICMPパケット損失がASPFプロセス中に発生したかどうかを確認します。レイヤ2 ICMPパケット転送が正しい場合は、display ip statisticsコマンドを実行して、レイヤ3でのパケット損失の原因を判別します。

```
<H3C> display ip statistics
Input:          sum                 263207520          local                 1772
bad protocol   0                                      bad format            0
bad checksum    0                                     bad options           0
Output:   forwarding                 24511617          local                 476
dropped                              21949             no route              156
compress fails 0
```

Fragment:input 0 output 0

dropped 0

fragmented 0 couldn't fragment 0

Reassembling:sum 0 timeouts 0

5. 問題が解決しない場合は、テクニカルサポートに連絡してください。

NATを介したping動作の失敗

症状

NATが成功したにもかかわらず、デバイスが異なるサブネット内の別のデバイスにpingを実行できません。

たとえば、PC1 10.1.1.1は、PC1のIPアドレスを220.1.1.1に変換するファイアウォールを介してPC2 220.1.1.2にpingします。PC2はPC1のICMPエコー要求を受信しましたが、PC1はPC2からのICMPエコー応答を受信できません。

ソリューション

この問題を解決するには、次の手順に従います

1. PC1およびPC2の入出力インターフェースがセキュリティゾーンに追加されていることを確認し、display security-policyコマンドを実行してセキュリティポリシーが設定されていることを確認します。

   <H3C> display security-policy ip

   Security-policy ip

   rule 0 name tom-tom1

   action pass counting

   enable source-zone tom

   destination-zone tom1

2. ファイアウォールでdisplay ip routing-tableコマンドを実行して、ファイアウォールRIBにPC1へのルートが含まれていることを確認します。

   <H3C> display ip routing-table 10.1.1.0

   PC1へのルートが存在しない場合は、ルーティングプロトコルの設定を調べ、プロトコルが正しく動作していることを確認します。

3. ファイアウォールでdisplay fibコマンドを実行して、ファイアウォールFIBにPC1へのルートが含まれていることを確認します。

   <H3C> display fib 10.1.1.0

   RIBにPC1へのルートが含まれていても、FIBに含まれていない場合は、テクニカルサポートに連絡してください。

4. ファイアウォールでdisplay arpコマンドを実行して、ファイアウォールARPテーブルにPC1(10.1.1.1)のIPアドレスのエントリが含まれていることを確認します。

   <H3C> display arp 10.1.1.1

5. ファイアウォールでdisplay sessionコマンドを実行して、セッションが正しく確立されていることを確認します。

6. ファイアウォールでセキュリティポリシーパケットデバッグをイネーブルにして、パケット拒否の統計情報を表示します。

   ASPFポリシーが適用されている場合は、ポリシーのdetect icmpを設定するか、Destination Zoneから送信元ゾーンへのリターンパケットを許可するセキュリティポリシーを設定する必要があります。設定しない場合、ファイアウォールはリターンパケットを拒否します。

<H3C> debugging security-policy packet ip acl ?

INTEGER<2000-2999> Specify a basic ACL

INTEGER<3000-3999> Specify an advanced ACL

Example output for packet denial is as follows:

*Jul 21 11:00:00:838 2017 F1090-IRF FILTER/7/PACKET: -Context=1; The packet is deny. Src-Zone=tom1, Dst-Zone=tom;If-In=, If-Out=Reth11(134); Packet Info:Src-IP=220.1.1.2, Dst-IP=10.1.1.1, VPN-Instance=,Src-Port=1024, Dst-Port=1025, Protocol= UDP(17), ACL=none, Rule-ID=0.

7. 問題が解決しない場合は、テクニカルサポートに連絡してください。

パケット損失

症状

パケット転送中にパケット損失が発生します。

ソリューション

この問題を解決するには、次の手順に従います

1. debugging security-policy packetコマンドを実行し、パケット損失の原因が不正なセキュリティポリシー設定にあるかどうかを確認します。

<H3C>*Jan 13 16:06:32:29820208350-2FILTER/7/PACKET:-Context=1;The packet is denied. Src-Zone=Untrust, Dst-Zone=Trust;If-In=GigabitEthernet1/0/14(17), If-Out=GigabitEthernet1/0/10(13); Packet Info:Src-IP=10.1.1.3, Dst-IP=100.1.1.3, VPN-Instance=, Src-MacAddr=3897-d6a9-1e58,Src-Port=1024, Dst-Port=1024, Protocol=TCP(6), Application=general_tcp(2086),Terminal=invalid(0), SecurityPolicy=r0, Rule-ID=0.

コマンドの出力にThe packet is deniedが含まれている場合、パケット損失は、セキュリティポリシーの設定が正しくないことが原因です。

2. debugging ip packetコマンドを実行して、失われたパケットに関する情報を表示します。

表6コマンド出力の説明

フィールド	フィールド説明
sending	パケットを送信します。
receiving	パケットを受信します。
Delivering	IPパケットを上位層に配信します。
interface	パケットを受信または送信したインターフェース。
version	パケットの IP バージョン。
headlen	パケットのヘッダー長。
tos	パケットのサービス タイプ。
pktlen	パケットの全長。
pktid	パケットの ID。
offset	パケットのフラグメンテーション オフセット。
ttl	パケットの生存時間。
protocol	パケットのプロトコル フィールド。
checksum	パケットのヘッダー チェックサム。

s パケットの送信元アドレス。

d パケットの宛先アドレス。

3. debug ip errorコマンドおよびdebug ip info aclコマンドを実行して、パケット損失の原因を判別します。

表 7パケット損失の原因

フィールド	説明
The number of queues of reassemble is MAX!	再構成キューの数が制限を超えました。
The queue of reassemble is full!	再構成キュー内のセグメント数が制限を超えました。
Reassemble Failed!	再構成に失敗する。
Get Interface CB failed!	転送制御ブロックの取得に失敗しました。
Release MBUF! Phase Num is *num*, Service ID is *id*, Bitmap is *%#lx!*	MBUFが解放される。num、id、%#lx引数は、それぞれフェーズ番号、サービスID、ビットマップを表します。
Broadcast NOT allowed to be forwarded!	出力インターフェースサブネットへのブロードキャストパケットの転送は許可されません。
Error interface is assigned!	エラー出力インターフェースが割り当てられています。

4. 問題が解決しない場合は、テクニカルサポートに連絡してください。

関連コマンド

コマンド	説明
display arp	ARPエントリを表示します。
display current-configuration | include lsr-id	現在のMPLS LSR IDを表示します。
display fib	FIBエントリを表示します。
display interface	インターフェース情報を表示します。
display ip interface brief	レイヤ3インターフェースの簡単なIP設定を表示します。
display ip routing-table	ルーティングテーブル情報を表示します。
display session	セッション情報を表示します。
display this	現在のビューで実行コンフィギュレーションを表示します。
interface	インターフェースビューを開始します。
display nat outbound	発信ダイナミックNATに関する情報を表示します。

IRFのトラブルシューティング

IRFファブリック確立失敗

症状

IRFファブリックを確立できません。

ソリューション

この問題を解決するには、次の手順に従います

1. メンバーデバイスの数が2を超えていないことを確認します。
2. display versionおよびdisplay system internal versionコマンドを実行して、メンバーデバイスが同じモデルであり、同じソフトウェアバージョンを実行していることを確認します。
   - 機種が異なる場合は、同じ機種を使用してください。
   - ソフトウェアバージョンが異なる場合は、ソフトウェアを同じバージョンにアップグレードします。

<H3C> display version
H3C Comware Software, Version 7.1.064, Ess 8601P08
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved. H3C SecPath F1090
uptime is 0 weeks, 0 days, 0 hours, 5 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-E8601P08.bin Boot
image version: 7.1.064, Ess 8601P08
Compiled Sep 10 2019 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-E8601P08.bin
System image version: 7.1.064, Ess 8601P08
Compiled Sep 10 2019 15:00:00

SLOT 1
CPU type: Multi-core CPU
DDR4 SDRAM Memory: 8192M
bytes FLASH: 7296M bytes
CPLD_A Version: 1.0
CPLD_B Version: 1.0
Release Version:SecPath F1090-8601P08
Basic BootWare Version:0.30
Extend BootWare Version:1.01
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.A
HD_BackBoard Version:Ver.D Pcb
Version:Ver.A
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.A, (Driver)1.0, (Cpld)1.0
Boot Type: Warm

3. 各メンバーデバイスのメンバーIDが一意であることを確認します。
   a. display irfコマンドを実行して、各メンバーデバイスのメンバーIDを表示します。

```
<H3C> display irf
MemberID        Role        Priority  CPU-Mac                 Description
*+1             Master      1         00ff-fbec-b003  ---
--------------------------------------------------------------------------------
* indicates the device is the master.
+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 00ff-fbec-b001 Auto upgrade
                                        : yes
Mac persistent                          : 6 min
Domain ID                               : 0
```

   b. メンバーIDが一意でない場合は、irf member renumberコマンドを実行して1つのメンバーデバイスのメンバーIDを変更します。
4. IRFポートにバインドされた物理インターフェースがIRF物理インターフェースとして動作できることを確認します。詳細については、コンフィギュレーションガイドのIRF設定を参照してください。
5. IRFポートバインディングと物理IRFリンク接続が正しいことを確認します。

重要:

2つの隣接するIRFメンバーを接続する場合は、一方のメンバーのIRFポート1の物理インターフェースを、もう一方のメンバーのIRFポート2の物理インターフェースに接続する必要があります。

   a. 各メンバーデバイスでdisplay irf configurationコマンドを実行し、IRF-Port1およびIRF-Port2フィールドでポートバインディングを確認します。
   b. 物理IRF接続がIRFポートバインディングと一致していることを確認します。
   c. バインディングエラーまたは接続の不一致がある場合は、IRFポートバインディングを再設定するか、IRF物理インターフェースを再接続します。
6. 少なくとも1つのIRF物理リンクがアップしていることを確認します。
   a. display interfaceコマンドを実行して、IRF物理インターフェースがアップ状態であることを確認します。

```
<H3C> display interface gigabitethernet 1/0/10

GigabitEthernet1/0/10
Current state: UP
Line protocol state: UP
Description: GigabitEthernet1/0/10 Interface Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet protocol processing: disabled
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0000-560a IPv6
Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0000-560a Media type is
twisted pair
Port hardware type is 1000_BASE_T
Last clearing of counters: Never
Peak value of input: 0 bytes/sec, at 2013-12-13 15:15:02
Peak value of output: 0 bytes/sec, at 2013-12-13 15:15:02
Last 300 seconds input:  0 packets/sec 0 bytes/sec
Last 300 seconds output:  0 packets/sec 0 bytes/sec
```

   b. IRF物理リンクが起動していない場合は、問題を特定して、少なくとも1つのIRF物理リンクを

起動します。リンクの両端のIRF物理インターフェースが起動すると、IRF物理リンクが起動します。インターフェースを起動するには、「インターフェースが起動しない」を参照してください。

7. 問題が解決しない場合は、H3Cサポートに連絡してください。

IRF分割

症状

IRFファブリックが分割されます。

ソリューション

この問題を解決するには、次の手順に従います

1. IRFポートダウンイベントのログメッセージを検索します。このイベントは、IRFファブリックがスプリットした時間を判断するのに役立ちます。

   %Jun2610:13:46:2332013H3CSTM/2/STM_LINK_STATUS_TIMEOUT:IRFport1isdownbecause heartbeat timed out.

   %Jun 26 10:13:46:436 2013 H3C STM/3/STM_LINK_STATUS_DOWN: -MDC=1; IRF port 2 is down.

2. IRF物理インターフェースが正しく動作していることを確認します。

   a. display interfaceコマンドを実行して、IRF物理インターフェースの状態を識別します。IRF物理インターフェースが起動していないか、その他の問題がある場合は、「インターフェースのトラブルシューティング」の説明に従って問題を特定して解決します。

      <H3C> display interface gigabitethernet 1/0/10

      GigabitEthernet1/0/10 current state: UP

      Line protocol current state: UP

      IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-e80d-c000 Description:

      GigabitEthernet2/6/0/1 Interface

      Loopback is not set

      Media type is optical fiber, Port hardware type is 1000_BASE_SX_SFP

      ...

   b. 問題が解決しない場合は、障害のあるIRF物理インターフェースをIRFポートから削除し、新しいIRF物理インターフェースをIRFポートにバインドします。

3. IRF irFスプリットイベントの原因となるハードウェアの問題を削除します。

   a. display versionコマンドを実行して、IRFリンクを持つIRFメンバーデバイスおよびカード(存在する場合)のアップタイムを特定します。

   b. IRFメンバーデバイスとカード(存在する場合)のアップタイムを比較して、IRFスプリットの前にメンバーデバイスまたはカードがリブートされたかどうかを確認します。

   c. IRFスプリットの原因がデバイスまたはカード(存在する場合)の再起動または電源障害の場合は、「ハードウェアのトラブルシューティング」の説明に従って問題を特定して解決します。

4. IRFスプリットの問題が解決しない場合は、デバイスの診断情報を収集し、その情報をH3Cサポートに送信します。

関連コマンド

コマンド	説明
display interface	インターフェース情報を表示します。 このコマンドを使用して、IRF物理インターフェースがアップ状態であるかどうかを識別します。
display irf	メンバーID、ロール、プライオリティ、ブリッジMACアドレス、各IRFメンバーの説明など、IRFファブリック情報を表示します。
display irf configuration	現在のメンバーID、新しいメンバーID、および各IRFメンバーデバイス上のIRFポートにバインドされている物理インターフェースなど、基本的なIRF設定を表示します。新しいメンバーIDは再起動時に有効になります。 このコマンドを使用して、一方のメンバーのIRFポート1の物理インターフェースが、もう一方のメンバーのIRFポート2の物理インターフェースに接続されているかどうかを識別します。
display version **display system internal version**	システムのバージョン情報を表示します。 このコマンドを使用して、メンバーデバイスが同じモデルであり、同じソフトウェアバージョンを実行しているかどうかを識別します。

RBMトラブルシューティング

RBMシステムセットアップエラー

症状

2つのデバイスでRBMシステムを形成することはできません。

ソリューション

この問題を解決するには、次の手順に従います

1. display versionコマンドを実行して、RBMシステムのメンバーデバイスが同じモデルであることを確認します。

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Feature 8660P08
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved. H3C SecPath
F1000-AI-60 uptime is 0 weeks, 1 day, 17 hours, 11 minutes Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-F8660P08.bin Boot
image version: 7.1.064, Feature 8660P08
  Compiled Jan 18 2021 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-F8660P08.bin
System image version: 7.1.064, Feature 8660P08
  Compiled Jan 18 2021 15:00:00 Feature
image(s) list:
  flash:/F1090FW-CMW710-DEVKIT-F8660P08.bin, version: 7.1.064
    Compiled Jan 18 2021 15:00:00
  flash:/F1090FW-CMW710-SECESCAN-F8660P08.bin, version: 7.1.064
    Compiled Jan 18 2021 15:00:00

SLOT 1
CPU type:                    Multi-core CPU
DDR4 SDRAM Memory:     8192M
bytes FLASH:               7296M bytes
CPLD_A                 Version:  1.0
CPLD_B                 Version:  2.0
Release                Version:SecPath F1000-AI-60-8660P08
Basic  BootWare  Version:1.07
Extend BootWare  Version:1.07
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.D
HD_BackBoard Version:Ver.A Pcb
Version:Ver.B
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0
```

[SUBCARD 2] NSQM1TG4FBA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0

2. Boot Type: Warm RBMシステムのメンバーデバイスが2つだけであることを確認します。
3. display irfコマンドを実行して、メンバーデバイスが一意のIRFメンバーIDを使用していることを確認します。メンバーデバイスが同じIRFメンバーIDを使用している場合は、irf memberコマンドを使用して、メンバーデバイスの1つのIRFメンバーIDを変更します。

```
<H3C>display  irf
MemberID       Role       Priority  CPU-Mac                  Description
*+1            Master  1             80e4-55d8-54ae  ---
--------------------------------------------------------------------------------
* indicates the device is the master.
+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 80e4-55d8-54ac Auto
upgrade                              : yes
Mac persistent                       : 6 min
Domain ID                            : 0
```

4. display interface briefコマンドを実行して、RBMデータおよび制御チャネル設定がメンバーデバイス上で一貫していることを確認します。
5. メンバーデバイスが同じソフトウェアバージョンを使用していることを確認します。

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Feature 8660P08
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved. H3C SecPath
F1000-AI-60 uptime is 0 weeks, 1 day, 17 hours, 11 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-F8660P08.bin Boot
image version: 7.1.064, Feature 8660P08
Compiled Jan 18 2021 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-F8660P08.bin
System image version: 7.1.064, Feature 8660P08
Compiled Jan 18 2021 15:00:00 Feature
image(s) list:
flash:/F1090FW-CMW710-DEVKIT-F8660P08.bin, version: 7.1.064
Compiled Jan 18 2021 15:00:00
flash:/F1090FW-CMW710-SECESCAN-F8660P08.bin, version: 7.1.064
Compiled Jan 18 2021 15:00:00

SLOT 1
CPU type:                    Multi-core CPU
DDR4 SDRAM Memory:      8192M
bytes FLASH:                 7296M bytes
CPLD_A                  Version:  1.0
CPLD_B                  Version:  2.0
Release                 Version:SecPath F1000-AI-60-8660P08
Basic  BootWare  Version:1.07
Extend BootWare  Version:1.07
BuckleBoard Version:Ver.A

BackBoard1 Version:Ver.A
```

BackBoard2 Version:Ver.D
HD_BackBoard Version:Ver.A Pcb
Version:Ver.B
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0 [SUBCARD 2]
NSQM1TG4FBA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0
Boot Type: Warm
[H3C-probe]dis system internal version
H3C SecPath F1000-AI-60 V800R006B01D660SP08
Comware V700R001B64D060SP08

6. RBMコントロールチャネルおよびデータチャネルのセットアップに使用されるインターフェースがアップしていることを確認します。インターフェースがダウンしている場合は、「インターフェースがアップにならない」の説明に従ってインターフェースのトラブルシューティングを行います。

<H3C>display interface GigabitEthernet 1/0/1

GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet1/0/1 Interface Bandwidth:
1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass Broadcast
max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 80e4-55d8-54b3 IPv6 packet frame
type: Ethernet II, hardware address: 80e4-55d8-54b3 Media type is twisted pair, loopback
not set, promiscuous mode not set 1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled Last link flapping: 1
days 17 hours 29 minutes
Last clearing of counters: Never
Current system time:2021-02-01 08:42:30 Beijing+08:00:00
Last time when physical state changed to up:2021-01-30 15:12:46 Beijing+08:00:00 Last time when physical state changed to down:2021-01-30 15:12:08 Beijing+08:00:00 Peak input rate: 8499998 bytes/sec, at 2021-01-30 15:18:39
Peak output rate: 5172061 bytes/sec, at 2021-01-30 15:12:53
Last 300 second input: 0 packets/sec 22 bytes/sec 0%
Last 300 second output: 0 packets/sec 25 bytes/sec 0%

7. メンバーデバイスが同じ宛先ポートを使用してRBM制御チャネルをセットアップし、RBM制御チャネルがアップしていることを確認します。

RBM_P

[F1090]display remote-backup-group status

Remote backup group information:
Backup mode: Dual-active Device
role: Primary
Data channel interface: Route-Aggregation64 Local IPv6:
100::1

Remote IPv6: 100::2 Destination port: 60064

Control channel status: Connected

Hot backup status:Enabled

Auto configuration synchronization: Enable Configuration

consistency check interval: 1 hour Delay-time: 1 min

RBMシステム分割

症状

RBMシステムが予期せず分割されます。

ソリューション

この問題を解決するには、次の手順に従います

1. RBMシステムスプリット時間(RBMによって使用されるインターフェースがダウンした時間)のログメッセージを確認します。

   RBM_P<F1010-VRRP-ZHU-1>%Feb 1 07:57:49:310 2021 F1010-VRRP-ZHU-1 LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted

   on port GigabitEthernet1/0/7 (IfIndex 8), neighbor's chassis ID is d461-fe39-d20c, port ID is GigabitEthernet1/0/7.

   %Feb 1 07:57:50:487 2021 F1010-VRRP-ZHU-1 IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/7 changed to down.

   %Feb 1 07:57:50:487 2021 F1010-VRRP-ZHU-1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/7 changed to down.

   %Feb 1 07:58:00:269 2021 F1010-VRRP-ZHU-1 RBM/6/RBM_CHANNEL: Local IPv6=202::1, remote IPv6=202::2, status=Disconnected

2. RBMが使用する物理インターフェースが正しく動作していることを確認します。インターフェースに異常がある場合は、「インターフェースのトラブルシューティング」の説明に従ってトラブルシューティングを行います。

3. DRシステムスプリットの原因について、インターフェース情報を確認します。

   RBM_P<F1010-VRRP-ZHU-1>display interface GigabitEthernet 1/0/7

   GigabitEthernet1/0/7

   Current state: UP

   Line protocol state: UP Description:

   link-f1010-bei Bandwidth: 1000000

   kbps Maximum transmission unit: 1500

   Allow jumbo frames to pass Broadcast

   max-ratio: 100%

   Multicast max-ratio: 100%

   Unicast max-ratio: 100%

   Internet address: 202.1.1.1/24 (Primary)

   IP packet frame type: Ethernet II, hardware address: e8f7-24d9-2875 IPv6 packet frame

   type: Ethernet II, hardware address: e8f7-24d9-2875 Media type is twisted pair, loopback not

   set, promiscuous mode not set 1000Mb/s, Full-duplex, link type is autonegotiation

   Output flow-control is disabled, input flow-control is disabled Output queue -

   Urgent queuing: Size/Length/Discards 0/1024/0 Output queue - Protocol queuing:

   Size/Length/Discards 0/500/0

   Output queue - FIFO queuing: Size/Length/Discards 0/75/0 Last link

flapping: 0 hours 0 minutes 19 seconds

Last clearing of counters: Never Current system

time:2021-02-01 08:00:09

Last time when physical state changed to up:2021-02-01 07:59:51 Last time when

physical state changed to down:2021-02-01 07:57:50 Peak input rate: 1694290

bytes/sec, at 2021-01-30 14:35:26

Peak output rate: 6245465 bytes/sec, at 2021-01-30 14:40:01

Last 300 second input: 1 packets/sec 132 bytes/sec 0%

Last 300 second output: 1 packets/sec 132 bytes/sec 0%

Input (total): 2404856 packets, 808021430 bytes

4. RBM制御チャネルをセットアップするためのインターフェースを提供するインターフェースモジュールのデバイスリブートレコードまたはリブートレコードについて、デバイスのアップタイムおよびログメッセージを確認します。DRシステムが分割されたときにインターフェースモジュールまたはメンバーデバイスがリブートした場合は、電源障害を確認します。
5. 故障したトランシーバーモジュールまたはRBM制御チャネルのセットアップに使用されたインターフェースを交換して、メンバーデバイスが再びRBMシステムを形成できることを確認します。
6. 問題が解決しない場合は、メンバーデバイスに関する情報を収集し、H3Cサポートに連絡してください。

ホットバックアップのトラブルシューティング

冗長グループに割り当てられていない場合、Rethインターフェースにpingできません。

症状

Rethインターフェースが冗長グループに含まれていない場合、デバイスは直接接続されたRethインターフェースにpingできません。

ソリューション

この問題を解決するには、次の手順に従います

1. Rethインターフェースのメンバーインターフェースがパケットを正しく送受信できることを確認します。
   a. debug ethernet packetコマンドを実行して、Rethインターフェースでのパケット伝送をデバッグし、コマンド出力に基づいてエラーを削除します。

      debugging ethernet packet interface Reth 1

   b. ARPラーニングをデバッグし、コマンド出力に基づいてエラーを削除するには、debugging arp errorコマンドを実行します。

      debugging arp error

   c. IP転送をデバッグし、コマンド出力に基づいてエラーを削除するには、debugging ip errorコマンドを実行します。

      debugging ip error

   d. ホットバックアップシステムの両方のメンバーデバイスでdisplay ethernet statisticsコマンドを実行し、エラーパケット数が送信パケット数とともに増加するかどうかを確認します。

      [H3C] display ethernet statistics slot 1

ETH receive packet statistics:

Totalnum	: 1000888	ETHIINum	: 1000888
SNAPNum	: 0	RAWNum	: 0
LLCNum	: 0	UnknownNum	: 0
ForwardNum	: 884856	ARP	: 0
MPLS	: 0	ISIS	: 0
ISIS2	: 0	IP	: 0
IPV6	: 0		

ETH receive error statistics:

NullPoint	: 0	ErrIfindex	: 3
ErrIfcb	: 0	IfShut	: 5
ErrAnalyse	: 0	ErrSrcMAC	: 0
ErrHdrLen	: 0		

ETH send packet statistics:

L3OutNum	: 325126	VLANOutNum	: 0
FastOutNum	: 92115615	L2OutNum	:

0 ETH send error statistics:

MbufRelayNum	: 0	NullMbuf	: 0
ErrAdjFwd	: 0	ErrPrepend	: 0
ErrHdrLen	: 0	ErrPad	: 0
ErrQosTrs	: 0	ErrVLANTrs	: 0
ErrEncap	: 287	ErrTagVLAN	: 0
IfShut	: 0	IfErr	: 0

2. Rethインターフェースがパケットを送受信できない場合は、インターフェースが正しく設定されていることを確認します。

a display reth interface コマンドを実行し、Physical status フィールドと Forwarding status フィールドを確認します。

```
<H3C>display reth interface Reth 1

Reth1 :
  Redundancy group  : fqs
  Member              Physical    status    Forwarding    status    Presence status
  GE1/1/1.500         UP                    Active                  Normal
  GE2/0/1.500         UP                    Inactive                Normal
```

a. Rethインターフェースの両方のメンバーインターフェースが非アクティブまたはダウンしている場合は、原因を特定して解決します。

b. メンバーインターフェースが正常に動作している場合は、正しいARPエントリがあるかどうかを確認します。メンバーインターフェースがサブインターフェースの場合は、ARPエントリに正しいVLAN IDが含まれている必要があります。

c. Rethインターフェースを再起動して、ARPエントリが正しくリフレッシュできることを確認します。

d. 物理メンバーインターフェースに関するパケット統計情報をチェックして、ドライバがCPUにパケットを正しく送信していることを確認します。

3. 問題が解決しない場合は、H3Cサポートに連絡してください。

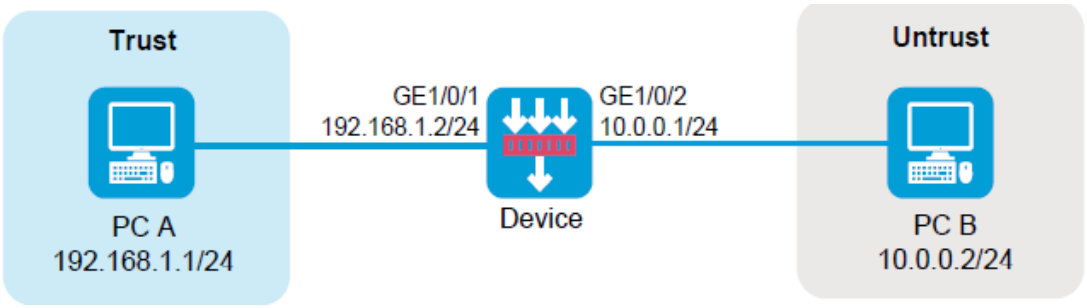
ポリシーNATのトラブルシューティング

内部ユーザーから外部ネットワークにアクセスできない

症状

内部ネットワーク内のPC Aは、ゲートウェイ装置を介して外部ネットワーク内のPC Bにアクセスできません。

図5 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies** ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy1です。
   - **Source Zone**: PC Aに接続されているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Destination Zone**: PC Bに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはUntrustです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。
   - **Destination IPv4 address**: PC BのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.2です。
5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

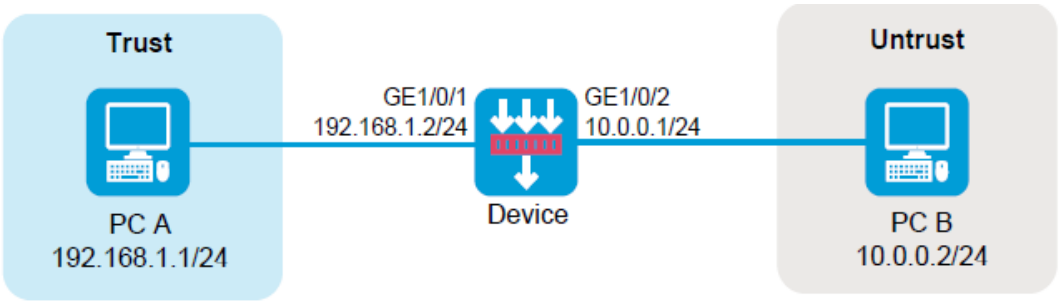
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Policy** ページにアクセスします。
3. **Create**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Rule name**: ルール名を指定します。この例では、名前はpolicy1です。
   - **Change Mode**: 送信元アドレス変換を変更モードとして選択します。
   - **Source Zone**: PC Aに接続されているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Destination Zone**: PC Bに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはUntrustです。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。
   - **Destination IPv4 address**: PC BのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.2です。
   - **Translation method**: 変換方式としてDynamic IP+portを選択します。
   - **Address**: 送信元アドレス変換のNATアドレスタイプを選択します。この例では、アドレスタイプはNATアドレスグループです。
   - **Source address after NAT**: 送信元アドレス変換用のパブリックNATアドレスグループを選択します。
5. **OK**をクリックします。

送信元アドレス変換エラー

症状

送信元アドレス変換が設定されたデバイスで2台のPCが接続されていますが、内部ネットワークのPC Aは外部ネットワークのPC Bにアクセスできません。

図6 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy2です。
   - **Source Zone**: PC Aに接続されているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Destination Zone**: PC Bに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはUntrustです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。
   - **Destination IPv4 address**: PC BのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.2です。
5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Policy**ページにアクセスします。
3. **Edit**アイコンをクリックして、送信元アドレス変換規則を変更します。
4. 表示される**Modify NAT policy**ダイアログボックスで、次のパラメータのアドレスが10.0.0.1/24ネットワーク内にあるかどうかを確認します。
   - NAT後の送信元IPアドレス。
   - アドレス変換用のネットワークアドレス。

- アドレス変換用のアドレスグループ内のアドレスオブジェクト。
- アドレス変換用のNATアドレスグループ内のアドレス。

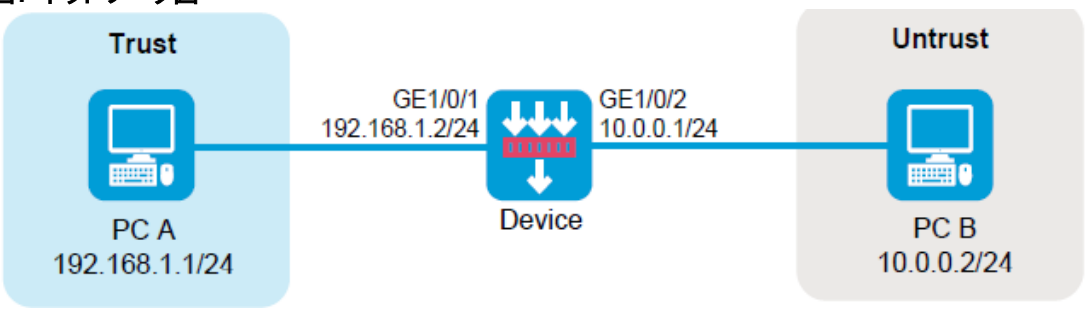
5. 該当する場合は、関連する設定を変更して、リターンパケットがデバイスのインターフェースGE 1/0/2に送信できることを確認します。
6. **OK**をクリックします。

宛先アドレス変換失敗

症状

宛先アドレス変換が設定されたデバイスで2台のPCが接続されていますが、外部ネットワークのPC Bは内部ネットワークのPC Aにアクセスできません。

図7 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy3です。
   - **Source Zone**: PC Bに接続されたインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
   - **Destination Zone**: PC Aに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはTrustです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
   - **Destination IPv4 address**: 宛先IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。

5. OKをクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

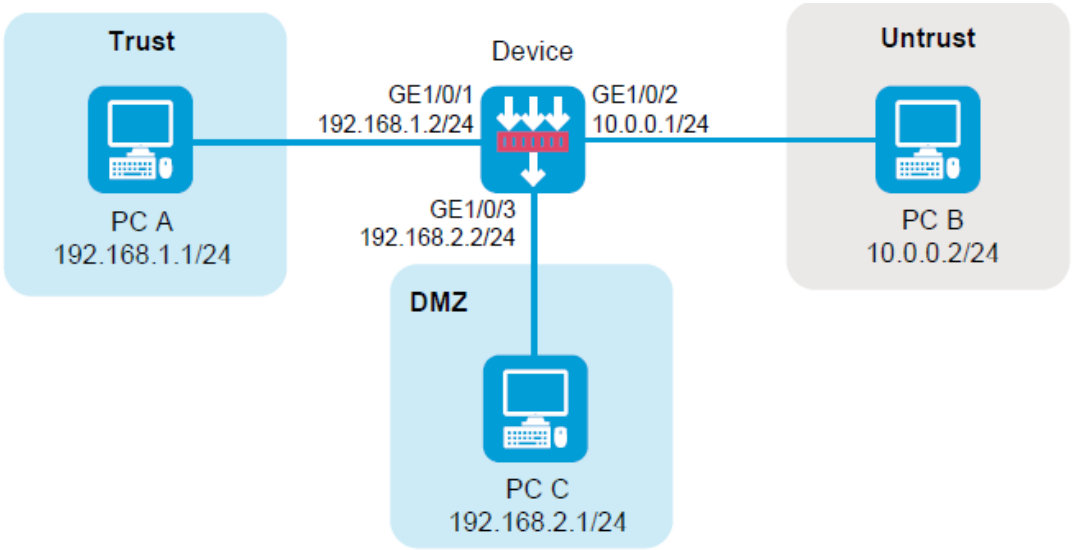
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Policy**ページにアクセスします。
3. **Edit**アイコンをクリックします。
4. 宛先アドレス変換規則を変更します。
5. **OK**をクリックします。

宛先アドレス変換失敗(宛先アドレス変換と統合されたソースアドレス変換)

症状

PC BとPC Cは、NATサーバー機能が設定されたデバイスを介して接続されています。ただし、PC Bは、パブリックアドレス10.0.0.100と宛先ポート80を使用してPC Cにアクセスできません。

図8 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. Createをクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy4です。

- **Source Zone**: PC Bに接続されたインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
- **Destination Zone**: PC Cに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはDMZです。
- **Action**: アクションとしてPermitを選択します。
- **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
- **Destination IPv4 address**: PC CのIPアドレスを宛先IPとして指定します。この例では、アドレスは192.168.2.1です。

5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

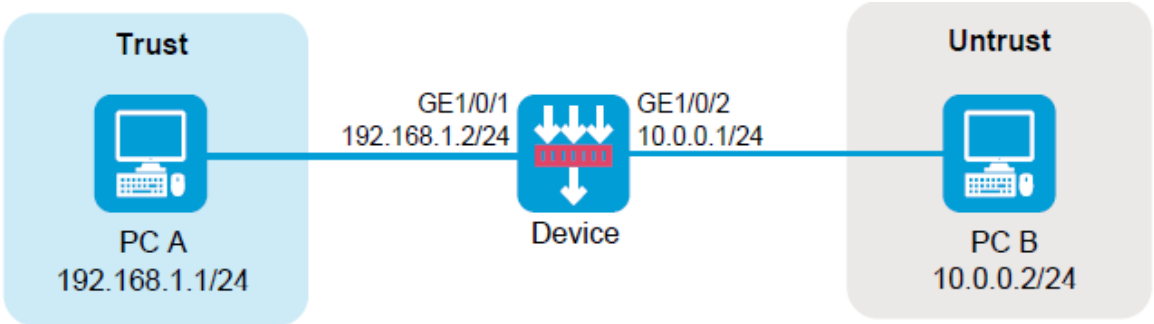
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Policy**ページにアクセスします。
3. ルールの**Translation method**カラムに**Dynamic IP+port**と表示されている場合は、**Edit**アイコンをクリックします。
4. 表示されたダイアログボックスで、NATアドレスグループのポート範囲からポート番号80を削除します。
5. **OK**をクリックします。

IP Sec設定の失敗(IPsecと統合されたNAT)

症状

2台のPCはIPsecと送信元アドレス変換の両方が設定されたデバイスで接続されていますが、PC Aが PC Bにパケットを送信した場合、送信元アドレス変換後のパケットに対してIPsec保護を行うことはできません。

図9 ネットワーク図



ソリューション

この問題を解決するには、次の手順に従います

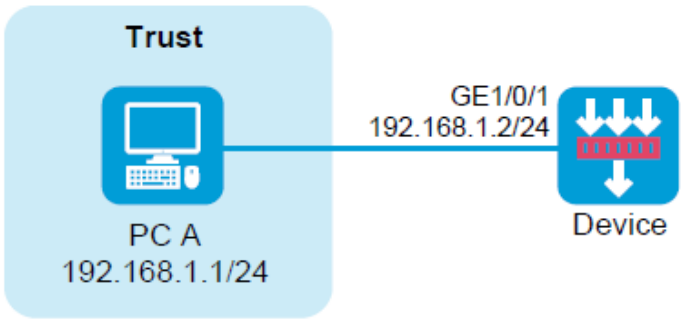
1. デバイスのWebインターフェースにログインします。
2. **Network > VPN > IPsec > IPsec Policies**ページにアクセスします。
3. 単一のIPsecポリシーを変更するには、**Edit**アイコンをクリックします。
4. **Data flow filter rule**領域で、フローをIPsecで保護するために、送信元アドレスと宛先アドレスをNAT後のアドレスに変更します。
5. **OK**をクリックします。

ポリシーベースNATで設定されたゲートウェイデバイスへの内部ユーザーからのアクセスの失敗

症状

内部ネットワーク内のPC Aがデバイスにアクセスできません。

図10 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy5です。
   - **Source Zone** :PC Aに接続するインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Destination Zone**: Destination Zoneとして**Local**を選択します。
   - **Action**: アクションとして**Permit**を選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アド

レスは192.168.1.1です。

- **Destination IPv4 address**: 内部ネットワークに接続されているインターフェースのIPアドレスを宛先IPとして指定します。この例では、アドレスは192.168.1.2です。

5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

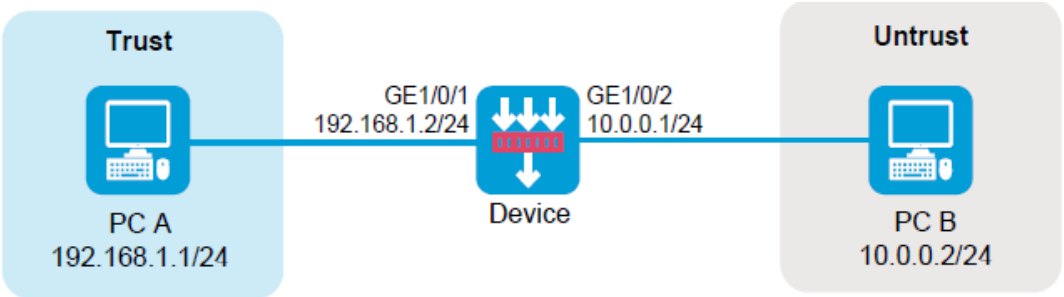
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Policy**ページにアクセスします。
3. **Source security zone**カラムに規則が*Any*と表示されている場合は、**Edit**アイコンをクリックします。
4. 表示されたダイアログボックスで、宛先アドレス変換の次のパケット一致パラメータを変更します。
   - **Destination Zone**: 宛先セキュリティゾーンを指定します。パラメータの値をLocalにすることはできません。
   - **Source IP**: 送信元IPv4アドレスを指定します。パラメータの値を192.168.1.1にすることはできません。
   - **Destination IP**: IPv4アドレスを指定します。パラメータの値を192.168.1.2にすることはできません。
5. **OK**をクリックします。

発信元アドレス変換が設定されたゲートウェイデバイスに外部ユーザーからアクセスできない

症状

ソースアドレス変換が設定されたゲートウェイデバイスを介して2台のPCが接続されていますが、PC Bからはアクセスできません。

図11 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy6です。
   - **Source Zone**: PC Bに接続されたインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
   - **Target Zone**: Destination ZoneとしてLocalを選択します。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
   - **Destination IPv4 address**: 外部ネットワークに接続されているインターフェースのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.1です。
5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

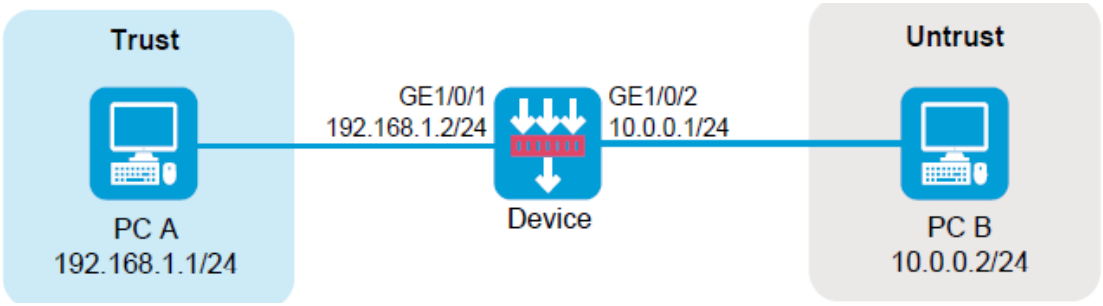
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Policy**ページにアクセスします。
3. 送信元アドレス変換のルールでTranslation methodカラムに**Dynamic IP**と表示されている場合は、**Edit**アイコンをクリックしてルールを編集します。
4. 送信元アドレス変換のアドレスオブジェクトグループまたはNATアドレスグループに、外部ネットワークに接続されたインターフェースのアドレスが含まれている場合は、そのアドレスをグループから削除します。
5. **OK**をクリックします。

外部ユーザーから宛先アドレス変換が設定されたゲートウェイデバイスへのアクセスの失敗

症状

宛先アドレス変換が設定されたゲートウェイデバイスを介して2台のPCが接続されていますが、外部PC Bからはアクセスできません。

図12 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy7です。
   - **Source Zone**: PC Bに接続されたインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source Zoneは**Untrust**です。
   - **Destination Zone**: Destination Zoneとして**Local**を選択します。
   - **Action**: アクションとして**Permit**を選択します。
   - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
   - **Destination IPv4 address**: デバイス上の外部ネットワークに接続されているインターフェースのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.1です。
5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. デバイスのWebインターフェースにログインします。
3. **Policies > NAT > NAT Policy**ページにアクセスします。
4. 宛先アドレス変換のルールエントリに**Multiple to one address translation**と表示された場合**Destination address translation method**カラムで、**Edit**アイコンをクリックします。
5. 宛先アドレス一致条件に、デバイス上の外部ネットワークに接続されているインターフェースのアドレスが含まれている場合は、サービス一致条件を確認します。
6. 条件にPC Bがデバイスにアクセスするために使用するサービスが含まれている場合は、実際の状況に基づいて次の解決方法を実行します。
   - PC Bがデバイスへのアクセスに使用するサービスを変更します。

- サービス一致条件からサービスを削除して、NATモジュールがそのサービスを含むトラフィックで宛先アドレス変換を実行しないようにします。

7. **OK**をクリックします。

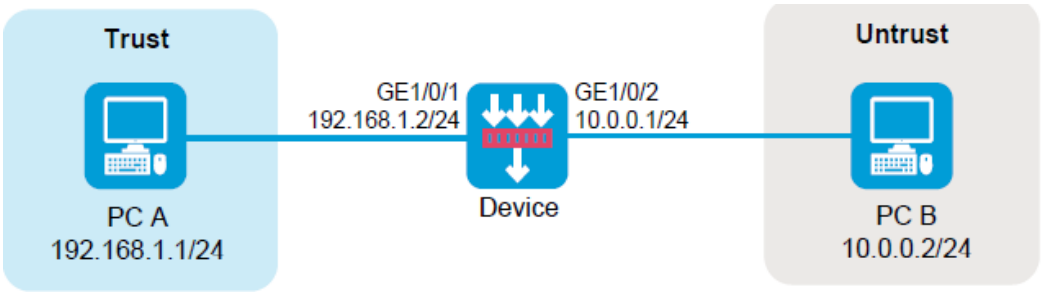
インターフェースNATのトラブルシューティング

内部ユーザーから外部ネットワークにアクセスできない

症状

内部ネットワーク内のPC Aは、ゲートウェイ装置を介して外部ネットワーク内のPC Bにアクセスできません。

図13 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy1です。
   - **Source Zone**: PC Aに接続するインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはTrustです。
   - **Destination Zone**: ンPC Bを接続するインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはUntrustです。
   - **Action**: アクションとして**Permit**を選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。

- **Destination IPv4 address**: PC BのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.2です。

5. **OK**をクリックします。

ソリューション(インターフェースNAT)

この問題を解決するには、次の手順に従います

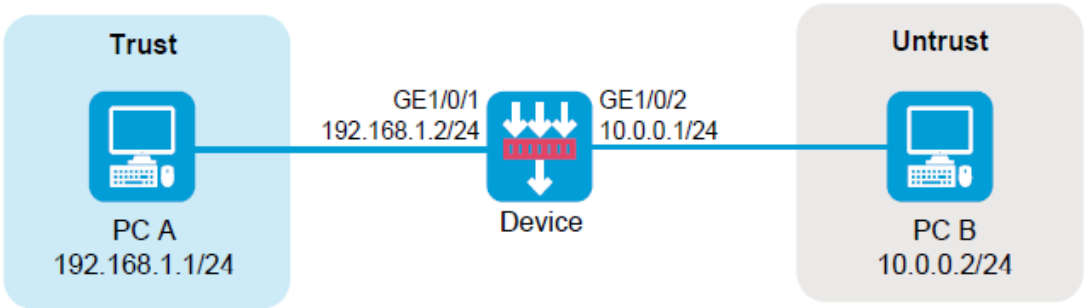
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > Dynamic NAT**ページにアクセスします。
3. **Outbound Dynamic NAT (ACL-Based)**タブをクリックします。
4. **Create**をクリックします。
5. 必要に応じて、ポリシーパラメータを設定します。
   - **Interface**: インターフェースを指定します。この例では、インターフェースはGE1/0/2です。
   - **ACL**: NATモジュールによって変換される発信パケットの送信元IPアドレスを定義するACLを指定します。
   - **Source address after NAT**: NATアドレスグループを指定します。この例では、IPアドレスは送信元アドレス変換に使用されるパブリックアドレスです。
   - **Translation mode**: 変換モードとしてPATを選択します。
6. **OK**をクリックします。

送信元アドレス変換エラー

症状

送信元アドレス変換が設定されたデバイスで2台のPCが接続されていますが、内部ネットワークのPC Aは外部ネットワークのPC Bにアクセスできません。

図14 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。

2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy2です。
   - **Source Zone**: PC Aに接続されているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source Zoneは**Trust**です。
   - **Destination Zone**: PC Bに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはUntrustです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。
   - **Destination IPv4 address**: PC BのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.2です。
5. **OK**をクリックします。

ソリューション(インターフェースNAT)

この問題を解決するには、次の手順に従います

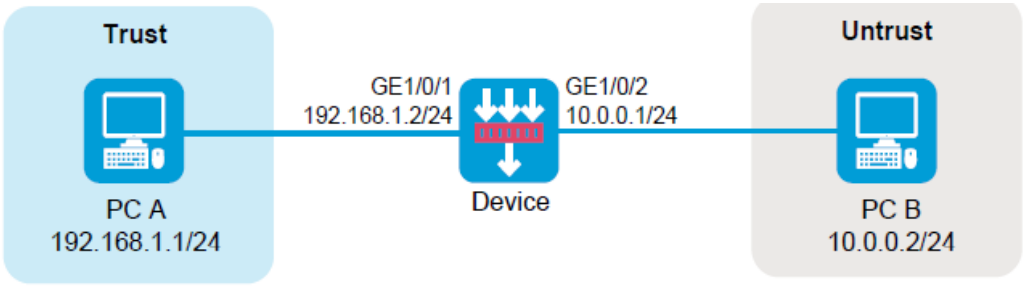
1. デバイスのWebインターフェースにログインします。
2. **Edit**アイコンをクリックして、送信元アドレス変換規則を変更します。
3. 表示されるダイアログボックスで、次のパラメータのアドレスが10.0.0.1/24ネットワーク内にあるかどうかを確認します。
   - NAT後の送信元アドレス。
   - アドレス変換用のネットワークアドレス。
   - アドレス変換のアドレスオブジェクトグループ内のアドレスオブジェクト。
   - アドレス変換用のNATアドレスグループ内のアドレス。
4. 該当する場合は、関連する設定を変更して、リターンパケットがデバイスのインターフェースGE 1/0/2に送信できることを確認します。
5. **OK**をクリックします。

宛先アドレス変換エラー

症状

宛先アドレス変換が設定されたデバイスで2台のPCが接続されていますが、外部ネットワークのPC Bは内部ネットワークのPC Aにアクセスできません。

図15 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. **Create**をクリックし、**Create a Policy**をクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy3です。
   - **Source Zone**: PC Bに接続されたインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
   - **Destination Zone**: PC Aに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはTrustです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
   - **Destination IPv4 address**: 宛先IPとしてPC AのIPアドレスを指定します。この例では、アドレスは192.168.1.1です。
5. **OK**をクリックします。

ソリューション(インターフェースNAT)

この問題を解決するには、次の手順に従います

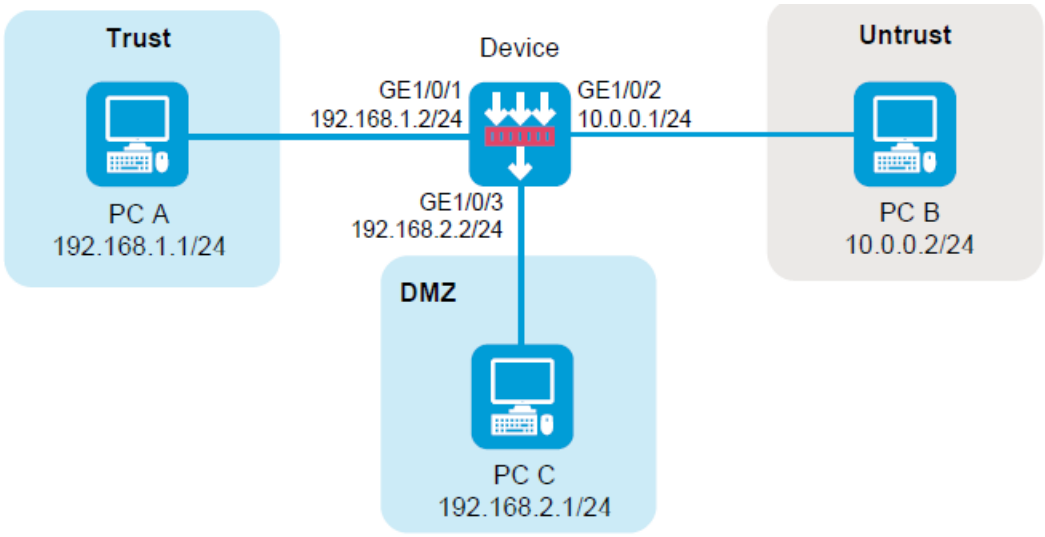
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Servers > Policy Configuration**ページにアクセスします。
3. NAT Serverのパブリックポートが実際に使用されているか確認してください。
4. そうでない場合は、パブリックポートがNATサーバー規則で実際に使用されていることを変更して確認します。
5. **OK**をクリックします。

宛先アドレス変換失敗(宛先アドレス変換と統合されたソースアドレス変換)

症状

PC BとPC Cは、NATサーバー機能が設定されたデバイスを介して接続されています。ただし、PC Bは、パブリックアドレス10.0.0.100と宛先ポート80を使用してPC Cにアクセスできません。

図16 ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. Createをクリックし、Create a Policyをクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy4です。
   - **Source Zone**: PC Bに接続されたインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
   - **Destination Zone**: PC Cに接続されたインターフェースが属するゾーンをDestination Zoneとして選択します。この例では、Destination ZoneはDMZです。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
   - **Destination IPv4 address**: PC CのIPアドレスを宛先IPとして指定します。この例では、

アドレスは192.168.2.1です。

5. OKをクリックします。

ソリューション(インターフェースNAT)

この問題を解決するには、次の手順に従います

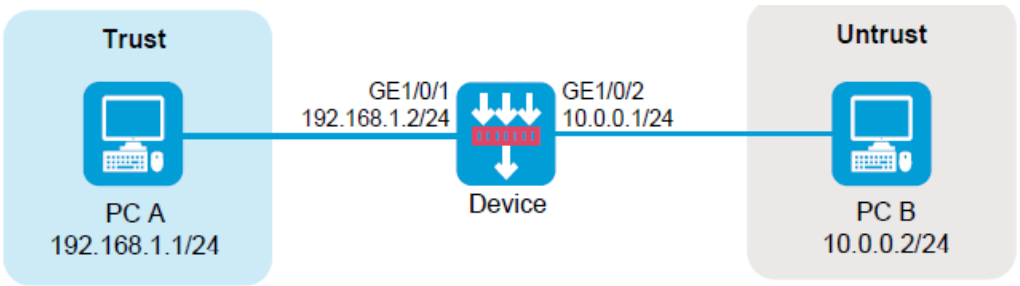
1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > Dynamic NAT**ページにアクセスします。
3. ルールの詳細を表示するには、**Outbound Dynamic NAT(Group-Based)**タブをクリックします。
4. アクションがPATの場合は、**Edit**アイコンをクリックして、NATアドレスグループのポート範囲からポート番号80を削除します。
5. **OK**をクリックします。
6. ルールの詳細を表示するには、**Outbound Dynamic NAT(ACL-Based)**タブをクリックします。
7. 変換モードがPATの場合は、**Edit**アイコンをクリックして、NATアドレスグループのポート範囲からポート番号80を削除します。
8. **OK**をクリックします。

IP Sec設定の失敗(IPsecと統合されたNAT)

症状

2台のPCがIPsecと送信元アドレス変換の両方が正しく設定されたデバイスで接続されていますが、PC AがPC Bにパケットを送信した場合、送信元アドレス変換後のパケットに対してIPsec保護を行うことはできません。

図17 ネットワーク図



ソリューション

この問題を解決するには、次の手順に従います

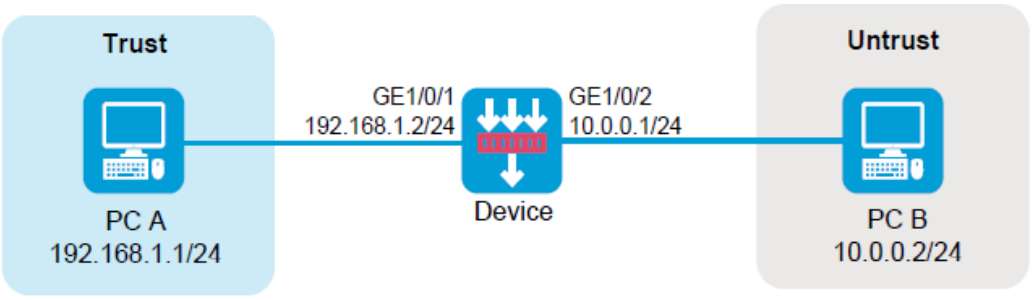
1. デバイスのWebインターフェースにログインします。
2. **Network > VPN > IPsec > IPsec Policies**ページにアクセスします。
3. **Edit**アイコンをクリックして、IPsecポリシーの設定を編集します。
4. **Data flow filter rule**領域で、NATの後のアドレスを送信元アドレスおよび宛先アドレスとして使用し、IPsecによって保護されるパケットを照合します。
5. **OK**をクリックします。

発信元アドレス変換が設定されたゲートウェイデバイスに外部ユーザーからアクセスできない

症状

ソースアドレス変換が設定されたゲートウェイデバイスを介して2台のPCが接続されていますが、PC Bはアクセスできません。

図18 ネットワークダイアグラム



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. Createをクリックし、Create a Policyをクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**: ポリシー名を指定します。この例では、名前はsecpolicy5です。
   - **Source Zone**: PC Bに接続しているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
   - Destination Zone: Destination ZoneとしてLocalを選択します。
   - **Action**: アクションとしてPermitを選択します。
   - **Source IPv4 address**: 送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
   - **Destination IPv4 address**: 外部ネットワークに接続されているインターフェースのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.1です。
5. **OK**をクリックします。

ソリューション(ポリシーベースNAT)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。

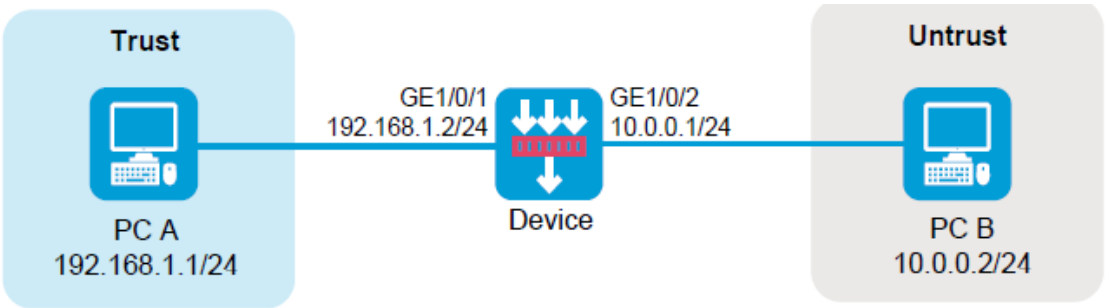
2. **Policies > NAT > Dynamic NAT**ページにアクセスします。
3. Outbound Dynamic NAT(Group-Based)タブをクリックして、Actionカラムが
ノーパット
4. アクションがNO-PATの場合は、Editアイコンをクリックして、パケット一致のNATアドレス
グループからIPアドレス10.0.0.1を削除します。
5. OKをクリックします。
6. Outbound Dynamic NAT(ACL-Based)タブをクリックして、変換方式が
columnはNO-PATです。
7. トランスレーションモードがNO-PATの場合は、Editアイコンをクリックしてを開きます。
ダイアログボックス:
   - アドレス変換のIPアドレスがアドレスグループに属している場合は、NATアドレスグループに10.0.0.1が含まれていないことを確認します。
   - 変換モードがEasy IPの場合、アドレス変換用に指定されたインターフェースはGE1/0/2にできません。
8. OKをクリックします。

外部ユーザーから宛先アドレス変換が設定されたゲートウェイデバイスへのアクセスの失敗

症状

宛先アドレス変換が設定されたゲートウェイデバイスを介して2台のPCが接続されていますが、外部PCBからはアクセスできません。

図19ネットワーク図



ソリューション(セキュリティポリシー)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > Security Policies > Security Policies**ページにアクセスします。
3. Createをクリックし、Create a Policyをクリックします。
4. 必要に応じて、ポリシーパラメータを設定します。
   - **Name**-ポリシー名を指定します。この例では、名前はsecpolicy6です。

- **Source Zone**: PC Bに接続しているインターフェースが属するゾーンをSource Zoneとして選択します。この例では、Source ZoneはUntrustです。
- **Destination Zone**: Destination ZoneとしてLocalを選択します。
- **Action**: アクションとしてPermitを選択します。
- Source IPv4 address:送信元IPとしてPC BのIPアドレスを指定します。この例では、アドレスは10.0.0.2です。
- **Destination IPv4 address**: デバイス上の外部ネットワークに接続されているインターフェースのIPアドレスを宛先IPとして指定します。この例では、アドレスは10.0.0.1です。

5. **OK**をクリックします。

ソリューション(インターフェースNAT)

この問題を解決するには、次の手順に従います

1. デバイスのWebインターフェースにログインします。
2. **Policies > NAT > NAT Servers > Policy Configuration**ページにアクセスします。
3. IPアドレス10.0.0.1がNATサーバー規則によって占有されているかどうかを確認します。
4. **Public IP address**カラムに表示されている場合は、規則の**Edit**アイコンをクリックします
5. 表示される**Edit NAT Server Rule**ダイアログボックスで、PC Bがデバイスにアクセスするためのポートをパブリックポートが占有しているかどうかを確認します。
6. ポートが占有されている場合は、次のいずれかのソリューションを選択します。
   - PC Bからデバイスへのトラフィック用のプロトコルまたは宛先ポートを変更します。
   - ACLベースのパケット一致ルールを変更して、トラフィックが宛先アドレス変換によって処理されないようにします。
7. **OK**をクリックします。

ダイナミックNATエラー

症状

ダイナミックNATが失敗するか、変換されたパケットを正しく転送できません。内部ネットワークのPC Aは、ゲートウェイデバイスを介して外部ネットワークのPC Bにアクセスできません。

ソリューション

この問題を解決するには、次の手順に従います

1. NATが正しく設定されていることを確認します。このセクションでは、アウトバウンドNATを例として使用します。

   [H3C] display nat outbound

NAT outbound information:

There are 1 NAT outbound rules. Interface: Route-Aggregation12

ACL: --- Address group: 257 Port-preserved: N

NO-PAT: N Reversible: N

2. NATパケットのデバッグをイネーブルにし、次のことを確認するには、debugging nat packetコマンドを使用します。
パケットを正しく変換できます。デバッグ情報の例を次に示します。

*May 13 09:58:48:083 2017 H3C NAT/7/COMMON: -slot =1;

PACKET: (Route-Aggregation12-in) Protocol: TCP

4.4.4.6: 21 - 4.4.5.11:11000(VPN: 0)---------- >

4.4.4.6: 21 - 192.168.1.2:13249(VPN: 0)

3. セッション情報が正しいことを確認します。

<H3C> display session table ipv4 verbose

Initiator:

Source IP/port: 192.168.1.2/13790

Destination IP/port: 4.4.4.6/21

DS-Lite tunnel peer: -

VPN instance/VLAN ID/VLL ID: -/-/- Protocol: TCP(6)

Responder:

Source IP/port: 4.4 4.6/21

Destination IP/port: 4.4.4.27/1060

DS-Lite tunnel peer: -

VPN instance/VLAN ID/VLL ID: -/-/- Protocol: TCP(6)

State: TCP_ESTABLISHED

Application: FTP

Start time: 2013-12-15 10:49:00 TTL: 3592s

Interface(in) : Route-Aggregation11

Interface(out): Route-Aggregation12

Zone(in) : Trust

Zone(out): menglei

Initiator->Responder: 3 packets 128 bytes

Responder->Initiator: 2 packets 130 bytes

4. 問題が解決しない場合は、H3Cサポートに連絡してください。

NATは失敗するが、発信インターフェースは外部ネットワークから正常にpingを実行できる

症状

ファイアウォールは、ネットワーク出力でゲートウェイとして機能します。ゲートウェイでNATが失敗し、内部ユーザーと外部ユーザーは互いに到達できませんが、発信インターフェースは外部ネットワークから正常にpingできます。

ソリューション

この問題を解決するには、次の手順に従います

1. NATアドレスグループがインターフェースと同じサブネットにあることを確認します。異なるサブネットにある場合は、NATアドレスグループへのルートがピア側で設定されていることを確認します。
2. NATアドレスグループまたはNATサーバードレスがインターフェースと同じサブネットにある場合は、アドレスグループまたはNATサーバーがgratuitous ARPパケットを送信でき、ピアエンドがMACアドレスを修正する方法を学習したことを確認します。gratuitous ARPパケットが直接接続されたデバイス上で送信されていることを確認できます。

   デバイスは、直接接続されていないデバイスのリンクアソシエーション解除を検出できず、対応するARPエントリを更新できません。Gratuitous ARPを使用すると、デバイスアソシエーション時にターゲットアドレスとして送信元デバイスのアドレスを含むARPパケットを送信できます。gratuitous ARPパケットを受信したデバイスは、自身のARPエントリを更新します。アドレスプールは、時間内にアドレスを更新できない場合があります。
3. ファイアウォールでパケットのデバッグまたはキャプチャをイネーブルにし、pingパケットが正しく転送されること(ping要求と応答の両方が検出されること)を確認します。
4. ピアデバイスからNATアドレスグループまたはNATサーバーに継続的にpingを実行します。ARPデバッグをイネーブルにして、ARPパケットが正しく受信できることを確認します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
display nat outbound	発信ダイナミックNATの設定を表示します。
display nat server	NATサーバーマッピングを表示します。
display session	セッションのバージョン情報を表示します。
save	実行コンフィギュレーションをコンフィギュレーションファイルに保存します。

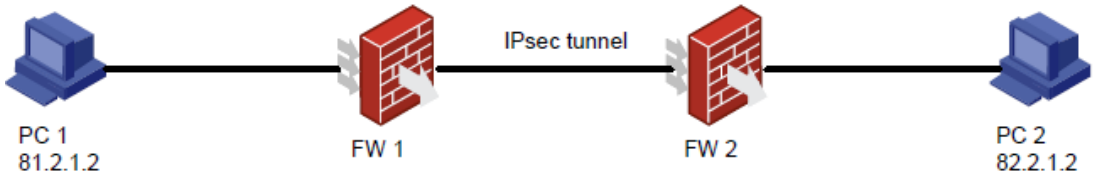
IPsecとIKEのトラブルシューティング

IPsec SAは正常に確立されましたが、IPsecで保護されたトラフィックを転送できません

症状

PC 1とPC 2間のトラフィックを保護するために、FW 1とFW 2間にIKEベースのIPsecトンネルが正常に確立されますが、PCは相互にpingできません。

図20 ネットワーク図



FW 1の設定:

- IP Secトンネルのローカルアドレスとリモートアドレスは、それぞれ81.2.0.1と14.5.1.1です。
- IP SecのACLルール:

  rule 0 permit ip source 81.2.0.0 0.0.0.255 destination 82.2.0.0 0.0.0.255

FW 2の設定:

- IP Secトンネルのローカルアドレスとリモートアドレスは、それぞれ14.5.1.1と81.2.0.1です。
- IP SecのACLルール:

  rule 0 permit ip source 82.2.0.0 0.0.0.255 destination 81.2.0.0 0.0.0.255

ソリューション

この問題を解決するには、次の手順に従います

1. ルートが到達可能であることを確認します。
2. ACLルールのパケットヒットカウントを表示し、ACLルールの設定が保護するトラフィックと一致していることを確認します。
3. FWが、ESPまたはAHカプセル化パケットの通過を許可していることを確認します。
4. **reset ipsec sa**コマンドおよびreset ike saコマンドを使用して、IPsec SAおよびIKE SAをクリアおよび再確立します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

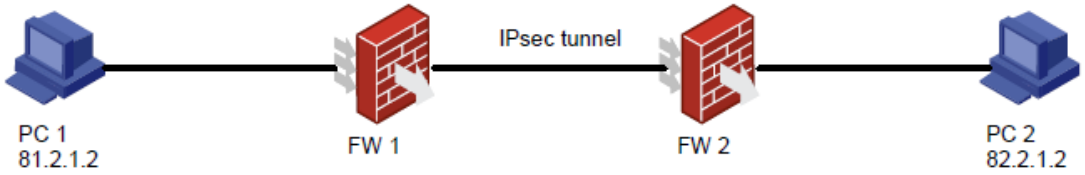
コマンド	説明
display ike sa	IKE SA情報を表示します。
display ipsec sa	IP Sec SA情報を表示します。
reset ike sa	IKE SAをクリアします。
reset ipsec sa	IPsec SAをクリアします。
save	実行コンフィギュレーションを指定したファイルに保存します。

IKE SAは正常に確立されましたが、IPsec SAを確立できません。

症状

PC 1とPC 2間のトラフィックを保護するために、FW 1とFW 2間にIKEベースのIPsecトンネルを確立します。IKE SAは正常に確立されますが、IPsec SAは確立できません。

図21 ネットワーク図



FW 1の設定:

- IP Secトンネルのローカルアドレスとリモートアドレスは、それぞれ81.2.0.1と14.5.1.1です。
- IP SecのACLルール:

  rule 0 permit ip source 81.2.0.0 0.0.0.255 destination 82.2.0.0 0.0.0.255

FW-2の設定:

- IP Secトンネルのローカルアドレスとリモートアドレスは、それぞれ14.5.1.1と81.2.0.1です。
- IP SecのACLルール:

  rule 0 permit ip source 82.2.0.0 0.0.0.255 destination 81.2.0.0 0.0.0.255

ソリューション

この問題を解決するには、次の手順に従います

1. ACLルールのパケットヒットカウントを表示し、ACLルールの設定が保護するトラフィックと一致していることを確認します。
2. FWが一貫したセキュリティプロトコル、暗号化および認証アルゴリズム、およびカプセル化モード設定を持っていることを確認します。
3. IP Secの設定が正しく、完全であることを確認します。たとえば、リモートアドレスまたはIKEプロファイルが正しく設定されていることを確認します。

4. reset ipsec saコマンドおよびreset ike saコマンドを使用して、IPsec SAおよびIKE SAをクリアおよび再確立します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

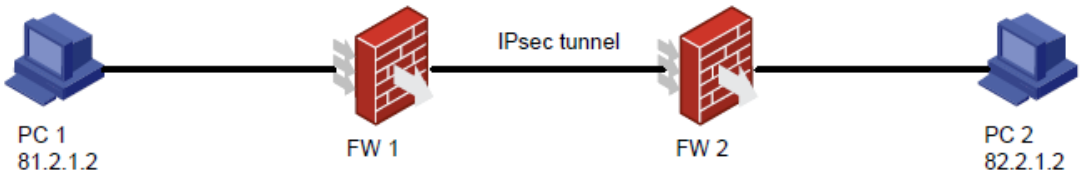
コマンド	説明
display ike sa	IKE SA情報を表示します。
display ipsec sa	IP Sec SA情報を表示します。
reset ike sa	IKE SAをクリアします。
reset ipsec sa	IPsec SAをクリアします。
display ipsec transform-set	IP Secトランスフォームセット情報を表示します。
display ipsec policy	IP Secポリシー情報を表示します。
save	実行コンフィギュレーションを指定したファイルに保存します。

IKE SAを確立できない

症状

PC 1とPC 2間のトラフィックを保護するために、FW 1とFW 2間にIKEベースのIPsecトンネルを確立します。ただし、IKE SAは確立できません。

図22 ネットワーク図



FW 1の設定:

- IP Secトンネルのローカルアドレスとリモートアドレスは、それぞれ81.2.0.1と14.5.1.1です。
- IP SecのACLルール:

  rule 0 permit ip source 81.2.0.0 0.0.0.255 destination 82.2.0.0 0.0.0.255

FW-2の設定:

- IP Secトンネルのローカルアドレスとリモートアドレスは、それぞれ14.5.1.1と81.2.0.1です。
- IP SecのACLルール:

  rule 0 permit ip source 82.2.0.0 0.0.0.255 destination 81.2.0.0 0.0.0.255

ソリューション

この問題を解決するには、次の手順に従います

1. FWが一貫したIKEプロポーザル設定を持っていることを確認します。これには、主に暗号化アルゴリズムと認証アルゴリズム、および認証モードの識別が含まれます。

2. IKE ID認証が成功することを確認します。
   - 事前共有キー認証の場合は、FWで設定されている事前共有キーが同じであることを確認します。
   - 証明書認証では、次の設定を確認します。
     - FW上の証明書が有効期間内であるか、取り消されていない。
     - 証明書には信頼できるCAがあり、同じCAによって署名されています。
     - FWは証明書内に一致するキーを持っています。
   - リモートIDの競合が存在しないことを確認します。競合は、異なるIKEプロファイル内の同一のリモートID設定によって引き起こされる可能性があります。
3. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
display ike proposal	すべてのIKEプロポーザルに関する設定情報を表示します。
display ike sa	IKE SA情報を表示します。
display ipsec sa	IP Sec SA情報を表示します。
reset ike sa	IKE SAをクリアします。
reset ipsec sa	IPsec SAをクリアします。
save	実行コンフィギュレーションを指定したファイルに保存します。

IP Secスマートリンクがリンク品質を検出しない

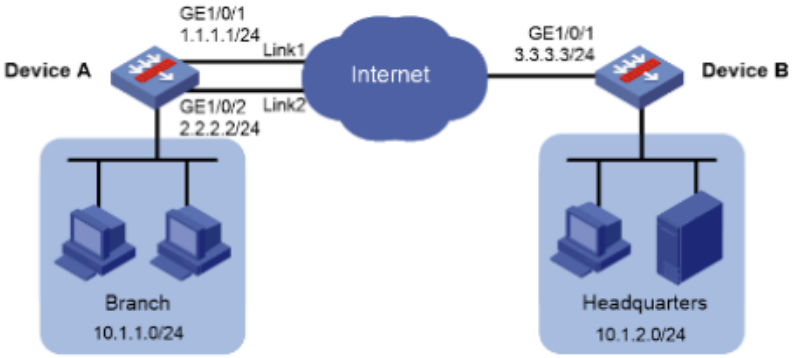
症状

支店はIPsec VPNを介して本社にアクセスします。支店がリンク1またはリンク2(リンク品質の高い方)を介して本社へのIPsecトンネルを確立できるように、IPsecスマートリンク選択を設定します。

- デバイスAは最初にリンク1を使用してIPsecトンネルを確立します。
- リンク1が高いパケット損失率または遅延が発生すると、デバイスAはリンク2に基づいて確立されたIPsecトンネルにトラフィックを自動的に切り替えます。

ただし、IPsecスマートリンクポリシーは期待どおりに機能できません。スマートリンクスイッチオーバーのリンク品質は検出されません。

図23 ネットワークダイアグラム



デバイスAのプライマリ設定

#インターフェースIPアドレスとゲートウェイIPアドレスを設定します。

<DeviceA> system-view

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 24

[DeviceA-GigabitEthernet1/0/1] gateway 1.1.1.3

[DeviceA-GigabitEthernet1/0/1] quit

[DeviceA] interface gigabitethernet 1/0/2

[DeviceA-GigabitEthernet1/0/2] ip address 2.2.2.2 24

[DeviceA-GigabitEthernet1/0/2] gateway 2.2.2.3

[DeviceA-GigabitEthernet1/0/2] quit

#policy1という名前のIPsecスマートリンクポリシーを設定し、そのポリシーでlink 1とlink 2を設定します。

[DeviceA] ipsec smart-link policy policy1

[DeviceA-ipsec-smart-link-policy-policy1] link 1 interface gigabitethernet 1/0/1 remote 3.3.3.3

[DeviceA-ipsec-smart-link-policy-policy1] link 2 interface gigabitethernet 1/0/2 remote 3.3.3.3

#リンクスイッチオーバーサイクルの最大数を4に設定します。

[DeviceA-ipsec-smart-link-policy-policy1] link-switch cycles 4

#ポリシーでIPsecスマートリンク選択を有効にします。

[DeviceA-ipsec-smart-link-policy-policy1] smart-link enable

[DeviceA-ipsec-smart-link-policy-policy1] quit

デバイスBのプライマリ設定

#インターフェースのIPアドレスを設定します。

<DeviceB> system-view

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] ip address 3.3.3.3 24

[DeviceB-GigabitEthernet1/0/1] quit

[DeviceB] acl advanced 3000

[DeviceB-acl-ipv4-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255

[DeviceB-acl-ipv4-adv-3000] rule permit ip source 3.3.3.0 0.0.0.255 destination 1.1.1.0 0.0.0.255

[DeviceB-acl-ipv4-adv-3000] rule permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.0 0.0.0.255

[DeviceB-acl-ipv4-adv-3000] quit

#デバイスBがデバイスAに接続されたサブネットに到達するようにスタティックルートを設定します。この例では、ルートのネクストホップアドレスとして3.3.3.1を使用しています。

[DeviceB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 1/0/1 3.3.3.1

[DeviceB] ip route-static 1.1.1.0 255.255.255.0 gigabitethernet 1/0/1 3.3.3.1

[DeviceB] ip route-static 2.2.2.0 255.255.255.0 gigabitethernet 1/0/1 3.3.3.1

ソリューション

この問題を解決するには、次の手順に従います

1. リンクが有効であることを確認します。たとえば、インターフェースにIPアドレスが割り当てられていて、インターフェースの状態がupであることを確認します。
2. スマートリンク設定が完了していることを確認します。たとえば、スマートリンクポリシーがIPsecポリシーで指定されていること、およびルートのネクストホップが正しく設定されていることを確認します。
3. IP Secポリシー設定が正しく、完全であることを確認します。
4. リンクスイッチオーバーサイクルの最大数をより大きな値に変更して、障害がリンクスイッチオーバーサイクル数の制限によって引き起こされないようにします。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
display ike sa	IKE SA情報を表示します。
display ipsec sa	IP Sec SA情報を表示します。
reset ike sa	IKE SAをクリアします。
reset ipsec sa	IPsec SAをクリアします。
display ipsec smart-link policy	IP Secスマートリンクポリシー情報を表示します。
display ipsec policy	IP Secポリシー情報を表示します(IPsecポリシー設定を確認し、指定されたスマートリンクポリシーを表示します)。
display acl 3000	ダイナミックACLルールに関する情報を表示します。
save	実行コンフィギュレーションを指定したファイルに保存します。

IP Secトンネルインターフェースベースの IPsecトンネルを確立できない

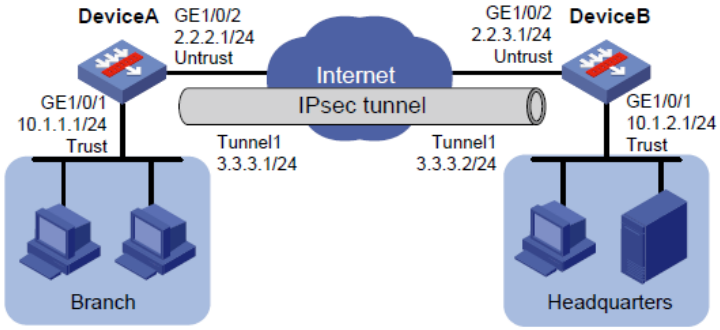
症状

支店と本社はどちらも固定IPアドレスを使用してインターネットにアクセスします。

支店サブネットが変更されても本社のIPsec設定が安定するように、IPsecトンネルインターフェースベースのIPsecがデバイスAとデバイスBに設定されます。このトンネルは、支店(10.1.1.0/24)と本社(10.1.2.0/24)の間のすべてのトラフィックを保護するために使用されます。

ただし、IPsecトンネルインターフェースベースのIPsecトンネルを期待どおりに確立できません。

図24 ネットワークダイアグラム



デバイスAのIPsecトンネルインターフェース設定:

IPsecトンネルインターフェースTunnel1を作成します。

[DeviceA] interface tunnel 1 mode ipsec

#トンネルインターフェースのIPアドレスを設定します。

[DeviceA-Tunnel1] ip address 3.3.3.1 255.255.255.0

#デバイスAのGE 1/0/2のIPアドレスをトンネルの送信元アドレスとして設定します。

[DeviceA-Tunnel1] source 2.2.2.1

#デバイスBのGE 1/0/2のIPアドレスをトンネルの宛先アドレスとして設定します。

[DeviceA-Tunnel1] destination 2.2.3.1

#IPsecプロファイルをトンネルインターフェースに適用します。

Apply an IPsec profile to the tunnel interface.

[DeviceA-Tunnel1] tunnel protection ipsec profile abc

[DeviceA-Tunnel1] quit

#トンネルインターフェースを通過するデバイスAからデバイスBへのスタティックルートを設定します。

[DeviceA] ip route-static 10.1.2.0 255.255.255.0 tunnel 1

デバイスBのIPsecトンネルインターフェース設定:

#IPsecトンネルインターフェースTunnel1を作成します。

[DeviceB] interface tunnel 1 mode ipsec

#トンネルインターフェースのIPアドレスを設定します。

[DeviceB-Tunnel1] ip address 3.3.3.2 255.255.255.0

#デバイスBのGE 1/0/2のIPアドレスをトンネルの送信元アドレスとして設定します。

[DeviceB-Tunnel1] source 2.2.3.1

#デバイスAのGE 1/0/2のIPアドレスをトンネルの宛先アドレスとして設定します。

[DeviceB-Tunnel1] destination 2.2.2.1

#IPsecプロファイルをトンネルインターフェースに適用します。

[DeviceB-Tunnel1] tunnel protection ipsec profile abc

[DeviceB-Tunnel1] quit

#トンネルインターフェースを通過するデバイスBからデバイスAへのスタティックルートを設定します。

[DeviceB] ip route-static 10.1.1.0 255.255.255.0 tunnel 1

ソリューション

この問題を解決するには、次の手順に従います

1. IP Secトンネルインターフェースの状態がアップであることを確認します。状態がダウンの場合は、トンネル設定の完全性をチェックします。共通のチェック項目には、送信元アドレス、宛先アドレス(コマンド構文のスペルが間違っている可能性があります)、およびトンネルインターフェースのIPアドレスが含まれます。
2. トンネル送信元インターフェースがアップ状態で、トンネル宛先アドレスが到達可能であることを確認します。
3. IP SecとIKEの基本設定が正しいことを確認します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
display ike sa	IKE SA情報を表示します。
display ipsec sa	IP Sec SA情報を表示します。
reset ike sa	IKE SAをクリアします。
reset ipsec sa	IPsec SAをクリアします。
display ip interface brief	インターフェースステート情報を表示します。
display interface Tunnel 1	トンネルステート情報を表示します。
save	実行コンフィギュレーションを指定したファイルに保存します。

ロードバランシングのトラブルシューティングCPU使用率とメモリ使用率が高くなる現象

仮想サーバーでパケット損失が発生するか、NQAオペレーションが失敗します。

ソリューション

この問題を解決するには、次の手順に従います

1. 実サーバーの状態を表示します。CPU使用率が高いと、仮想サーバーでNQA操作の失敗またはパケット損失が発生する可能性があります。
2. メモリ使用率が高いと、新しい要求が廃棄されます。

関連コマンド

コマンド	説明
display virtual-server statistics	仮想サーバーの統計情報を表示します。
display real-server statistics	実サーバーの統計情報を表示します。
debugging lb all	ロードバランシングのすべてのデバッグ機能をイネーブルにします。
debugging lb error	ロードバランシングエラーのデバッグをイネーブルにします。
debugging lb event	ロードバランシングイベントのデバッグをイネーブルにします。
debugging lb fsm	ロードバランシングステートマシンのデバッグをイネーブルにします。
debugging lb packet	ロードバランシングパケットのデバッグをイネーブルにします。

不均等なロードバランシング

症状

ロードバランシングは不均一です。

ソリューション

この問題を解決するには、次の手順に従います

1. ロードバランシングにラウンドロビンアルゴリズムを使用します。
2. LBカードには複数のCPUコアがあります。ロードバランシングはコアごとに実行されます。このため、実サーバー間で接続が不均等に分散される可能性があります。最小接続アルゴリズムまたはランダムを使用してください。
3. 送信元IPアドレスハッシュアルゴリズムを使用している場合は、送信元IPアドレスの数が十分であることを確認します。

4. LBポリシーを設定して、より詳細なトラフィック分類を実現します。

関連コマンド

コマンド	説明
display real-server statistics [**name** *real-server-name*]	実サーバーの統計情報を表示します。
display virtual-server Statistics [**name** *virtual-server-name*]	仮想サーバーの統計情報を表示します。
reset real-server statistics [*real-server-name*]	実サーバーの統計情報をクリアします。
reset virtual-server statistics [*virtual-server-name*]	仮想サーバーの統計情報をクリアします。

システム管理のトラブルシューティング

CPU使用率が高い

症状

デバイスのCPU使用率は依然として60%を超えており、コマンドの実行速度は非常に遅い。

<H3C> display cpu-usage

Slot 1 CPU 0 CPU usage:

13% in last 5 seconds

13% in last 1 minute

13% in last 5 minutes

display cpu-usage history コマンドは、直近 60 分間の CPU 使用率を表示します。

<H3C> display cpu-usage history

100%|

95%|

90%|

85%|

80%|

75%|

70%|

65%|

60%|

55%|

50%|

45%|

40%|

35%|

30%|

25%|

```
 20%|
 15%|
 10%|
  5%|      #
     ----------------------------------------------------------------------------------------------------
   10        20              30              40              50      60  (minutes) cpu-usage (CPU 0)
          last 60 minutes (SYSTEM)
```

ソリューション

この問題を解決するには、次の手順に従います

1. 設定されているルーティングポリシーが多すぎないかどうかを確認します。

設定されたルーティングポリシーを表示し、設定されているルーティングポリシーが多すぎてCPU使用率が高くなっていないかどうかを確認するには、display route-policyコマンドを使用します。

```
<H3C> display route-policy
Route-policy: policy1
permit : 1
if-match cost 10 continue: next node 11
apply comm-list a delete
```

2. トラフィックループが発生したかどうかを確認します。

トラフィックループが発生すると、ネットワークフラップが発生し、大量のプロトコルパケットがCPUに送信されて処理されるため、CPU使用率が高くなる可能性があります。トラフィックループが発生するとブロードキャストが発生する可能性があります。デバイスの多くのポートが大量のトラフィックを処理しなければならず、ポート使用率が90%以上に達する可能性があります。

```
<H3C> display interface GigabitEthernet1/0/2

GigabitEthernet1/0/2 current state: UP
Line protocol current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-e80d-c000 Description:
GigabitEthernet2/6/0/1 Interface
Loopback is not set
Media type is optical fiber, Port hardware type is 1000_BASE_SX_SFP 1000Mbps-
speed mode, full-duplex mode
……
Last clearing of counters: Never
  Peak value of input: 123241940 bytes/sec, at 2013-06-27 14:33:15
  Peak value of output: 80 bytes/sec, at 2013-06-27 14:13:00
  Last 300 second input:  26560 packets/sec 123241940 bytes/sec 99%
  Last 300 second output:  0 packets/sec 80 bytes/sec 0%
……
```

トラフィックループが発生した場合は、次の手順を実行します。

a. リンク接続とポート設定が正しいかどうかを確認します。

b. 接続されたスイッチでSTPがイネーブルになっているかどうか、および設定が正しいかどうかを確認します。

c. ルーティング設定が正しいかどうか、およびルーティングループが存在するかどうかを確認します。

3. パケットが高速転送されているかどうかを確認します。

   display ip fast-forwarding cacheコマンドを実行して、パケットの転送エントリが出力に存在するかどうかを表示します。エントリが存在しない場合、パケットは高速転送されません。

   ```
   <H3C> display ip fast-forwarding cache

   Total number of fast-forwarding entries: 78
   SIP                SPort DIP                DPort Pro Input_If        Output_If
   Flg 40.1.20.2      65535 30.1.2.2           1024  6   Reth4           Reth3          1
   192.168.96.40  53342 192.168.205.33  23            6   GE1/0/0         N/A              1
   30.1.2.2           1024  40.1.20.2          65535 6   Reth3           Reth4          1
   192.168.205.33     23    192.168.96.52      60824 6   InLoop0         GE1/0/0          1
   120.0.0.1          1701  120.0.0.2          1701  17  InLoop0         GE1/0/2.120 1
   40.1.20.2          65529 30.1.2.2           1024  6   Reth4           Reth3          1
   130.2.1.115        1701  130.2.1.1          1701  17  Reth4           N/A            1
   30.1.2.2           1024  40.1.20.2          65533 6   Reth3           Reth4          1
   40.1.20.2          65526 30.1.2.2           1024  6   Reth4           Reth3          1
   50.1.1.2           1024  60.1.1.2           1024  6   Reth1           Tun1           1
   192.168.205.33 37932 192.168.100.53  0             1   InLoop0         GE1/0/0          1
   30.1.2.2           1024  40.1.20.2          65529 6   Reth3           Reth4          1
   30.1.2.2           1024  40.1.20.2          65527 6   Reth3           Reth4          1
   60.1.1.2           1024  50.1.1.2           1024  6   Tun1            Reth1          1
   40.1.20.2          65532 30.1.2.2           1024  6   Reth4           Reth3          1
   ```

   また、コマンドにIPアドレスを入力して、そのIPアドレスを送信元または宛先IPアドレスとして使用するパケットが高速転送されるかどうかを確認することもできます。

   ```
   <H3C> display ip fast-forwarding cache 12.1.1.1
   Total number of fast-forwarding entries: 2
   SIP       Sport     DIP       DPort     Pro       Input_If  Output_If          Flg
   12.1.1.2  49216     12.1.1.1  3784      17        InLoop0   N/A                1
   ```

   問題が解決しない場合は、display cpu-usageコマンドを実行し、コマンド出力とその他の関連情報をテクニカルサポートに提供して分析を依頼します。

4. オブジェクトポリシーまたはACLアクセラレーションがイネーブルになっているかどうかを確認します。

   ```
   #
   object-policy ip EXTERNAL-Local
     rule 0 pass vrf external_vpn
     rule 1 pass vrf 7tgaklptgb9o19babgnm3kbst8
     accelerate
   #
   ```

   アクセラレーションがディセーブルになっているオブジェクトポリシーまたはACLに50を超えるルールがあると、CPU使用率が高くなる可能性があります。display object-policy accelerate summary ipコマンドおよびdisplay acl accelerate summaryコマンドを使用すると、アクセラレーションでイネーブルになっているオブジェクトポリシーおよびACLを表示できます。

5. オブジェクトポリシーのIPアドレスオブジェクトグループが、除外されたIPアドレスまたは不連続なワイルドカードマスクで設定されているかどうかを確認します。

   除外IPアドレスまたは不連続ワイルドカードマスクがIPアドレスオブジェクトグループに設定されている場合は、オブジェクトポリシーアクセラレーションが失敗し、CPU使用率が高くなります。関連する設定を削除する必要があります。

6. NAT444ポートブロックリソースが十分かどうかを確認します。

   NAT444で設定されたネットワークでは、トラフィックのバースト(パケットの送信元ポートは頻繁に変更されますが、送信元と宛先のIPアドレスと宛先ポート番号は変更されません)により、

NAT444ポートリソースが枯渇する可能性があります。

display system internal nat statisticsを実行します。シャーシXスロットX cpu 1 in failedコマンドをプローブビューで使用して、「NAT444 failed to translate port」フィールドなどのカウントが大幅に増加しているかどうかを確認します。

カウントが大幅に増加している場合は、display nat port-block static c 1 s X c 1コマンドを使用して、どのアドレスのマッピングが大量のポートリソースを占有しているかを特定し、そのアドレスが属するNATアドレスグループの設定を調べて、占有されているポートリソースが上限に達しているかどうかを判断します。

ポートリソースの上限に達した場合は、設定を変更し、ポートブロックリソースを増やします。

7. デバイスで大量のブロードキャストまたはマルチキャストパケットが受信されているかどうかを確認します。

display counters rate inbound interfaceコマンドを実行して、受信したブロードキャストまたはマルチキャストパケット数が大幅に増加しているかどうかを確認します。

カウントが大幅に増加している場合は、QoSを使用してパケットをレート制限し、大幅な増加の原因を特定します。

8. トラフィックのバーストが発生するかどうかを確認します。

セキュリティのパケットがセキュリティポリシーによって拒否およびドロップされた場合、CPU使用率が高くなる可能性があります。次のコマンドを実行すると、多数のパケットがドロップされたかどうかを確認できます。

[H3C-probe]display system internal aspf statistics zone-pair ipv4 chassis X slot X cpu 1

[H3C-probe]display system internal ip packet-drop statistics chassis X slot X cpu 1

大量のパケットがドロップされた場合は、次の手順を実行します。

a. 次のコマンドを実行して、パケット特性を確認します。

debug ip packet

debug ip info

debug aspf packet

b. セキュリティポリシーでのパケットの許可、攻撃防止ポリシーの設定、パケット特性に基づくQoSなどのアクションを実行します。

メモリ使用率が高い

症状

カードのメモリ使用率は70%を超えたままです。

カードのメモリ使用量を表示するには、display memory コマンドを使用します。コマンド出力の Total は合計メモリ サイズ、Used は使用済みメモリ サイズ、FreeRatio は空きメモリの比率を示します。

<H3C> display memory slot 2

The statistics about memory is measured in KB: Slot 2:

Total	Used	Free	Shared	Buffers	Cached	FreeRatio	Mem:
	16375408	2514664	13860744	0	1396	177968	84.6%
-/+ Buffers/Cache:		2335300	14040108				
Swap:	0	0	0				

ソリューション

この問題を解決するには、次の手順に従います

1. display process memoryコマンドを複数回実行して、次の操作を行います。

- カード上のすべてのプロセスのメモリ使用量を表示します。
- メモリ使用量が継続的に増加しているプロセスを特定します。

プロセスのメモリ使用量が継続的に増加している場合、そのプロセスにメモリリークが発生する可能性があります。ダイナミックメモリとは、デバイスに動的に割り当てられたヒープメモリのことで、メモリリークが発生すると値が大きくなります。

<H3C> display process memory slot 2

JID	Text	Data	Stack	Dynamic	Name
1	132	700	32	156	scmd
2	0	0	0	0	[kthreadd]
3	0	0	0	0	[migration/0]
4	0	0	0	0	[ksoftirqd/0]
5	0	0	0	0	[watchdog/0]
6	0	0	0	0	[migration/1]
7	0	0	0	0	[ksoftirqd/1]
8	0	0	0	0	[watchdog/1]
9	0	0	0	0	[migration/2]
10	0	0	0	0	[ksoftirqd/2]
11	0	0	0	0	[watchdog/2]
12	0	0	0	0	[migration/3]
13	0	0	0	0	[ksoftirqd/3]
14	0	0	0	0	[watchdog/3]
15	0	0	0	0	[migration/4]
16	0	0	0	0	[ksoftirqd/4]
17	0	0	0	0	[watchdog/4]

…
…

18919	128	76416	64	2240	diagd

……

この出力は、ID 18919のプロセスが最も多くのメモリを使用していることを示しています。

2. display process memory heapコマンドを複数回実行して、次の操作を行います。

- ユーザープロセス18919のヒープメモリ使用状況を表示します。
- メモリ使用量が継続的に増加しているメモリブロックを特定します。

メモリブロックのメモリ使用量が継続的に増加している場合、メモリがリークする可能性があります。

<H3C> display process memory heap job 18919 verbose

Heap usage:

Size	Free	Used	Total	Free Ratio
32	541	39	580	93.3%
48	6	43	49	12.2%
64	534	32499	33033	1.6%

80	538	47	585	92.0%
112	0	534	534	0.0%
128	0	4	4	0.0%
160	0	4	4	0.0%
176	0	4	4	0.0%
256	0	2	2	0.0%
288	0	1	1	0.0%
304	0	1	1	0.0%
336	0	1	1	0.0%
688	0	4	4	0.0%
1184	0	2	2	0.0%
1456	0	2	2	0.0%
1984	0	1	1	0.0%
2032	0	2	2	0.0%
4144	0	1	1	0.0%
13792	1	0	1	100.0%

Large Memory Usage:
Used Blocks : 0
Used Memory(in bytes): 0
Free Blocks : 3
Free Memory(in bytes): 211200
Summary:
Total virtual memory heap space(in bytes) : 2490368 Total physical memory heap space(in bytes) : 2293760 Total allocated memory(in bytes) : 2170560

関連コマンド

コマンド	説明
display cpu-usage	現在のCPU使用率統計情報を表示します。
display cpu-usage history	CPU使用率の履歴統計を座標系で表示します。
display interface	インターフェース情報を表示します。
display memory	メモリ使用状況情報を表示します。
display process memory	カード上の各プロセスのメモリ使用量情報を表示します。
display process memory heap	ユーザープロセスのヒープメモリ使用量を表示します。
displaysysteminternalkernel memory pool	カーネルメモリ割り当て情報を表示します。

SSL VPNのトラブルシューティング

SSL VPN Webインターフェースへのログインの失敗

症状

クライアントはSSL VPNゲートウェイにpingを実行できますが、SSL VPNログインページを開くことはできません。

ソリューション

この問題を解決するには、次の手順に従います

1. PKIドメインがSSLサーバーポリシービューで指定されていることを確認します。

   ```
   [H3C] ssl server-policy XXX
   [H3C-ssl-server-policy-XXX] display this
   #
   ssl server-policy XXX
     pki-domain XXX
   #
   return
   ```

2. CA証明書とローカル証明書がPKIドメインにインポートされていることを確認します。ローカル証明書が、クライアント用の証明書ではなく、CAがサーバーに発行した証明書であることを確認します。

   PKIドメインの証明書情報を表示するには、次のコマンドを使用します。

   ```
   display pki certificate domain XXXX ca
   display pki certificate domain XXXX local
   ```

3. SSL VPNゲートウェイをイネーブルにした後で証明書をインポートするか、SSLサーバーポリシーを変更する場合は、SSL VPNゲートウェイを再度イネーブルにして、設定を有効にする必要があります。

   次のコマンドを順番に実行して、SSL VPNゲートウェイを再度イネーブルにします。

   - **undo service enable**
   - **service enable**

4. 問題が解決しない場合は、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
ssl server-policy*policy-name*	SSLサーバーポリシーを作成し、SSLサーバーポリシービューを開始します。
pki-domain *domain-name*	SSLサーバーポリシーで使用されるPKIドメインを指定します。
display pki certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }	証明書情報を表示します。
sslvpn gateway*gateway-name*	SSL VPNゲートウェイを作成し、SSL VPNゲートウェイビューを開始します。
service enable	SSL VPNゲートウェイをイネーブルにします。

ブラウザからSSL VPNゲートウェイへのログインの失敗

症状

ユーザーはブラウザからSSL VPN Webインターフェースを開くことはできますが、SSL VPNゲートウェイにログインすることはできません。

ソリューション

この問題を解決するには、次の手順に従います

1. SSL VPNゲートウェイのアドレスが到達可能であることを確認します。
   - pingが許可されている場合は、PCからSSL VPNゲートウェイアドレスにpingを実行します。
   - pingが許可されていない場合は、パケットをキャプチャして接続を確認します。
2. SSL VPNゲートウェイ情報を表示して、次のことを確認します。
   - SSL VPNゲートウェイが起動していることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNゲートウェイは起動しています。SSL VPNゲートウェイが起動していない場合は、WebインターフェースからSSL VPNゲートウェイをイネーブルにするか、CLIからSSL VPNゲートウェイビューでservice enableコマンドを実行します。
   - SSL関連の設定が正しいことを確認します。デフォルトでは、デバイスは自己署名証明書。CA署名証明書を使用するには、SSL VPNゲートウェイにSSLサーバーポリシーを適用します。CA署名証明書の使用を取り消すには、SSL VPNゲートウェイに対するSSLサーバーポリシーの適用を取り消します。
   - SSL VPNゲートウェイで使用されているSSLサーバーポリシーが目的のポリシーであることを確認します。

     使用されているSSLサーバーポリシーの設定が編集された場合、またはSSL VPNゲートウェイに別のSSLサーバーポリシーが設定されている場合は、SSL VPNゲートウェイを再度イネーブルにして、新しい設定を有効にします。

     SSL VPNゲートウェイを再度イネーブルにするには、undo service enableコマンドを実行して

からservice enableコマンドを実行します。

次に、SSL VPNゲートウェイ情報の例を示します。

[Device] display sslvpn gateway

Gateway name: gw

Operation state: Up IP:

1.1.1.2 Port: 2000

SSL server policy configured: sslnew SSL server

policy in use: ssl

Front VPN instance: Not configured

3. SSL VPNコンテキスト情報を表示して、次のことを確認します。

- SSL VPNコンテキストがアップしていることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNコンテキストはアップしています。SSL VPNコンテキストがアップしていない場合は、WebインターフェースからSSL VPNコンテキストをイネーブルにするか、CLIからSSL VPNコンテキストビューでservice enableコマンドを実行します。
- SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていることを確認します。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられている場合は、Associated SSL VPN gatewayフィールドにSSL VPNゲートウェイの名前が表示されます。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていない場合は、Webインターフェースから関連付けるか、CLIからSSL VPNコンテキストビューでgatewayコマンドを実行します。

次に、SSL VPNコンテキスト情報の例を示します。

[Device] display sslvpn context

Context name: ctx

Operation state: Up Associated SSL

VPN gateway: gw

SSL client policy configured: sslnew SSL client

policy in use: ssl

4. すべてのサービスモジュールでSSL VPNゲートウェイリスニングアドレスとポートが正しく設定されていること、および各サービスモジュールのリスニングポートがイネーブルになっていることを確認します。

次に、TCPプロキシ情報の例を示します。

<Device> display tcp-proxy slot 1

Local Addr:port Foreign Addr:port State Service type

1.1.1.2:2000 0.0.0.0:0 LISTEN SSLVPN

5. SSL VPNユーザーが正しく設定されていることを確認します。

- ローカルユーザーの場合ローカルユーザーがネットワークアクセスユーザーであり、ユーザーのサービスタイプがSSL VPNであり、ユーザーがリソースグループへのアクセスを許可されており、リソースグループが正しく設定されていることを確認します。
- リモートユーザーの場合リモート認証サーバー上のユーザーのユーザーグループがSSL VPNコンテキストでリソースグループとして設定されていることを確認します。ユーザーグループとリソースグループは同じ名前を使用する必要があります。

6. サーバーとクライアントで証明書認証がイネーブルになっている場合は、サーバーとクライアントに証明書が正しくインストールされていることを確認します。

関連コマンド

コマンド	説明
display tcp-proxy	TCPプロキシに関する簡単な情報を表示します。
display sslvpn context	SSL VPNコンテキスト情報を表示します。
display sslvpn gateway	SSL VPNゲートウェイ情報を表示します。

ブラウザから内部リソースにアクセスできない

症状

ユーザーは、ブラウザからSSL VPNゲートウェイに正常にログインした後、内部リソースにアクセスできません。

ソリューション

この問題を解決するには、次の手順に従います

1. アクセスリソースが次のいずれかの方法で構成されていることを確認します。
   - リソース・リストを構成します。次に例を示します。

     #urlitemという名前のURLアイテムを作成し、URLアイテムにリソースURLを指定します。

     [Device-sslvpn-context-ctxweb1] url-item urlitem

     [Device-sslvpn-context-ctxweb1-url-item-urlitem] url http://20.2.2.2

     [Device-sslvpn-context-ctxweb1-url-item-urlitem] quit

     #SSL VPNコンテキストctxweb1にurllistという名前のURLリストを作成します。

     [Device-sslvpn-context-ctxweb1] url-list urllist

     #URLリストの見出しをwebとして設定します。

     [Device-sslvpn-context-ctxweb1-url-list-urllist] heading web

     #URLリストurllistにURLアイテムurlitemを割り当てます。

     [Device-sslvpn-context-ctxweb1-url-list-urllist] resources url-item urlitem

     [Device-sslvpn-context-ctxweb1-url-list-urllist] quit

     #SSL VPNコンテキストctxweb1に対してresourcegrp1という名前のSSL VPNポリシーグループを作成します。
     URLリストurllistをWebアクセス用のポリシーグループに追加します。

     [Device-sslvpn-context-ctxweb1] policy-group resourcegrp1

     [Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] resources url-list urllist

     [Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] quit
   - ACLまたはURI ACLを設定して内部サーバーへのアクセスを許可し、SSL VPN Webアクセス用のACLを指定します。次に例を示します。

     [Device-sslvpn-context-ctxweb1] policy-group resourcegrp1

     [Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] filter web-access acl 3000
2. SSL VPNゲートウェイが内部リソースに正常にpingできることを確認します。必要に応じて、ピアデバイスに到達するルートを追加します。
3. SSL VPNゲートウェイ情報を表示して、次のことを確認します。

- SSL VPNゲートウェイが起動していることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNゲートウェイは起動しています。SSL VPNゲートウェイが起動していない場合は、WebインターフェースからSSL VPNゲートウェイをイネーブルにするか、CLIからSSL VPNゲートウェイビューでservice enableコマンドを実行します。
- SSL関連の設定が正しいことを確認します。デフォルトでは、デバイスは自己署名証明書。CA署名証明書を使用するには、SSL VPNゲートウェイにSSLサーバーポリシーを適用します。CA署名証明書の使用を取り消すには、SSL VPNゲートウェイに対するSSLサーバーポリシーの適用を取り消します。
- SSL VPNゲートウェイで使用されているSSLサーバーポリシーが目的のポリシーであることを確認します。

  使用されているSSLサーバーポリシーの設定が編集された場合、またはSSL VPNゲートウェイに別のSSLサーバーポリシーが設定されている場合は、SSL VPNゲートウェイを再度イネーブルにして、新しい設定を有効にします。

  SSL VPNゲートウェイを再度イネーブルにするには、undo service enableコマンドを実行してからservice enableコマンドを実行します。

次に、SSL VPNゲートウェイ情報の例を示します。

```
[Device] display sslvpn gateway

Gateway name: gw
Operation state: Up  IP:
1.1.1.2  Port: 2000
SSL server policy configured: sslnew SSL server
policy in use: ssl
Front VPN instance: Not configured
```

4. SSL VPNコンテキスト情報を表示して、次のことを確認します。

- SSL VPNコンテキストがアップしていることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNコンテキストはアップしています。SSL VPNコンテキストがアップしていない場合は、WebインターフェースからSSL VPNコンテキストをイネーブルにするか、CLIからSSL VPNコンテキストビューでservice enableコマンドを実行します。
- SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていることを確認します。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられている場合は、Associated SSL VPN gatewayフィールドにSSL VPNゲートウェイの名前が表示されます。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていない場合は、Webインターフェースから関連付けるか、CLIからSSL VPNコンテキストビューでgatewayコマンドを実行します。

次に、SSL VPNコンテキスト情報の例を示します。

```
[Device] display sslvpn context

Context name: ctx
Operation  state:  Up Associated SSL
VPN gateway: gw
SSL client policy configured: sslnew SSL client
policy in use: ssl
```

5. アップリンクとダウンリンクの両方が正常に動作していることを確認します。アップリンクまたはダウンリンクエラーは、次のいずれかの状況で発生する可能性があります。

- 内部リソースへのルートはSSL VPNゲートウェイに設定されていません。ルート設定のためにデバイスのルーティングテーブルを確認できます。
- 内部サーバーには、SSL VPNゲートウェイに到達するルートがありません。
- アドレス競合が発生した。
- 不適切なPolicy-Based Routing(PBR;ポリシーベースルーティング)が設定されています。

- 不適切なSSL VPNロードバランシングが設定されています。
- デバイスはデュアルアクティブモードで動作します。

  この問題を解決するには、dual-activeモードをactive/standbyモードに変更し、アップリンクインターフェースとダウンリンクインターフェースを冗長インターフェースに変更します。

関連コマンド

コマンド	説明
url-item	URLアイテムを作成してそのビューを表示するか、既存のURLアイテムのビューを表示します。
url-list	URLリストを作成してそのビューに入るか、または既存のURLリストのビューに入ります。
url	URLアイテムのURLを指定します。
heading	URLリストの見出しを設定します。
resources url-item	URLリストにURLアイテムを割り当てます。
policy-group	SSL VPNポリシーグループを作成してそのビューを表示するか、既存のSSL VPNポリシーグループのビューを表示します。
resources url-list	SSL VPNポリシーグループにURLリストを割り当てます。
filter web-access acl	Webアクセスフィルタリングの高度なACLを指定します。
display sslvpn context	SSL VPNコンテキスト情報を表示します。
display sslvpn gateway	SSL VPNゲートウェイ情報を表示します。

INodeクライアントからSSL VPNゲートウェイ情報を取得できない

症状

ユーザーは、ブラウザでSSL VPNゲートウェイのアドレスを入力してもSSL VPN Webインターフェースにアクセスできません。または、ゲートウェイアドレスを入力した後、INodeクライアントがSSL VPNゲートウェイ情報を取得できません。

ソリューション

この問題を解決するには、次の手順に従います

1. SSL VPNゲートウェイのアドレスが到達可能であることを確認します。
   - pingが許可されている場合は、PCからSSL VPNゲートウェイアドレスにpingを実行します。
   - pingが許可されていない場合は、パケットをキャプチャして接続を確認します。
2. SSL VPNゲートウェイ情報を表示して、次のことを確認します。
   - SSL VPNゲートウェイが起動していることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNゲートウェイは起動しています。SSL VPNゲートウェイが起動

していない場合は、WebインターフェースからSSL VPNゲートウェイをイネーブルにするか、CLIからSSL VPNゲートウェイビューでservice enableコマンドを実行します。

- SSL関連の設定が正しいことを確認します。デフォルトでは、デバイスは自己署名証明書。CA署名証明書を使用するには、SSL VPNゲートウェイにSSLサーバーポリシーを適用します。CA署名証明書の使用を取り消すには、SSL VPNゲートウェイに対するSSLサーバーポリシーの適用を取り消します。
- SSL VPNゲートウェイで使用されているSSLサーバーポリシーが目的のポリシーであることを確認します。

  使用されているSSLサーバーポリシーの設定が編集された場合、またはSSL VPNゲートウェイに別のSSLサーバーポリシーが設定されている場合は、SSL VPNゲートウェイを再度イネーブルにして、新しい設定を有効にします。

  SSL VPNゲートウェイを再度イネーブルにするには、undo service enableコマンドを実行してからservice enableコマンドを実行します。

次に、SSL VPNゲートウェイ情報の例を示します。

```
[Device] display sslvpn gateway

Gateway name: gw
Operation state: Up  IP:
1.1.1.2  Port: 2000
SSL server policy configured: sslnew SSL server
policy in use: ssl
Front VPN instance: Not configured
```

3. SSL VPNコンテキスト情報を表示して、次のことを確認します。

- SSL VPNコンテキストがアップしていることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNコンテキストはアップしています。SSL VPNコンテキストがアップしていない場合は、WebインターフェースからSSL VPNコンテキストをイネーブルにするか、CLIからSSL VPNコンテキストビューでservice enableコマンドを実行します。
- SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていることを確認します。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられている場合は、[Associated SSL VPN gateway]フィールドにSSL VPNゲートウェイの名前が表示されます。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていない場合は、Webインターフェースから関連付けるか、CLIからSSL VPNコンテキストビューでgatewayコマンドを実行します。

次に、SSL VPNコンテキスト情報の例を示します。

```
[Device] display sslvpn context

Context name: ctx
Operation  state:  Up Associated SSL
VPN gateway: gw
SSL client policy configured: sslnew SSL client
policy in use: ssl
```

4. すべてのサービスモジュールでSSL VPNゲートウェイリスニングアドレスとポートが正しく設定されていること、および各サービスモジュールのリスニングポートがイネーブルになっていることを確認します。

次に、TCPプロキシ情報の例を示します。

```
<Device> dis tcp-proxy slot 1
Local Addr:port     Foreign  Addr:port        State     Service type
1.1.1.2:2000        0.0.0.0:0                 LISTEN    SSLVPN
```

関連コマンド

コマンド	説明
display tcp-proxy	TCPプロキシに関する簡単な情報を表示します。
display sslvpn context	SSL VPNコンテキスト情報を表示します。
display sslvpn gateway	SSL VPNゲートウェイ情報を表示します。

INodeクライアントからSSL VPNゲートウェイにログインできない

症状

INodeクライアントはSSL VPNゲートウェイ情報を正常に取得しますが、SSL VPNログインは失敗します。

ソリューション

この問題を解決するには、次の手順に従います

1. SSL VPNゲートウェイのアドレスが到達可能であることを確認します。
   - pingが許可されている場合は、PCからSSL VPNゲートウェイアドレスにpingを実行します。
   - pingが許可されていない場合は、パケットをキャプチャして接続を確認します。
2. SSL VPNゲートウェイ情報を表示して、次のことを確認します。
   - SSL VPNゲートウェイが起動していることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNゲートウェイは起動しています。SSL VPNゲートウェイが起動していない場合は、WebインターフェースからSSL VPNゲートウェイをイネーブルにするか、CLIからSSL VPNゲートウェイビューでservice enableコマンドを実行します。
   - SSL関連の設定が正しいことを確認します。デフォルトでは、デバイスは自己署名証明書。CA署名証明書を使用するには、SSL VPNゲートウェイにSSLサーバーポリシーを適用します。CA署名証明書の使用を取り消すには、SSL VPNゲートウェイに対するSSLサーバーポリシーの適用を取り消します。
   - SSL VPNゲートウェイで使用されているSSLサーバーポリシーが目的のポリシーであることを確認します。

     使用されているSSLサーバーポリシーの設定が編集された場合、またはSSL VPNゲートウェイに別のSSLサーバーポリシーが設定されている場合は、SSL VPNゲートウェイを再度イネーブルにして、新しい設定を有効にします。

     SSL VPNゲートウェイを再度イネーブルにするには、undo service enableコマンドを実行してからservice enableコマンドを実行します。

以下は、SSL VPN AC インターフェース構成の例です:

```
[Device] interface SSLVPN-AC 1
[Device-SSLVPN-AC1] ip address 1.1.1.1 24
[Device-SSLVPN-AC1] quit
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] ip-tunnel interface SSLVPN-AC 1
```

[Device-sslvpn-context-ctx] quit

[Device] display interface SSLVPN-AC 1 brief

Brief information on interfaces in route mode: Link: ADM -

administratively down; Stby - standby Protocol: (s) – spoofing

Interface		Link	Protocol	Primary IP	Description
SSLVPN-AC1	UP	UP		1.1.1.1	

3. SSL VPNコンテキスト情報を表示して、次のことを確認します。

- SSL VPNコンテキストがアップしていることを確認します。Operation stateフィールドにUpと表示されている場合、SSL VPNコンテキストはアップしています。SSL VPNコンテキストがアップしていない場合は、WebインターフェースからSSL VPNコンテキストをイネーブルにするか、CLIからSSL VPNコンテキストビューでservice enableコマンドを実行します。
- SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていることを確認します。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられている場合は、[Associated SSL VPN gateway]フィールドにSSL VPNゲートウェイの名前が表示されます。SSL VPNコンテキストがSSL VPNゲートウェイに関連付けられていない場合は、Webインターフェースから関連付けるか、CLIからSSL VPNコンテキストビューでgatewayコマンドを実行します。

次に、SSL VPNコンテキスト情報の例を示します。

[Device] display sslvpn context

Context name: ctx

Operation state: Up Associated SSL

VPN gateway: gw

SSL client policy configured: sslnew SSL client

policy in use: ssl

4. SSL VPN ゲートウェイのリスニング アドレスとポートがすべてのサービス モジュールで正しく設定されていること、および各サービス モジュールのリスニング ポートが有効になっていることを確認します。以下は、TCP プロキシ情報の例です。

<Device> display tcp-proxy slot 1

Local Addr:port	Foreign Addr:port	State	Service type
1.1.1.2:2000	0.0.0.0:0	LISTEN	SSLVPN

5. SSL VPN ACインターフェースが作成され、インターフェースにIPアドレスが設定され、ユーザーのSSL VPNコンテキストでインターフェースが指定されていることを確認します。

次に、SSL VPN ACインターフェースの設定例を示します。

[Device] interface SSLVPN-AC 1

[Device-SSLVPN-AC1] ip address 1.1.1.1 24

[Device-SSLVPN-AC1] quit

[Device] sslvpn context ctx

[Device-sslvpn-context-ctx] ip-tunnel interface SSLVPN-AC 1

[Device-sslvpn-context-ctx] quit

[Device] display interface SSLVPN-AC 1 brief

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby – standby

Protocol: (s) – spoofing

Interface		Link	Protocol	Primary IP	Description
SSLVPN-AC1	UP	UP		1.1.1.1	

6. アドレスプールが設定されており、ユーザーのSSL VPNコンテキストまたは認可リソースグルー

プに指定されていることを確認します。アドレスプールには、SSL VPNゲートウェイのアドレスを含めることはできません。

次に、アドレスプールの設定と適用の例を示します。
[Device] sslvpn ip address-pool name 1.1.1.1 1.1.1.10

[Device] sslvpn context ctx

[Device-sslvpn-context-ctx] ip-tunnel address-pool name mask 24

7. SSL VPNユーザーが正しく設定されていることを確認します。
   - ローカルユーザーの場合ローカルユーザーがネットワークアクセスユーザーであり、ユーザーのサービスタイプがSSL VPNであり、ユーザーがリソースグループへのアクセスを許可されており、リソースグループが正しく設定されていることを確認します。
   - リモートユーザーの場合リモート認証サーバー上のユーザーのユーザーグループがSSL VPNコンテキストでリソースグループとして設定されていることを確認します。ユーザーグループとリソースグループは同じ名前を使用する必要があります。
8. サーバーとクライアントで証明書認証がイネーブルになっている場合は、サーバーとクライアントに証明書が正しくインストールされていることを確認します。
9. INodeクライアントが最新バージョンであることを確認します。

関連コマンド

コマンド	説明
display tcp-proxy	TCPプロキシに関する簡単な情報を表示します。
display sslvpn context	SSL VPNコンテキスト情報を表示します。
display sslvpn gateway	SSL VPNゲートウェイ情報を表示します。
sslvpn ip address-pool	IPv4アドレスプールを作成します。
ip-tunnel address-pool	IPアクセス用のIPv4アドレスプールを指定します。

INodeクライアントから内部リソースにアクセスできない

症状

INodeクライアントからSSL VPNゲートウェイに正常にログインした後、ユーザーは内部リソースにアクセスできません。

ソリューション

この問題を解決するには、次の手順に従います

1. SSL VPN ACインターフェースがセキュリティゾーンに追加され、セキュリティポリシーによって許可されていることを確認します。
2. INodeクライアントに割り当てられたVNICのIPアドレスがセキュリティゾーンに追加され、セキュリティポリシーによって許可されていることを確認します。
3. ACLまたはURI ACLを設定して内部サーバーへのアクセスを許可し、SSL VPN Webアクセス用のACLを指定します。次に例を示します。

[Device-sslvpn-context-ctxip1] policy-group resourcegrp1

[Device-sslvpn-context-ctxip1-policy-group-resourcegrp1] filter web-access acl 3000

4. SSL VPNゲートウェイが内部リソースに正常にpingできることを確認します。必要に応じて、ピアデバイスに到達するルートを追加します。
5. INodeクライアントが最新バージョンであることを確認します。
6. アップリンクとダウンリンクの両方が正常に動作していることを確認します。アップリンクまたはダウンリンクエラーは、次のいずれかの状況で発生する可能性があります。
   - 内部リソースへのルートはSSL VPNゲートウェイに設定されていません。ルート設定のためにデバイスのルーティングテーブルを確認できます。
   - 内部サーバーには、SSL VPNゲートウェイに到達するルートがありません。
   - デバイスはデュアルアクティブモードで動作します。
   - この問題を解決するには、dual-activeモードをactive/standbyモードに変更し、アップリンクインターフェースとダウンリンクインターフェースを冗長インターフェースに変更します。
   - アドレス競合が発生した。
   - 不適切なPolicy-Based Routing(PBR;ポリシーベースルーティング)が設定されています。
   - 不適切なSSL VPNロードバランシングが設定されています。

関連コマンド

コマンド	説明
policy-group	SSL VPNポリシーグループを作成してそのビューを表示するか、既存のSSL VPNポリシーグループのビューを表示します。
filter web-access acl	Webアクセスフィルタリング用の拡張ACLを指定します。

INodeクライアントユーザーのアイドルSSL VPNセッションの終了に失敗する

症状

INodeクライアントユーザーのSSL VPNセッションは、ライセンスリソースを消費して長時間アイドル状態であっても、期限切れになりません。

ソリューション

INodeクライアントユーザーのSSL VPNセッションが期限切れにならないように、INodeクライアントは定期的にキープアライブメッセージを送信します。内部リソースにアクセスしないユーザーを強制的にオフラインにするように、アイドルカット機能を設定できます。

アイドルカット機能は、SSL VPNセッションのアイドルカットトラフィックしきい値を設定します。アイドルタイムアウト時間内に指定したしきい値未満のトラフィックを生成するSSL VPNセッションは終了します。次に、アイドルカットトラフィックしきい値を1000 KBに設定する例を示します。

<Device> system-view

[Device] sslvpn context ctx1

[Device-sslvpn-context-ctx1] idle-cut traffic threshold 1000

関連コマンド

コマンド	説明
sslvpn context	SSL VPNコンテキストを作成してそのビューを開始するか、既存のSSL VPNコンテキストのビューを開始します。
idle-cut traffic-threshold	SSL VPNセッションアイドルカットトラフィックしきい値を設定します。

ユーザーのフィルター、モニター、およびIPバインド設定が有効にならない

症状

SSL VPNユーザーに対するローカルユーザービューのACLフィルタリング、モニタリング、およびIPバインディング設定は有効になりません。

ソリューション

この問題を解決するには、これらの設定をローカルユーザービューではなくSSL VPNコンテキストビューで設定します。これは、一部のSSL VPNユーザー管理設定はSSL VPNコンテキストビューでしか設定できないためです。

関連コマンド

コマンド	説明
sslvpn context	SSL VPNコンテキストを作成してそのビューを開始するか、既存のSSL VPNコンテキストのビューを開始します。

SSL VPNゲートウェイへの再ログインの失敗

症状

以前のログイン成功後に、ユーザーがSSL VPNゲートウェイへの再ログインに失敗しました。

ソリューション

この問題を解決するには、次の手順に従います

1. 各アカウントの同時ログイン数に制限が設定されているかどうかを確認します。この例では、最大数は1に設定されています。

   [Device] sslvpn context ctx

[Device-sslvpn-context-ctx] max-onlines 1

2. このような制限が必要ない場合は、max-onlinesコマンドの設定を削除できます。制限が設定されていて、この制限を削除しない場合は、強制ログアウト機能を有効にできます。ログインが試行されたが、アカウントを使用したログインが最大に達した場合、この機能により、アイドル時間が最も長いユーザーがログアウトされ、新しいログインが許可されます。

   強制ログアウト機能を設定するには、次のコマンドを実行します。

   [Device] sslvpn context ctx

   [Device-sslvpn-context-ctx] force-logout max-onlines enable

関連コマンド

コマンド	説明
sslvpn context	SSL VPNコンテキストを作成してそのビューを開始するか、既存のSSL VPNコンテキストのビューを開始します。
force-logout max-onlines enable	強制ログアウト機能をイネーブルにします。

WeChat Work(またはWeCom)認証の設定の失敗

症状

WeChat Work認証が設定された後、ユーザーがWeChat Work(またはWeCom)クライアントからリソースにアクセスできませんでした。

ソリューション

1. デバイスにDNSサーバーが設定されていることを確認します。
2. 信頼できるSSL証明書がインストールされていることを確認します。
3. WeChat Work認証でイネーブルにされたSSL VPNコンテキストが、SSL VPNゲートウェイに排他的に関連付けられていることを確認します。次に例を示します。

   [H3C]sslvpn context ctx

   [H3C-sslvpn-context-ctx]display this

   sslvpn context ctx

   gateway gw domain sslvpn
4. API サーバー アドレス、会社 ID、アプリの秘密鍵、承認ポリシー グループ フィールド名、ポリシー グループ名など、SSL VPN コンテキストのパラメーターが正しく構成されていることを確認します。認可ポリシー グループを指定する場合、グループ名は WeChat Work 管理プラットフォームでユーザーが所属する組織の ID と同じである必要があります。許可ポリシー グループが指定されていない場合は、デフォルト ポリシー グループを設定する必要があります。

   [H3C]sslvpn context ctx

   [H3C-sslvpn-context-ctx]display this

   sslvpn context ctx gateway gw

   domain sslvpn

   wechat-work-authentication enable

   wechat-work-authentication url https://qyapi.weixin.qq.com

   wechat-work-authentication corp-id ww918e2ea10664acd3

wechat-work-authentication app-secret agZO0L15DmOBw-BBx9s5UmOForvCx-WEtKQWqfBQy Ts

wechat-work-authentication authorize-field department

wechat-work-authentication open-platform-url user-defined https://open.weixin.qq.com

5. WeChat作業管理プラットフォームにログインし、WeChatオープンプラットフォーム上のSSL VPNゲートウェイへのリダイレクトリンクが正しく設定されていることを確認します。

関連コマンド

コマンド	説明
sslvpn context	SSL VPNコンテキストを作成してそのビューを開始するか、既存のSSL VPNコンテキストのビューを開始します。
gateway	SSL VPNコンテキストをSSL VPNゲートウェイに関連付けます。
wechat-work-authentication enable	WeChat Work認証を有効にします。
wechat-work-authentication url	WeChat Work APIサーバーのURLを指定します。
wechat-work-authentication corp-id	WeChat Work認証用の企業IDを指定します。
wechat-work-authentication app-secret	WeChat Work認証用のアプリ秘密鍵を指定します。
wechat-work-authentication authorize-field	許可ポリシーグループフィールドの名前を指定します。
wechat-work-authentication open-platform-url	WeChatオープンプラットフォームURLを指定します。

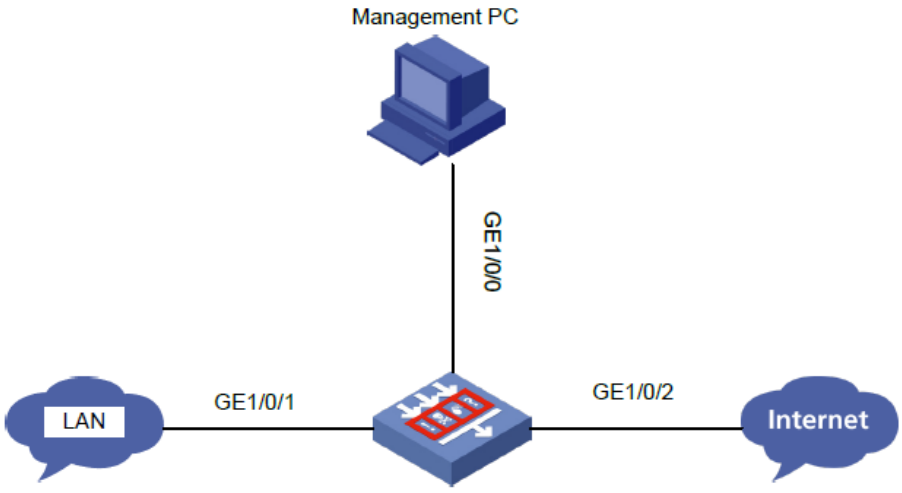
DPIのトラブルシューティング

IPSまたはアンチウイルスが誤って合法的なトラフィックを傍受

症状

IPSまたはアンチウイルスは、LAN上のユーザーを攻撃から保護するためにファイアウォールで設定されます。LAN内のユーザーがインターネットにアクセスできず、ファイアウォールがIPS攻撃ログまたはアンチウイルス攻撃ログを報告します。

図25 ネットワーク図



ファイアウォールの設定:

```
#
app-profile 0_IPv4
 ips apply policy default mode protect
 anti-virus apply policy default mode protect
 #
  security-policy ip
    rule 0 name ips
    action  pass
    profile 0_IPv4
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. IPS攻撃ログまたはアンチウイルス攻撃ログの送信元IPアドレスがユーザーのIPアドレスであり、宛先IPアドレスがサーバーのIPアドレスであることを確認します。ある場合は、IPS攻撃ログまたはアンチウイルス攻撃ログに攻撃IDを記録します。
2. IPSが正しいトラフィックを誤って代行受信した場合は、次のアクションを実行します。
   a. IPSポリシーを作成します。
   b. トラフィックが一致するIPSシグニチャをディセーブルにするか、許可およびロギングするアクションを設定します。
      チェックボックスをオンにします。
   c. ファイアウォールに適用されるセキュリティポリシーでIPSポリシーを指定します。
3. アンチウイルスが誤って正当なトラフィックを傍受した場合は、次のアクションを実行します。
   a. ウイルス対策ポリシーを作成します。
   b. トラフィックが一致するウイルスシグニチャをディセーブルにするか、許可するアクションを設定しウイルスシグニチャのロギング。
   c. ファイアウォールに適用されるセキュリティポリシーでアンチウイルスポリシーを指定します。
4. ホストがサーバーに送信するパケットをキャプチャして、IPSまたはアンチウイルス攻撃ログが誤って生成されたかどうかを識別します。

- 「はい」の場合は、IPSまたはウイルスシグニチャを変更します。
- 一致しない場合は、IPSまたはウイルスシグニチャと一致するユーザーからのトラフィックを許可するようにファイアウォールを設定します。

関連コマンド

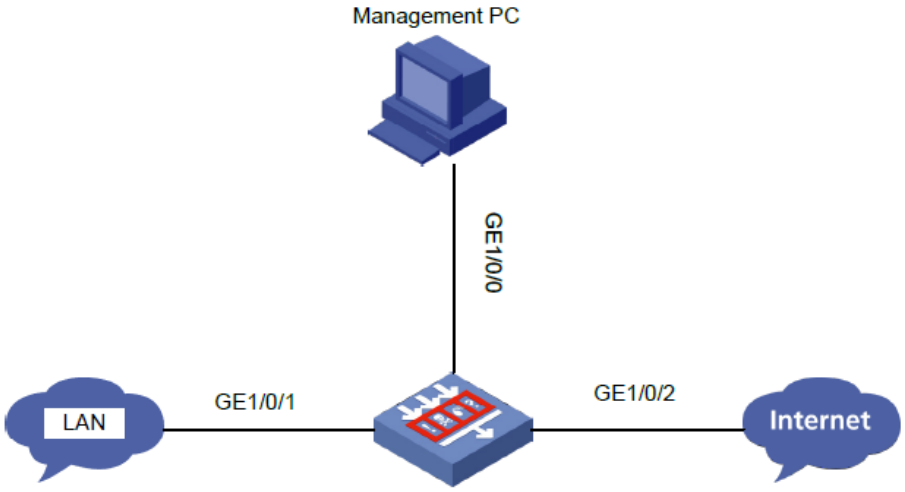
コマンド	説明
ips policy *policy-name*	IPSポリシーを作成してそのビューを表示するか、既存のIPSポリシーのビューを表示します。 デフォルトでは、defaultという名前のIPSポリシーが存在します。デフォルトのIPSポリシーは編集または削除できません。
signature override { **pre-defined** | **user-defined** } *signature-id* { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }	IPSポリシー内のIPSシグニチャのステータスとアクションを変更します。 デフォルトでは、定義済みのIPSシグニチャは、システムによって定義されたアクションとステートを使用します。ユーザー定義のIPSシグニチャは、シグニチャのインポート元であるIPSシグニチャファイルに定義されたアクションとステートを使用します。 デフォルトのIPSポリシーのシグニチャアクションとステータスは変更できません。
anti-viruspolicy *policy-name*	アンチウイルスポリシーを作成してそのビューを表示するか、既存のアンチウイルスポリシーのビューを表示します。 デフォルトでは、defaultという名前のアンチウイルスポリシーが存在します。デフォルトのアンチウイルスポリシーは編集または削除できません。
exception signature *signature-id*	シグニチャをシグニチャ例外として設定します。

IPSまたはWAFが攻撃トラフィックの捕捉や攻撃ログの生成に失敗する

症状

IPSやWAFは、LAN上のユーザーを攻撃から保護するためにファイアウォール上に設定されていますが、攻撃者はインターネットから内部ターゲットサーバーへの攻撃(クロスサイトスクリプト攻撃やブルートフォース攻撃など)を成功させ、サーバーのパスワードを解読することができます。ファイアウォールは攻撃ログを生成しません。

図26 ネットワーク図



ファイアウォールの設定:

```
#
app-profile 0_IPv4
 ips apply policy default mode protect
 waf apply policy default mode protect
 #
  security-policy ip
  rule 0 name ips
 action  pass
  profile 0_IPv4
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. ファイアウォールにIPSまたはWAFのライセンスがインストールされていることを確認します。
2. DPIがデバイス上で正しく動作していることを確認します。

   [H3C] display inspect status Chassis 0

   Slot 1:

   Running status: normal
3. ファイアウォールが最新の IPS 署名ライブラリまたは最新の WAF 署名ライブラリを使用していることを確認します。

   <H3C> display ips signature library

   IPS signature library information:

Type	SigVersion	ReleaseTime	Size
Current	1.0.81	Thu Oct 31 08:35:05 2019	4639264
Last	1.0.80	Sat Oct 12 07:58:23 2019	4565664
Factory	1.0.0	Fri Dec 28 06:27:33 2018	76496

   <H3C>display waf signature library

   WAF signature library information:

Type	SigVersion	ReleaseTime	Size(bytes)
Current	1.0.2	Thu Oct 31 03:22:10 2019	1018752
Last	1.0.0	Fri Dec 28 08:53:30 2018	19824
Factory	1.0.0	Fri Dec 28 08:53:30 2018	19824

4. IPSポリシー設定またはWAFポリシー設定が有効になっていることを確認します。IPSポリシー設定またはWAFポリシー設定は、CLI(inspect activateコマンドを使用)またはWebインターフェースから有効にできます。

[H3C-probe] display system internal inspect dim-rule

Slot 1:

0	2	IPS	TCP	HTTP
0	2147483650	FFILTER	TCP	
0	2147483651	FFILTER	TCP	
0	4	IPS	TCP	HTTP
0	2147483652	FFILTER	TCP	
0	5	IPS	TCP	HTTP

[H3C-probe]display system internal inspect dim-rule | include WAF

0	1	WAF	TCP	HTTP
0	16	WAF	TCP	HTTP
0	37	WAF	TCP	HTTP
0	38	WAF	TCP	HTTP
0	43	WAF	TCP	HTTP

5. ホストとサーバー間で、次の要件を満たすセッションが確立されていることを確認します。

- 送信元IPアドレスと宛先IPアドレスが、指定されたセキュリティゾーンにあります。
- IPSポリシーまたはWAFポリシーWAFポリシーを指定したDPIが有効になっています。

#ホストによって開始されたIPv4ユニキャストセッションに関する情報を表示します。

[H3C] display session table ipv4 source-ip 1.1.1.101 verbose

Slot 1:

Initiator:

Source IP/port: 1.1.1.101/34679

Destination IP/port: 2.2.2.12/5190 DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/- Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/10 Source security zone: Trust

Responder:

Source IP/port: 2.2.2.12/5190

Destination IP/port: 1.1.1.101/34679 DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/- Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/11 Source security zone: Untrust

State: TCP_ESTABLISHED

Application: AOL

Start time: 2016-01-21 16:13:16 TTL: 1194s

Initiator->Responder: 3 packets 930 bytes

Responder->Initiator: 1 packets 92 bytes

Total sessions found: 1

#DPIエンジンインスペクション規則の試合の統計を表示します。

[H3C-probe]display system internal inspect hit-statistics
Slot 1:

Rule ID	Module	Rule hits	AC hits	PCRE try	PCRE hits
5041	APR	0	3	0	0
5126	APR	0	9	0	0
5127	APR	0	9	0	0
8584	IPS	1	2	0	0
9410	APR	0	1	0	0
21768	IPS	0	2	0	0
21852	IPS	1	2	0	0
22114	IPS	0	2	0	0
22406	IPS	1	1	0	0
23089	IPS	2	2	4	2
23213	IPS	0	4	2	2
23271	IPS	0	2	1	0
23341	IPS	1	2	1	1
23722	IPS	2	8	2	2
23804	IPS	0	1	0	0
18096	WAF	0	4	2	0
23311	WAF	1	14	1	1
23791	WAF	0	2	1	0
23915	WAF	0	8	4	0

6. トラフィックヒットがイネーブルになっているIPSシグニチャまたはWAFシグニチャ、およびシグニチャに対してアクションが指定されていることを確認します。

- シグニチャオーバーライドの事前定義8 enableリセットロギングを使用できます。コマンドを使用して、IPSシグニチャをイネーブルにし、シグニチャのアクションを指定します。
- signature override pre-defined pre-defined 56 enable reset loggingコマンドを使用すると、定義済みのWAFシグニチャを有効にし、そのシグニチャに対するアクションを指定できます。

[H3C]display ips signature pre-defined 8

Type : Pre-defined

Signature ID: 8 Status

: Disable

Action : Permit & Logging

Name :(MS11-015)DVR-MS_Vulnerability
Protocol : TCP
Severity : Critical Fidelity
: Medium
Direction : To-client
Category :Vulnerability
Reference : CVE-2011-0042;MS11-015;

[H3C]display waf signature pre-defined 56
Type : Pre-defined
Signature ID: 56 Status
:Disable
Action : Permit & Logging
Name :CVE-2012-3351_LongTail_JW_Player_XSS_Vulnerability Protocol
: TCP
Severity : Medium Fidelity
: Medium Direction
: To-server
Category : Vulnerability
Reference :CVE-2012-3351;

7. 問題が解決しない場合は、IPSシグニチャライブラリまたはWAFシグニチャライブラリが
はこの攻撃をサポートしていません。この場合は、攻撃パケットをキャプチャし、H3Cサポートに連絡してください。

関連コマンド

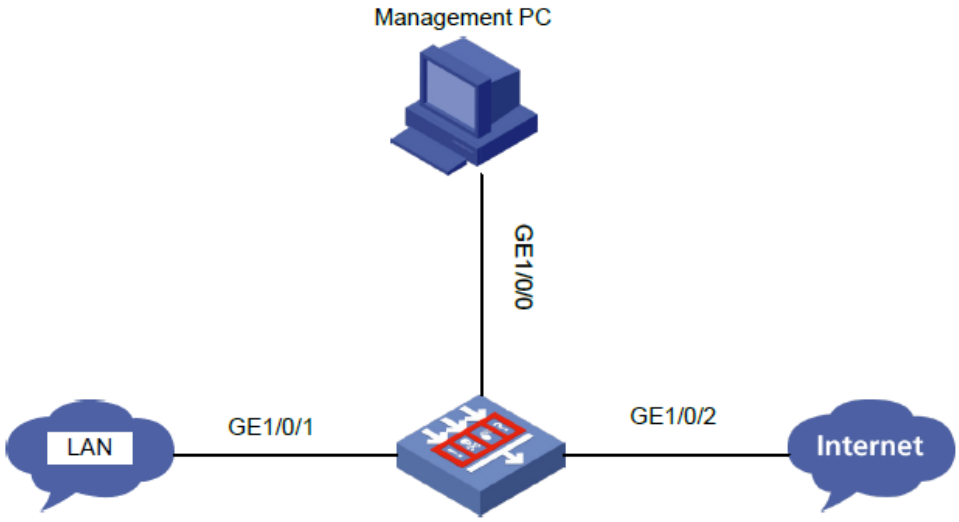
コマンド	説明
ips policy *policy-name*	IPSポリシーを作成してそのビューを表示するか、既存のIPSポリシーのビューを表示します。 デフォルトでは、defaultという名前のIPSポリシーが存在します。デフォルトのIPSポリシーは編集または削除できません。
Waf policy*policy-name*	WAFポリシーを作成して表示するか、既存のWAFポリシーWAFポリシーのビューを表示します。 デフォルトでは、defaultという名前のWAFポリシーが存在します。デフォルトのWAFポリシーの編集や削除はできません。
Signature override { **pre-defined** | **user-defined** } *signature-id* { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }	IPSまたはWAFポリシー内のIPSまたはWAFシグニチャのステータスとアクションを変更します。 デフォルトでは、定義済みのIPSまたはWAFシグニチャは、システムによって定義されたアクションと状態を使用します。ユーザー定義のIPSまたはWAFシグニチャは、シグニチャのインポート元であるIPSまたはWAFシグニチャファイルに定義されたアクションと状態を使用します。 デフォルトのIPSポリシーまたはWAFポリシーでは、シグニチャアクションとステータスを変更できません。
Inspect activate	DPIサービスモジュールのポリシーおよび規則の設定をアクティブにします。 デフォルトでは、DPIサービスポリシーおよび規則の作成、変更、および削除は有効になりません。
Display system internal inspect hit-statistics [*module-id*] [*rule-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]	DPIエンジンインスペクション規則の試合の統計を表示します。
Display inspect status	DPIエンジンのステータスを表示します。

アプリケーションレート制限が有効にならない

症状

Thunderのダウンストリームトラフィックレートを制限するためにファイアウォールで帯域幅管理が設定されていますが、Thunderのダウンストリームトラフィックレートは正しく制限されていません。

図27 ネットワークダイアグラム



ファイアウォールの設定:

```
traffic-policy
 rule 1 name Thunder
   action qos profile Thunder_20M
   source-zone Trust
   destination-zone Untrust
   application app-group 1
   profile name thunder_20m
   bandwidth downstream maximum 20000
   bandwidth upstream maximum
```

ソリューション

この問題を解決するには、次の手順に従います

1. ファイアウォールで最新のAPRシグニチャライブラリが使用されていることを確認します。
   最新のAPRシグニチャライブラリにアクセスし、会社のWebサイトにアクセスしてシグニチャファイルをダウンロードします。
2. DPIエンジンが有効になっていることを確認します。Undo inspect bypassコマンドを使用して、DPIエンジンを有効にできます。
3. アプリケーション監査および管理ポリシー設定がアクティブ化されていることを確認します。
   Inspect activateコマンドを使用して、アプリケーション監査および管理ポリシー設定をアクティブ化できます。

   [H3C-probe] display system internal inspect dim-rule

   Slot 1:

MdcID	MoudleName	Total MD5 rules		
0	Anti-Virus	0		
MdcID	RuleID	ModuleName	L4ProName	uiAppIdL5
1	1	AUDIT	TCP	WECHAT_LOGIN_IOS_TCP_M
0	1	IPS	TCP	HTTP
0	2147483649	FFILTER	TCP	
1	2	AUDIT	TCP	WECHAT_LOGIN_ANDROID_TCP_M
0	2	IPS	TCP	HTTP

0	2147483650	FFILTER	TCP	
1	3	AUDIT	TCP	WECHAT_SENDTEXT_WINDOWS_TCP_M
0	2147483651	FFILTER	TCP	
1	4	AUDIT	TCP	WECHAT_SENDTEXT_IOS_TCP_M
0	4	IPS	TCP	HTTP

4. アプリケーション監査および管理ポリシーが有効になっており、ポリシールールに基づいてトラフィックを処理できることを確認します。Rule move Thunder before bコマンドを使用してトラフィックルールを新しい位置に移動し、ファイアウォールがポリシールールを使用してThunderのダウンストリームトラフィックを処理できるようにします。
5. セッション内のアプリケーションシグニチャがユーザー定義アプリケーショングループに追加され、アプリケーショングループにトラフィックポリシーが適用されていることを確認します。

```
<H3C> display session table ipv4 verbose

Slot 1:
Initiator:
Source   IP/port:  1.1.1.195/51353  Destination
IP/port: 2.2.2.51/59287 DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet1/0/10 Source security
zone: Trust
Responder:
Source              IP/port: 2.2.2.51/59287
Destination IP/port: 1.1.1.195/51353 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet1/0/11 Source security
zone: Untrust
State: TCP_SYN_RECV Application:
GENERAL_TCP
Start time: 2016-01-21 17:51:44  TTL: 951s
Initiator->Responder:            1 packets          56 bytes
Responder->Initiator:            1 packets          56 bytes
```

セッション内のほとんどのアプリケーションがGENERAL_TCPまたはGENERAL_UDPである場合、Thunderに対して新しいシグニチャを定義する必要があることを示します。この場合は、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
traffic-policy	トラフィックポリシービューを開始します。
Rule move *rule-name1* { **after** | **before**}*rule-name2*	トラフィックルールを新しい位置に移動します。

Display traffic-policy statistics bandwidth {**downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name*}	トラフィックルールのトラフィック統計情報を表示します。

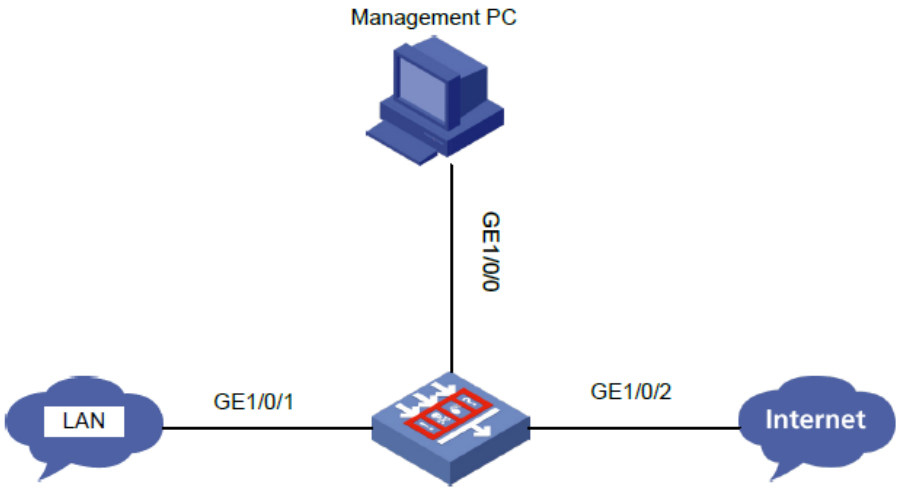
ファイルフィルタリングまたはデータフィルタリングが有効にならない

症状

ファイルフィルタリングは、LANとインターネット間で転送される機密ファイルをブロックしてログに記録するようにファイアウォールで構成されます。ただし、LAN内のユーザーは機密ファイルをインターネットにアップロードでき、ファイアウォールはファイルフィルタリングログを生成しません。

データフィルタリングは、LANとインターネット間で転送されるデータのセキュリティを確保するためにファイアウォールで構成されます。ただし、LAN内のユーザーは、銀行カード番号やIDカード番号などの機密データをインターネットにアップロードできます。データフィルタリングログは生成されません。

図28 ネットワーク図



ファイアウォールの設定:

```
 #
file-filter policy ffilter
 rule ffilter
  filetype-group ffilter
  application all
  direction both
  action drop logging
#
file-filter filetype-group ffilter
 pattern    0  text    pe
 pattern    1  text    elf
```

```
 pattern 10 text vsdx
 pattern 11 text msg
 pattern 12 text pub
 pattern 13 text zip
 pattern 14 text rar
 pattern 15 text tar.gz
 pattern 16 text tgz
 pattern 2 text doc
 pattern 3 text pdf
 pattern 4 text xls
 pattern 5 text ppt
 pattern 6 text docx
 pattern 7 text xlsx
 pattern 8 text pptx
 pattern 9 text vsd
#
data-filter keyword-group dfilter
 pre-defined-pattern name bank-card-number pre-
 defined-pattern name credit-card-number pre-defined-
 pattern name id-card-number
 pre-defined-pattern name phone-number #
data-filter policy dfilter rule dfilter
  keyword-group dfilter
  application all direction both
  action drop logging
#
app-profile 0_IPv4
 file-filter apply policy ffilter
 data-filter apply policy dfilter
 #
security-policy ip
rule 0 name ffilter
action pass
profile 0_IPv4
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. DPIがデバイス上で正しく動作していることを確認します。

   ```
   [H3C] display inspect status
   Chassis 0 Slot 1:
   Running status: normal
   ```

   正常な実行ステータスは、DPIが正常に動作していることを示します。

2. ファイルタイプグループに、転送されたファイルのタイプが含まれていることを確認します。
3. 使用するアプリケーション層プロトコルが、ファイルフィルタリングポリシーのファイルフィルタリング規則またはデータフィルタリングポリシーのデータフィルタリング規則に指定されていることを確認します。ファイルフィルタリング規則またはデータフィルタリング規則は、HTTP、FTP、SMTP、

IMAP、NFS、POP3、RTMPおよびSMBの各プロトコルに適用できます。

4. ファイルフィルタリングポリシー設定またはデータフィルタリングポリシー設定がアクティブになっていることを確認します。

10桁のIDを持つファイルフィルタリング規則は、定義済みのファイルフィルタリング規則です。定義済みのファイルフィルタリングポリシー設定は、CLI(System-viewでinspect activateコマンドを使用)またはWebインターフェースからアクティブにできます。

CLIからデータフィルタリングポリシー設定をアクティブにできます(inspect activateコマンド)、またはWebインターフェースから実行できます。
Command in system view) or from the Web interface.

[H3C-probe] display system internal inspect dim-rule | include FFILTER

```
 23              FFILTER                 TCP

                HTTP 0                  2147483671  FFILTER

                TCP

0               24              FFILTER                 TCP

                FTP 0           2147483672  FFILTER TCP

1               25              FFILTER                 TCP

                SMTP 0          2147483673  FFILTER TCP

1               26              FFILTER                 TCP

                IMAP 0          2147483674  FFILTER TCP

1               27              FFILTER                 TCP

                POP3 0          2147483675  FFILTER TCP

1               28              FFILTER                 TCP

                NFS 0           2147483676  FFILTER TCP

1               29              FFILTER                 TCP             MICROSOFT-DS

1               30              FFILTER                 TCP             RTMP
```

[H3C-probe]display system internal inspect dim-rule | include DFILTER

```
1               24              DFILTER                 TCP             HTTP

1               25              DFILTER                 TCP             FTP-DATA

1               26              DFILTER                 TCP             SMTP
1               27              DFILTER                 TCP             IMAP

1               28              DFILTER                 TCP             POP3

1               29              DFILTER                 TCP             NFS
```

1	30	DFILTER	TCP	MICROSOFT-DS
1	31	DFILTER	TCP	RTMP

5. ホストとサーバー間で、次の要件を満たすセッションが確立されていることを確認します。

- 送信元IPアドレスと宛先IPアドレスが、指定されたセキュリティゾーンにあります。
- ファイルフィルタリングポリシーまたはデータフィルタリングポリシーが指定されたDPIは、セキュリティゾーンで有効になっています。

#ホストによって開始されたIPv4ユニキャストセッションに関する情報を表示します。

```
[H3C-probe] display session table ipv4 source-ip 7.0.1.2 verbose

Slot 2:
Initiator:
  Source          IP/port: 7.0.1.2/50779
  Destination IP/port: 7.0.0.2/80 DS-Lite
  tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
  TCP(6)
  Inbound interface: GigabitEthernet2/0/2 Source
  security zone: Trust
Responder:
  Source          IP/port: 7.0.0.2/80
  Destination IP/port: 7.0.1.2/50779 DS-Lite
  tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
  TCP(6)
  Inbound interface: GigabitEthernet2/0/3 Source
  security zone: Untrust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-15 11:31:01   TTL: 1197s
Initiator->Responder:                7 packets          1073 bytes
Responder->Initiator:                7 packets          2413 bytes

検出されたセッションの合計数:1
```

6. DPIエンジンインスペクション規則の試合の統計を表示します。

```
[H3C-probe]display system  internal  inspect hit-statistics
Slot 2:
```

Rule ID	Module	Rule hits	AC hits	PCRE try	PCRE hits
2147483650	FFILTER	2	2	0	0
2147483657	FFILTER	1	1	0	0
2147483669	FFILTER	2	2	0	0
3432	APR	2	2	0	0

定義済みのファイルフィルタリング規則だけにヒットカウントがある場合、転送されたファイルに誤った拡張子が付いている可能性があります。File-filter false-extension action dropコマンドを使用して、このようなファイルに対して廃棄アクションを設定し、ファイアウォールがファイルをブロックしてログに記録できるかどうかを確認できます。

7. 問題が解決しない場合は、ファイアウォールがファイルのエンコード形式をサポートしていない可能性があります。この場合は、ホストとファイアウォールの間で交換されるパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

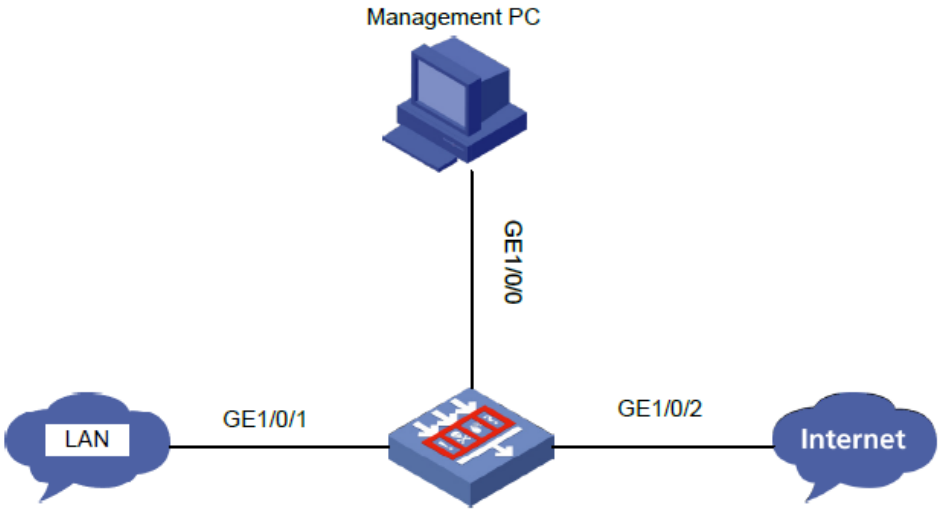
コマンド	説明
file-filter policy *policy-name*	ファイルフィルタリングポリシーを作成してそのビューを表示するか、または既存のファイルフィルタリングポリシーのビューを表示します。 既定では、defaultという名前のファイルフィルタポリシーが存在します。既定のファイルフィルタポリシーは編集または削除できません。
filetype-group *group-name*	ファイルタイプグループをファイルフィルタリング規則に適用します。 デフォルトでは、ファイルフィルタリング規則には次の名前のファイルタイプグループが含まれています。 デフォルト。
inspect activate	DPIサービスモジュールのポリシーおよび規則の設定をアクティブにします。 デフォルトでは、DPIサービスポリシーおよび規則の作成、変更、および削除は有効になりません。
display system internal inspect hit-statistics [*module-id*] [*rule-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]	DPIエンジンインスペクション規則の試合の統計を表示します。
display inspect status	DPIエンジンのステータスを表示します。
file-filter false-extension action { **drop**| **permit** }	偽の拡張子を持つファイルを含むパケットのアクションを設定します。
data-filter apply policy *policy-name*	データフィルタリングポリシーをDPIアプリケーションプロファイルに適用します。 デフォルトでは、データフィルタリングポリシーはDPIアプリケーションプロファイルに適用されません。
data-filter keyword-group *keywordgroup-name*	キーワードグループを作成してそのビューを入力するか、既存のキーワードグループのビューを入力します。

SSL復号化が有効にならない

症状

SSL復号化プロキシポリシーおよびIPSは、LANおよびインターネット上のユーザーにセキュアなHTTPSトランスポートを提供するためにファイアウォールで構成されます。ただし、攻撃者はインターネットから暗号化されたHTTPS攻撃(クロスサイトスクリプト攻撃やブルートフォース攻撃など)を正常に起動し、ターゲットサーバーのパスワードをクラックできます。ファイアウォール上のIPSは攻撃をインターセプトしたり、攻撃ログを生成したりしません。SSL復号化機能は有効になりません。

図29 ネットワーク図



ファイアウォールの設定:

```
#
app-proxy-policy
    rule 1 name ssl-proxy
    action ssl-decrypt
  #
app-profile 0_IPv4
 ips apply policy default mode protect
 #
security-policy ip
rule 0 name ips
 action pass
profile 0_IPv4
#
```

ソリューション

1. ファイアウォールが暗号化されていないHTTPトラフィックをインターセプトできることを確認します。

   ファイアウォールが暗号化されていないHTTPトラフィックの傍受に失敗した場合は、「IPSまたはWAFが攻撃トラフィックの傍受または攻撃ログの生成に失敗する」に従って解決してください。

   ファイアウォールが暗号化されていないHTTPトラフィックをインターセプトできる場合は、次の手順に進みます。

2. ファイアウォールがSSLプロキシを実装できることを確認します。

   ```
   [H3C]display app-proxy server-certificate
   Slot 1:
   Total server certificates: 1
   Certificate info: BreakingPoint_serverA_2048.server.int Proxy count: 6996
   Most recent proxy time: 2019/11/18 10:23:48 First proxy at:
   2019/11/15 17:21:12
   ```

3. ネットワークがレイヤ3ネットワークであることを確認します。現在のソフトウェアバージョンでは、SSL復号化はレイヤ2ネットワークでサポートされていません。

4. DPIがデバイス上で正しく動作していることを確認します。

[H3C] display inspect status

Chassis 0 Slot 1:

Running status: normal

正常な実行ステータスは、DPIが正常に動作していることを示します。

5. HTTPSサーバーがユーザー定義のSSLホスト名ホワイトリストにないことを確認します。

[H3C] display app-proxy ssl whitelist hostname predefined

Chrome HSTS-defined hostnames:

status	Hostname
enabled	2mdn.net
enabled	accounts.firefox.com
enabled	aclu.org
enabled	activiti.alfresco.com
enabled	adamkostecki.de enabled
	addvocate.com
enabled	adsfund.org
enabled	aie.de

...

<H3C> display app-proxy ssl whitelist ip all

Slot 1:

IP address	Port
9.9.9.5	443
9.9.9.6	443
9.9.9.7	443
9.9.9.8	443
9.9.9.9	443
9.9.9.10	443
9.9.9.11	443
9.9.9.12	443

HTTPサーバーがホワイトリストに含まれている場合は、次のコマンドを使用して、ユーザー定義のSSLホスト名ホワイトリストからサーバーのホスト名を削除します。

[H3C] undo app-proxy ssl whitelist user-defined-hostname

<H3C> reset app-proxy ssl whitelist ip

[H3C] app-proxy ssl whitelist activate

6. トラフィックがカード間で転送されないことを確認します。SSL復号化はサポートされていません
カード間トラフィックを復号化する。

<H3C>display session table ipv4 source-ip 7.0.1.2 verbose

Slot 1:

Initiator:

Source IP/port: 7.0.1.2/55933

Destination IP/port: 8.8.8.2/443 DS-Lite

tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/- Protocol:

TCP(6)

Inbound interface: GigabitEthernet2/0/2 Source security

zone: Trust

Responder:

Source IP/port: 8.8.8.2/443
Destination IP/port: 7.0.1.2/55933

DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: Reth1 Source
security zone: Trust
State: INACTIVE
Application: HTTPS Rule
ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43 TTL: 299s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:
Source IP/port: 7.0.1.2/55852
Destination IP/port: 8.8.8.2/80 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet2/0/2 Source security
zone: Trust
Responder:
Source IP/port: 8.8.8.2/80
Destination IP/port: 7.0.1.2/55852 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol: TCP(6)
Inbound interface: Reth1 Source
security zone: Trust
State: INACTIVE
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:02 TTL: 257s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:
Source IP/port: 7.0.1.2/55932
Destination IP/port: 8.8.8.2/443 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol: TCP(6)
Inbound interface: GigabitEthernet2/0/2 Source security
zone: Trust
Responder:
Source IP/port: 8.8.8.2/443
Destination IP/port: 7.0.1.2/55932

DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:

TCP(6)
Inbound interface: Reth1 Source
security zone: Trust
State: INACTIVE
Application: HTTPS Rule
ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43 TTL: 299s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0

bytes Total sessions found: 3

Slot 2:
Initiator:
Source IP/port: 7.0.1.2/55933
Destination IP/port: 8.8.8.2/443 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet2/0/2 Source security
zone: Trust
Responder:
Source IP/port: 8.8.8.2/443
Destination IP/port: 7.0.1.2/55933 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol: TCP(6)
Inbound interface: Reth1 Source
security zone: Trust
State: TCP_TIME_WAIT
Application: HTTPS Rule
ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43 TTL: 0s
Initiator->Responder: 6 packets 776 bytes
Responder->Initiator: 7 packets 899 bytes

Initiator:
Source IP/port: 7.0.1.2/55852
Destination IP/port: 8.8.8.2/80 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet2/0/2 Source security
zone: Trust
Responder:
Source IP/port: 8.8.8.2/80
Destination IP/port: 7.0.1.2/55852 DS-Lite
tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: Reth1 Source
security zone: Trust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:02 TTL: 1157s
Initiator->Responder: 8 packets 1256 bytes
Responder->Initiator: 9 packets 3456 bytes

Initiator:
Source IP/port: 7.0.1.2/55932
Destination IP/port: 8.8.8.2/443 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet2/0/2 Source security
zone: Trust
Responder:
Source IP/port: 8.8.8.2/443
Destination IP/port: 7.0.1.2/55932 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol: TCP(6)
Inbound interface: Reth1 Source
security zone: Trust
State: TCP_TIME_WAIT
Application: HTTPS Rule
ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43 TTL: 1s
Initiator->Responder: 7 packets 816 bytes
Responder->Initiator: 7 packets 899
bytes Total sessions found: 3

7. 問題が解決しない場合は、ファイアウォールがこの問題に対する防御をサポートしていない可能性があります。
この場合、ホストとファイアウォールの間で交換されるパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

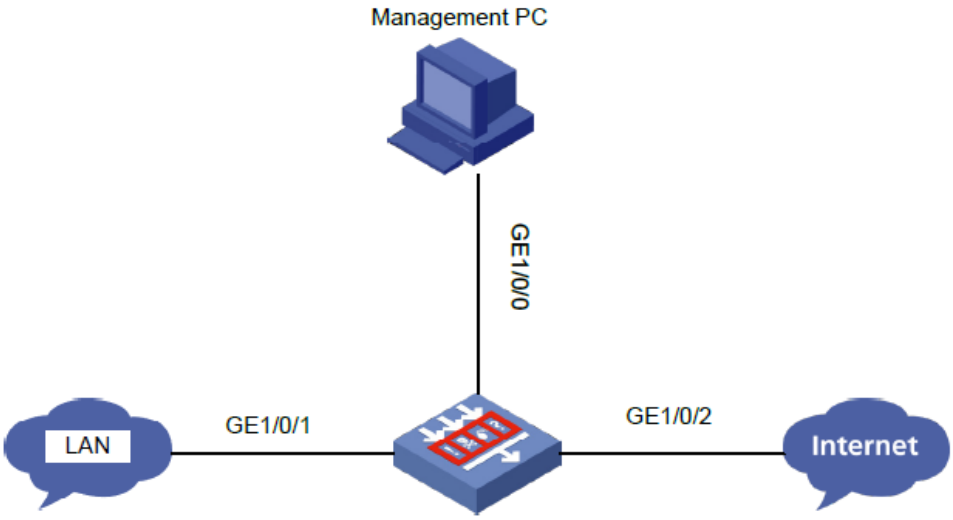
コマンド	説明
app-proxy-policy	プロキシポリシービューを開始します。
app-proxy ssl whitelist user-defined-hostname ***host-name***	ユーザー定義のSSLホスト名ホワイトリストにホスト名を追加します。 サーバー証明書のDNS名(DNS Name)またはCommon Nameの値にSSLホスト名ホワイトリストのホスト名が含まれている場合、デバイスはそのサーバー宛てのSSL接続をプロキシしません。
display app-proxy ssl whitelist ip { all | ***ip-address*** **}**	SSL IPアドレスのホワイトリストを表示します。
display inspect status	DPIエンジンのステータスを表示します。

アプリケーションの監査と管理が有効にならない

症状

アプリケーションの監査と管理は、LANとインターネット間で転送されるデータのセキュリティを確保するためにファイアウォール上で構成されます。ただし、ユーザーは監査ポリシーによって拒否されると想定される機密性の高い動作(ファイル転送やログインなど)を正常に実行でき、ファイアウォールは監査ログを生成しません。

図30 ネットワーク図



ファイアウォールの設定:

```
#
uapp-control
 policy name default audit
  rule 1 app-category IM behavior FileTransfer bhcontent any keyword include any
  action deny audit-logging
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. デバイスが最新のAPRシグニチャライブラリを使用していることを確認します。
   最新のAPRシグニチャライブラリにアクセスし、会社のWebサイトにアクセスしてシグニチャファイルをダウンロードします。
2. DPIエンジンが有効になっていることを確認します。undo inspect bypassコマンドを使用して、DPIエンジンを有効にできます。
3. アプリケーション監査および管理ポリシー設定がアクティブになっていることを確認します。アプリケーション監査および管理ポリシー設定は、CLI(System-viewでinspect activateコマンドを使用)またはWebインターフェースからアクティブにできます。

   [H3C-probe] display system internal inspect dim-rule

   Slot 1:

   MdcID MoudleName Total MD5 rules 0
   0 Anti-Virus

MdcID	RuleID	ModuleName	L4ProName	uiAppIdL5
1	1	AUDIT	TCP	WECHAT_LOGIN_IOS_TCP_
M 0	1	IPS	TCP	HTTP
0	2147483649	FFILTER	TCP	
1	2	AUDIT	TCP	WECHAT_LOGIN_AND ROID_TCP_
M 0	2	IPS	TCP	HTTP
0	2147483650	FFILTER	TCP	
1	3	AUDIT	TCP	WECHAT_SENDTEXT_ WINDOWS_TCP_M
0	2147483651	FFILTER	TCP	
1	4	AUDIT	TCP	WECHAT_SENDTEXT_ IOS_TCP_M
0	4	IPS	TCP	HTTP

4. アプリケーション監査および管理ポリシーがイネーブルになっており、ポリシー規則に基づいてトラフィックを処理できることを確認します。
5. ホストとサーバー間で、次の要件を満たすセッションが確立されていることを確認します。
   - 送信元IPアドレスと宛先IPアドレスが、指定されたセキュリティゾーンにあります。
   - アプリケーション監査および管理ポリシーが指定されたDPIは、セキュリティゾーンで有効になっています。

   [H3C-probe]display session table ipv4 source-ip 7.0.1.2 verbose

   Slot 2:

Initiator:
Source IP/port: 7.0.1.2/50779
Destination IP/port: 7.0.0.2/80 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet2/0/2 Source security
zone: Trust
Responder:
Source IP/port: 7.0.0.2/80
Destination IP/port: 7.0.1.2/50779 DS-Lite
tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
TCP(6)
Inbound interface: GigabitEthernet2/0/3 Source security
zone: Untrust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-15 11:31:01 TTL: 1197s
Initiator->Responder: 7 packets 1073 bytes
Responder->Initiator: 7 packets 2413 bytes

Total sessions found: 1

6. 問題が解決しない場合は、ファイアウォールがこのアプリケーションの監査をサポートしていない可能性があります。この場合は、ホストとファイアウォールの間で交換されるパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

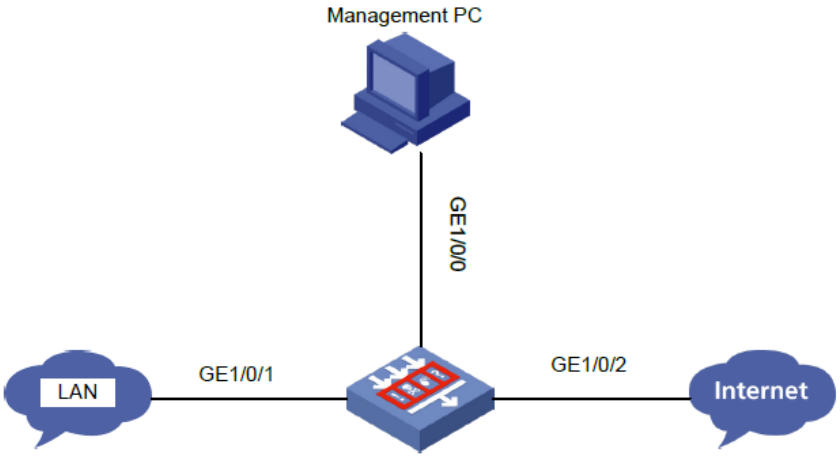
コマンド	説明
inspect activate	DPIサービスモジュールのポリシーおよび規則の設定をアクティブにします。 デフォルトでは、DPIサービスポリシーおよび規則の作成、変更、および削除は有効になりません。
display inspect status	DPIエンジンのステータスを表示します。

URLフィルタリングが有効にならない

症状

URLフィルタリングは、LANユーザーからインターネットへのWebアクセスを制限するためにファイアウォールで構成されています。ただし、ユーザーは潜在的に有害なWebサイト(ポルノWebサイトなど)にアクセスでき、ファイアウォールはURLフィルタリングログを生成しません。

図31 ネットワーク図



ファイアウォールの設定:

```
#
url-filter policy url
 default-action permit logging
 category Pre-Botnet action reset logging
 category Pre-ChildAbuse action reset logging
 category Pre-CriminalActivity action reset logging
 category Pre-Discrimination action reset logging
 category Pre-Divining action reset logging
 category Pre-Drugs action reset logging
 category Pre-Gamble action reset logging
 category Pre-Hacking action reset logging
 category Pre-IllegalSoftware action reset logging
 category Pre-Lottery action reset logging
 category Pre-MaliciousURL action reset logging
 category Pre-Phishing action reset logging
 category Pre-Pornography action reset logging
 category Pre-Religion action reset logging
 category Pre-SchoolCheating action reset logging
 category Pre-Spam action reset logging
 category Pre-Suicide action reset logging
 category Pre-Violence action reset logging
#
app-profile 0_IPv4
 url-filter apply policy url
 #
security-policy ip
rule 0 name url
action pass
counting enable
profile 0_IPv4
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. デバイスが最新のURLフィルタリングシグニチャライブラリを使用していることを確認します。最新のURLフィルタリングシグニチャライブラリをインストールするには、会社のWebサイトにアクセスし、シグニチャファイルをダウンロードします。
2. DPIエンジンが有効になっていることを確認します。undo inspect bypassコマンドを使用して、DPIエンジンを有効にできます。
3. アクセスしたWebページがHTTPSで暗号化されたWebページであることを確認します。ある場合は、ファイアウォールでSSL復号化を有効にします。
4. URLフィルタリングポリシー設定がアクティブになっていることを確認します。URLフィルタリングポリシー設定は、CLI(システムビューでinspect activateコマンドを使用)またはWebインターフェースからアクティブにできます。

   [H3C-probe] display system internal inspect dim-rule

   Slot 1:

MdcID	MoudleName	Total MD5 rules
0	Anti-Virus	0

MdcID	RuleID	ModuleName	L4ProName	uiAppIdL5
0	356581376	UFLT	TCP	HTTP
0	268435456	UFLT	TCP	HTTP
0	356646912	UFLT	TCP	HTTP
0	268435457	UFLT	TCP	HTTP
0	431030273	UFLT	TCP	HTTP
0	384958465	UFLT	TCP	HTTP
0	2147483649	FFILTER	TCP	
0	447873026	UFLT	TCP	HTTP
0	268435458	UFLT	TCP	HTTP

5. ホストとサーバー間で、次の要件を満たすセッションが確立されていることを確認します。
   - 送信元IPアドレスと宛先IPアドレスが、指定されたセキュリティゾーンにあります。

   URLフィルタリングポリシーが指定されたDPIは、セキュリティゾーンで有効になっています。

   [H3C-probe]display session table ipv4 source-ip 7.0.1.2 verbose

   Slot 2:

   Initiator:

   Source IP/port: 7.0.1.2/50779

   Destination IP/port: 7.0.0.2/80 DS-Lite

   tunnel peer: -

   VPN instance/VLAN ID/Inline ID: -/-/- Protocol:

   TCP(6)

```
  Inbound interface: GigabitEthernet2/0/2 Source
  security zone: Trust
Responder:
  Source            IP/port: 7.0.0.2/80
  Destination IP/port: 7.0.1.2/50779 DS-Lite
  tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/- Protocol:
  TCP(6)
  Inbound interface: GigabitEthernet2/0/3 Source
  security zone: Untrust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-15 11:31:01   TTL: 1197s
Initiator->Responder:              7 packets          1073 bytes
Responder->Initiator:              7 packets          2413 bytes

Total sessions found: 1
```

6. ユーザーがアクセスするURLが、ユーザー定義のURLカテゴリと正確に一致していることを確認します。

7. 問題が解決しない場合は、WebサイトのURLがURLフィルタリングシグニチャライブラリに含まれていない可能性があります。この場合は、ホストとファイアウォールの間で交換されるパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

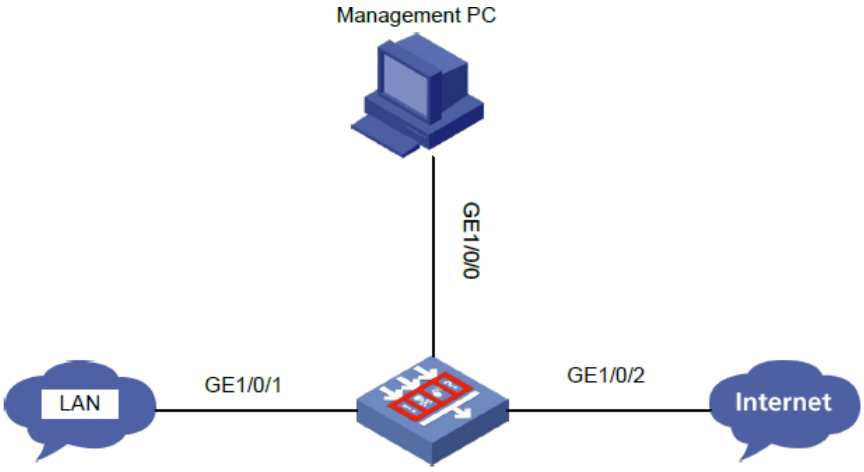
コマンド	説明
url-filter apply policy *policy-name*	URLフィルタリングポリシーをDPIアプリケーションプロファイルに適用します。 デフォルトでは、DPIアプリケーションプロファイルにURLフィルタリングポリシーは適用されません。
inspect activate	DPIサービスモジュールのポリシーおよび規則の設定をアクティブにします。 デフォルトでは、DPIサービスポリシーおよび規則の作成、変更、および削除は有効になりません。
display inspect status	DPIエンジンのステータスを表示します。

サーバー接続検出が有効にならない

症状

保護されたサーバーによって開始された不正な接続をブロックしてログに記録するために、サーバー接続検出(SCD)がファイアウォールに構成されています。ただし、ファイアウォールはこのような接続を識別してログに記録できません。

図32 ネットワーク図



ファイアウォールの設定:

```
#
scd policy name default-7.0.0.2
protected-serv er 7.0.0.2
logging enable
policy enable
rule 1
  permit-dest-ip 7.0.0.255
  protocol udp port 137 to 138
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. ファイアウォール上のSCDに対して高速ログ出力が無効になっていることを確認します。

   高速ログ出力とsyslog出力は相互に排他的です。SCDログ(syslog)を出力するには、SCDの高速ログ出力を無効にします。
2. 次の条件が存在することを確認します。
   - SCDポリシーが使用可能になり、ポリシー内の保護されたサーバーによって開始された不正な接続のロギングが使用可能になりました。
   - 不正な接続のソースIPアドレスが保護されたサーバーのIPアドレスと一致します。不正な接続の宛先IPアドレスは、SCDポリシー内のルールの宛先IPアドレス基準と一致します。

```
<H3C> display scd policy
Id      Name                Protected server        Rules     Logging      Policy status
1       12                  1.2.2.3                 1         Enabled      Enabled
2       default-7.0.0.2     7.0.0.2                 1         Enabled      Enabled
```

3. すべてのセキュリティ・ポリシー・ルールに対してトラフィックの一致順序を確認します。ファイアウォールが、他のポリシーではなくSCDポリシーに基づいて、不正な接続のトラフィックを処理していることを確認します。
4. 問題が解決しない場合は、ファイアウォールがこのタイプのトラフィックの識別をサポートしていない可能性があります。この場合は、ホストとサーバー間で交換されたパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

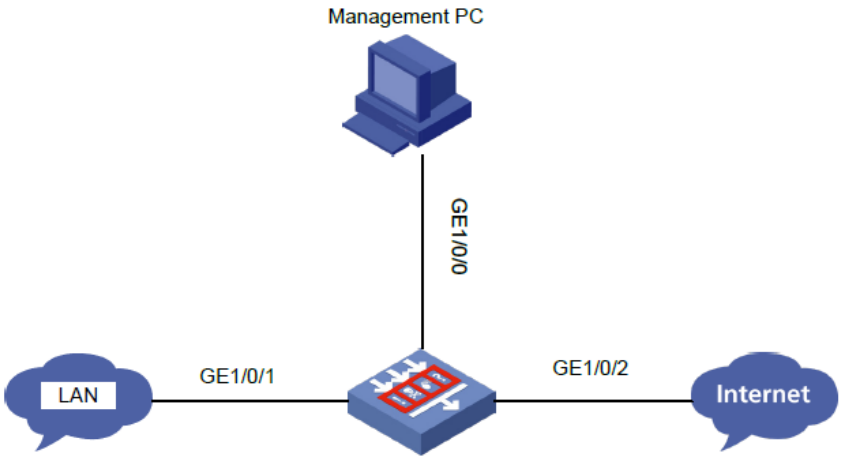
コマンド	説明
scd policy name*policy-name*	SCDポリシーを作成してそのビューを入力するか、既存のSCDポリシーのビューを入力します。
Display scd policy [**name** *policy-name*]	SCDポリシー情報を表示します。

IPレピュテーションが有効にならない

症状

IPレピュテーションは、評判の悪いIPアドレスからの攻撃を防止するためにファイアウォールで設定されます。ただし、IPレピュテーションリストにあるIPアドレスのインターネットユーザーはローカルユーザーと正常に通信でき、ファイアウォールはIPレピュテーションログを生成しません。

図33 ネットワーク図



ファイアウォールの設定:

```
#
ip-reputation

global enable
 top-hit-statistics enable
 attack-category        1    action    deny   logging     enable
```

```
attack-category        2   action   deny   logging    disable
attack-category        3   action   deny   logging    enable
attack-category        4   action   deny   logging    enable
attack-category        5   action   deny   logging    enable
attack-category        6   action   deny   logging    enable
attack-category        7   action   deny   logging    enable
attack-category        8   action   deny   logging    enable
attack-category        9   action   deny   logging    enable
attack-category       10 action     deny     logging   enable
attack-category       11 action    deny     logging   enable
attack-category       12  action     deny     logging    enable
attack-category       13  action     deny     logging    enable
attack-category       14  action     deny     logging    enable
attack-category       15  action     deny     logging    enable
attack-category       16  action     deny     logging    enable
attack-category       17  action     deny     logging    enable
attack-category       18  action     deny     logging    enable
attack-category       19  action     deny     logging    enable
attack-category       20  action     deny     logging    enable
attack-category       21  action     deny     logging    enable
attack-category       22  action     deny     logging    enable
#
```

ソリューション

この問題を解決するには、次の手順に従います

1. ファイアウォールにIPレピュテーションのライセンスがインストールされていることを確認します。
2. インターネットユーザーのIPアドレスが、IPレピュテーションの例外IPアドレスとして設定されていないことを確認します。
3. IPアドレスの攻撃カテゴリに一致するパケットに対して実行するアクションとしてdenyが指定されており、その攻撃カテゴリに対してロギングがイネーブルになっていることを確認します。

   ```
   [H3C-ip-reputation] display  ip-reputation attack-category

   Attack id              Attack name                  Action        Logging
   ---------------------------------------------------------------------------
   1                      C&C                          deny          enable
   2                      Network_Worm                 deny          disable
   3                      Risk_Software                deny          enable
   4                      Malware                      deny          enable
   5                      Trojan                       deny          enable
   6                      Infectious_Virus             deny          enable
   ```

4. 問題が解決しない場合は、インターネットユーザーのIPアドレスがIPレピュテーションライブラリに含まれていない可能性があります。この場合は、ホストとサーバー間で交換されるパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

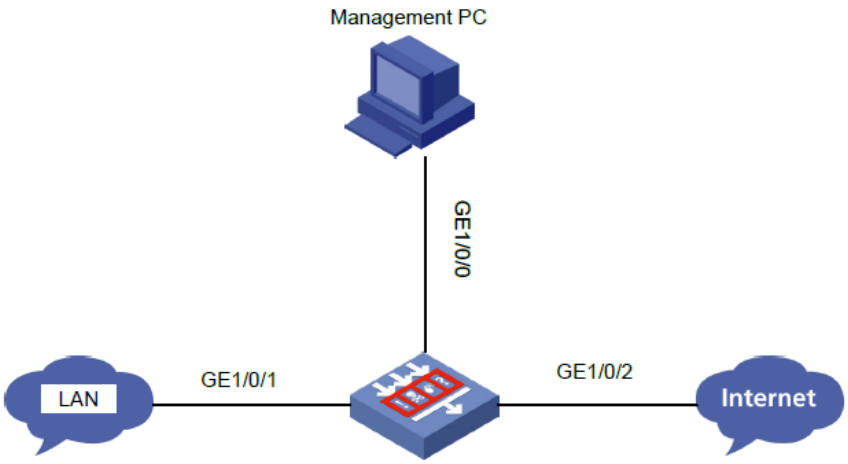
コマンド	説明
display ip-reputation attack-category	IPレピュテーションの攻撃カテゴリに関する情報を表示します。 攻撃カテゴリのアクションを指定しない場合は、事前定義されたアクションが表示されます。
display ip-reputation exception	例外IPアドレスを表示します。 このコマンドは、IPレピュテーションがイネーブルになっている場合に、例外IPアドレス(存在する場合)を表示します。

データ分析センターがログの表示または更新に失敗する

症状

DPIサービスは、LANとインターネット間で転送される情報のセキュリティを確保するためにファイアウォール上で構成されます。データ分析センターは、集中分析およびレポート作成のために様々なサービスからログデータを収集するように構成されます。ただし、データ分析センターは、DPIサービス用に生成されたログを表示できないか、ログをリフレッシュできません。

図34 ネットワークダイアグラム



ファイアウォールの設定:

```
#
app-profile 0_IPv4
 ips apply policy default mode protect
 data-filter apply policy default
 url-filter apply policy default
 file-filter apply policy default
 anti-virus apply policy default mode protect
 #
security-policy ip
rule 0 name 1
```

action pass
profile 0_IPv4
source-zone Trust
source-zone Untrust
destination-zone Trust
destination-zone Untrust
#

ソリューション

この問題を解決するには、次の手順に従います

1. DPIがデバイス上で正しく動作していることを確認します。

   [H3C] display inspect status

   Chassis 0 Slot 1:
   Running status: normal

2. DPIエンジンインスペクション規則の試合の統計を表示します。

   [H3C-probe]display system internal inspect hit-statistics

   Slot 1:

Rule ID	Module	Rule hits	AC hits	PCRE try	PCRE hits
0	FFILTER	0	78225	0	0
0	DFILTER	0	545415	0	0
1	FFILTER	0	78225	0	0
1	DFILTER	0	545415	0	0
2	FFILTER	52341	78225	52341	52341
2	DFILTER	0	545415	0	0
3	FFILTER	0	78225	0	0
3	DFILTER	0	545415	0	0
4	FFILTER	25884	78225	25884	25884
4	DFILTER	0	545415	0	0
2147483652	FFILTER	359139	359139	0	0
5	FFILTER	0	78225	0	0
5	DFILTER	0	545415	0	0
2147483653	FFILTER	9	9	0	0
6	FFILTER	0	78225	0	0
6	DFILTER	0	545415	0	0
2147483654	FFILTER	207554	207554	0	0
7	FFILTER	0	78225	0	0
7	DFILTER	0	545415	0	0
2147483656	FFILTER	159715	159715	0	0
2147483657	FFILTER	985048	985048	0	0

3. 一定時間待って、ファイアウォールがログを生成するかどうかを確認します。
4. ファイアウォールとローカルPCの時刻が一致していることを確認します。システム時刻は、CLI(clock datetimeコマンド)またはWebインターフェースから変更できます。

   <H3C> display clock

   18:37:21 UTC Tue 11/26/2019

5. ファイアウォールで、ソフトウェア高速転送用のセッション統計収集が有効になっていることを確認します。この機能を有効にするには、session statistics enableコマンドを使用できます。フロー・ログなどの一部のタイプのログを出力するには、この機能を有効にする必要があります。

6. ファイアウォールで、css、gif、ico、jpg、js、png、swfおよびxmlなどの定義済リソースタイプのリソースへのアクセスのURLフィルタリンロギングが有効になっていることを確認します。定義済{css gif ico jpg js pngを除くundo url-filterログを使用できます。
swf xml}コマンドを使用して、これらのリソースタイプのURLフィルタリングロギングを有効にします。
7. 記憶域時間制限、記憶域スペース使用制限および記憶域制限トリガーアクションが各サービスに適切に設定されていることを確認します。設定を設定するには、dac storage service service-type service-name limit{hold-タイムタイム-value usage usage-value action{delete log-only}}コマンドを使用します。デフォルト設定に戻すことができます。
8. 問題が続く場合は、ntopdプロセスに例外があることを示している可能性があります。この場合は、交換されたパケットをキャプチャしてから、H3Cサポートに連絡してください。

関連コマンド

コマンド	説明
url-filter log except pre-defined {**css**|**gif**|**ico**|**jpg**|**js**|**png** | **swf** | **xml** }	定義済みリソースタイプのリソースにアクセスするためのURLフィルタリングロギングをディセーブルにします。
session statistics enable	ソフトウェア高速転送のセッション統計収集を有効にします。
display inspect status	DPIエンジンのステータスを表示します。
dac storage service *service-type service-name* **limit** { **hold-time** *time-value* | **usage** *usage-value* | **action**{**delete**|**log-only**}}	サービスのストレージ時間制限、ストレージ・スペース使用制限、またはストレージ制限によってトリガーされるアクションを設定します。