トラフィック分離に VRF-Lite を使用する NAC レイヤ 3 アウトオブバンド設計ガイド

目次

概要

注: このドキュメントの情報は通知なく変更されることがあります。 可能であれば、すべての推奨事項を確認してください。

このドキュメントの目的は、NAC サーバ（CAS）がリアル IP ゲートウェイ（ルーティング）モードで設定されている、レイヤ 3 Out of Band（OOB; アウトオブバンド）導入での NAC の VRF-Lite ベースの実装を説明することです。 レイヤ 3 アウトオブバンドは、急速に NAC の最も人気のある導入方式の 1 つになっています。 この人気の推移は、いくつかの力学に基づいています。 第一に、ハードウェア リソースの優れた使用率が挙げられます。 レイヤ 3 OOB 方式で NAC の導入を行うことで、単一の NAC アプライアンスは、より多くのユーザに対応するように拡張できます。 また、NAC アプライアンスを、キャンパスまたは組織にわたって分散するよりも、中央に配置するようにできます。 つまり、レイヤ 3 OOB 導入は、資本支出と運用費の両方の面でかなりコスト効果が高くなります。 レイヤ 3 OOB アーキテクチャで NAC を導入するには、広く使用されている次の 2 つのアプローチがあります。

1. ディスカバリホストベースのアプローチ：NAC サーバ（CAS）に到達するために、NAC エージェント内の固有の機能を使用します。 ACL は、ダーティ ネットワークのアクセス スイッチ制御トラフィック強制に適用されました。 詳細は、『SWISS プロトコルを使用した NAC サーバ（CAS）への接続』を参照してください。
2. VRF ベースのアプローチ：VRF を使用して CAS への認証されていないトラフィックをルー

ティングします。 NAC サーバ（CAS）に設定されたトラフィック ポリシーは、ダーティ ネットワーク上の強制に使用されます。 このアプローチには 2 つのサブアプローチがあります。 最初のアプローチでは、VRF がインフラストラクチャ全体に行き渡っており、その場合、すべてのレイヤ 3 デバイスがタグ スイッチングに参加します。 2 番目のアプローチでは VRF-Lite と GRE トンネルを使用して、タグ スイッチングを認識しないレイヤ 3 デバイス経由で VRF をトンネルします。 2 番目のアプローチのメリットは、コア インフラストラクチャに必要なのが最小限の設定変更であることです。

注: レイヤ 3 OOB は最も一般的な導入方式の 1 つである一方で、必ずしもすべての環境の最適なソリューションではありません。 特定の要件にさらに適した、選択可能なその他のオプションが存在します。 これらの他の NAC 設計オプションの詳細は、『導入の計画』を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- レイヤ 2 およびレイヤ 3 のインフラストラクチャ操作および設定に関する基本知識
- Cisco NAC アプライアンス、およびそれに関連するさまざまな実装方式の相違点に関する基本知識
- すべての NAC 導入および設計は、明確なビジネス要件に基づく必要があります。 これらはこのテスト セットアップ用のビジネスの要求想定です:ユーザは、全体としてネットワークにアクセスを付与される前に認証される必要があります。アクセスは、ユーザが誰であるかに基づいて制限されます。 これらの特権が Active Directory（AD）のグループ メンバシップにマップされます。 そのグループは、Guests、Contractors、Employees です。AD グループ メンバシップに基づいて、ユーザは各グループに適切なネットワーク アクセス特権を持つ VLAN に配置されます。ゲストユーザ トラフィックは認証の後でさえもネットワークの他から分離され続けます。ユーザがネットワークに許可された後、NAC アプライアンスをトラフィック パス内に入らなくする必要があります。 これによって、NAC アプライアンスがボトルネックになることが防止され、検証されたユーザがネットワークのすべての可能性を使用することが許可されます。
- NAC には、このドキュメントで説明しない機能が数多くあります。 このガイドの目的は、VRF-Lite ベースのレイヤ 3 アウトオブバンド NAC 導入に必要な設計ガイドラインと設定を詳しく説明し、文書化することです。 このガイドは、ポスチャ評価や修正は詳しく説明しません。 NAC アプライアンス（Clean Access）および完全な 機能についての詳細は www.cisco.com/go/nac （登録ユーザのみ）で見つけることができます。

使用するコンポーネント

このドキュメントは、特定のソフトウェアや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。

表記法

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

設定

インフラストラクチャ設定

はじめに

VRF-Lite ベースのレイヤ 3 OOB NAC 導入を検討するときには、考慮することが非常に重要であるいくつかの設計原則があります。 その原則をここに示し、その重要性についても簡単に説明します。

1. **トラフィック分類とエンジニアリング**：このタイプの NAC 設計用に理解し、念頭に置く主な概念は、ダーティとして分類されたトラフィックが NAC サーバ（CAS）の信頼できない側に流れる*必要がある*ということです。 NAC 実装の設計を行っているときは、この原則を常に念頭に置いてください。 さらに、クリーン ネットワークとダーティ ネットワークは、互いに直接通信することを許可しない必要があります。 VRF を伴うレイヤ 3 OOB 設計では、NAC サーバ（CAS）は、クリーン ネットワークとダーティ ネットワークの間の隔離と安全な通信を確実にする強制ポイントまたはコントローラとして機能します。
2. **トラフィックの分離**：認証されておらず、承認されていないホストから発信されるすべてのトラフィックに対してトラフィックとパスの分離を提供するために、適切な強制メカニズムが確実に選択されていることが重要です。 VRF-Lite は、ここで使用されて、データとコントロール プレーンの全面的な分離（VRF）を実施します。
3. **中央集中型の強制**：VRF-Lite 方式がルーティングによって作成された自然なパス選択に従うので、 トポロジ変更、アクセス制御要件、アドレス変更は、インフラストラクチャにわたって ACL を操作する必要性を作り出しません。 VRF-Lite とともに GRE トンネルを使用すると、複数のホップを設定する必要なく、NAC サーバのちょうど前にダーティなトラフィックを廃棄する柔軟性が提供されます。 GRE とともにある VRF-Lite は、エッジ レイヤ 3 デバイスの設定だけを必要とします。 これは、パス分離要件を提供するために接触する必要のあるデバイスの数を大幅に削減します。
4. **困難さ**：継続的なメンテナンスとともにある実装の困難さ。 ネットワーク内の NAC レイヤ 3 OOB に使用する傾向にあるアプローチを判断するときには、実装の簡単さと持続的運用コスト、特に動的な環境におけるテクノロジーの実装の複雑さを考慮することが重要です。

注: NAC アプライアンスは、それにトラフィックが提示される方法に気づきません。 いいかえると、NAC アプライアンス自体は、トラフィックが GRE トンネル経由で到着するかどうか、ポリシー ベースのルーティング設定、VRF ルーティングなどを経由してリダイレクトされたかどうかは優先しません。

注: 可能な限り最良のエンドユーザ体験を提供するために、エンドユーザのブラウザが信頼する証明書を使用するようにしてください。 NAC サーバ上で自己生成された証明書の使用は、本番環境には推奨されません。

注: NAC サーバ用の証明書をその「信頼できない」インターフェイスの IP アドレスで常に生成します。

次に示すのは、VRF を伴うデバイス仮想化の図です。 この方式は、パス分離用のコントロール プレーンとデータ プレーンを提供します。

トポロジ

次の図は、この資料の作成に使用したトポロジを表しています。 内部ネットワークはグローバル ルーティング テーブル経由でルーティングされ、それに関連付けられた VRF はありません。 DIRTY VRF には Dirty_VLAN と関連する通過ネットワークだけが含まれ、そのネットワークは DIRTY_VLAN を送信元とするすべてのデータが NAC アプライアンスのダーティ側経由で強制的に流れることを必要とします。 Guest VRF には GUEST_VLAN と関連する通過ネットワークが含まれ、そのネットワークは、ファイアウォール上の独立したサブインターフェイス上の GUEST_VLAN を送信元とするすべてのデータを終了させることを必要とします。 3 つの仮想ネットワークそれぞれは、同一の物理インフラストラクチャ上で維持され、トラフィックとパスの分離がそれぞれ完備されて提供されます。

プロセスのフロー

このセクションでは、エージェントがインストールされている状態とされていない状態の両方でネットワーク アクセスを取得するために必要なものの基本的なプロセス フローを示します。 これらのプロセス フローは、マクロ分析的な性質があり、機能決定手順だけを含んでいます。 発生するすべてのオプションやステップは含んでおらず、また、エンドポイント評価基準をベースにする承認決定は含んでいません。

設定

設定情報は、VRF-Lite/GRE を使ったパス分離用にネットワークを設定するために必要な手順と、レイヤ 3 OOB リアル IP ゲートウェイとしてネットワークに NAC アプライアンスを挿入するために必要な設定を詳しく説明します。

注: VRF-Lite は、2 つ以上の仮想ネットワークのサポートをイネーブルにする機能です。 また、VRF-Lite は、仮想ネットワーク間で IP アドレスが重複することを許容します。 ただし、IP アドレス重複は NAC 実装には推奨しません。その理由は、インフラストラクチャ自体が重複するアドレスをサポートする間に、複雑度と不正なレポートのトラブルシューティングを作り出す可能性があるためです。

VRF-Lite は異なる仮想ネットワーク用のルートを区別するために入力インターフェイスを使用し、1 つ以上のレイヤ 3 インターフェイスを各 VRF に関連付けることによって、仮想パケット転送テーブルを形成します。 VRF 内のインターフェイスは、イーサネット ポートなどのような物理的なものにすることも、 サブインターフェイス、トンネル インターフェイス、または VLAN SVI などのような論理的なものにすることもできます。 レイヤ 3 インターフェイスは一度に 1 つの VRF にしか属することができないことに注意してください。

VRF-Lite の重要な考慮事項

- VRF-Lite は、定義先のスイッチにとってローカルでだけ重要であり、VRF メンバシップは入力インターフェイスによって判断されます。 パケット ヘッダーまたはペイロードの操作は実行されません。
- VRF-Lite のあるスイッチは、複数のセキュリティ ドメインによって共有され、すべてのセキュリティ ドメインにはそれら独自のルーティング テーブルがあります。
- VRF-Lite によって、複数のセキュリティ ドメインがネットワーク デバイス間の同一の物理リンクを共有できます。 複数の VLAN または GRE トンネルのあるトランク ポートは、パケットをさまざまなセキュリティ ドメインから分離するトラフィック分離を提供します。
- すべてのセキュリティ ドメインには独自の VLAN が必要になります。
- VRF-Lite は、 ラベル交換、LDP 隣接関係、ラベル付きパケットというすべての MPLS-VRF 機能はサポートしません。

- レイヤ 3 TCAM リソースはすべての VRF 間で共有されます。 1 つの VRF が十分な CAM スペースを持つことを確実にするには、**maximum routes** コマンドを使用します。
- VRF-Lite を使用する Catalyst スイッチは、1 つのグローバルなネットワークと最大 64 の VRF をサポートできます。 サポートされるルートの合計数は、TCAM のサイズによって限定されます。
- ほとんどのルーティング プロトコル（BGP、OSPF、EIGRP、RIP、およびスタティック ルーティング）は、VRF-Lite を実行するデバイス間で使用できます。
- VRF 間のルートをリークする必要がある場合以外は、VRF-Lite で BGP を実行する必要はありません。
- VRF-Lite は、パケット スイッチング レートに影響しません。
- マルチキャストと VRF-Lite は、同一のレイヤ 3 インターフェイス上に同時には設定できません。
- **router ospf** の下の **capability vrf-lite** サブコマンドは、ネットワーク デバイス間のルーティング プロトコルとして OSPF を設定するときに使用します。

VRF の定義

設計の例では、要件は、認証されていないユーザまたは DIRTY ユーザの両方とともに GUESTS に対してパス分離を提供します。 他のすべてのトラフィックは、内部ネットワークを利用するために許可されます。 これには、2 つの VRF の定義が必要になります。 次に設定例を示します。

```
!
ip vrf DIRTY
!--- Names the VRF and places you into VRF Configuration
Mode description DIRTY_VRF_FOR_NAC !--- Gives the VRF a
user friendly description field for documentation rd
10:1 !--- Creates a VRF table by specifying a route
distinguisher. !--- Enter either an AS number and an
arbitrary number (xxx:y) or an !--- IP address and
arbitrary number (A.B.C.D:y). ! ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS rd 30:1 !
```

VLAN またはインターフェイスと VRF の関連付け

レイヤ 3 スイッチまたはルータに VRF が定義された後、VRF-Lite 設定に参加するインターフェイスを、属している VRF と関連付ける必要があります。 前述のように、物理インターフェイスと仮想インターフェイスのどちらも VRF と関連付けることができます。 含まれているのは、VRF と関連付けられた物理インターフェイス、スイッチされる仮想インターフェイス、サブインターフェイス、トンネル インターフェイスの例です。

```
!
interface FastEthernet0/1
ip vrf forwarding GUESTS
!!Associates the interface with the appropriate VRF
defined in Step 1!!
ip address 192.168.39.1 255.255.255.252
!
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface Vlan100
ip vrf forwarding DIRTY
```

```
ip address 192.168.100.1 255.255.255.0
!
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.254.1
!
```

2 つのデバイス間の VRF の拡張

インフラストラクチャの 2 点間の VRF を拡張する容認可能な方式はいくつか存在します。 使用する方式は次の基準に基づいて選択してください。

1. プラットフォームの機能：プラットフォームの機能を考慮して、現在のすべての Cisco レイヤ 3 対応のエンタープライズ スイッチングおよびルーティング プラットフォームは VRF-Lite をサポートしています。 これらには、Catalyst 6500、4500、3750、3560 の各プラットフォームが含まれ、またこれらに限定されません。
2. 適切な Cisco IOS® を実行するルーティング プラットフォームは、7600、3800、2800、1800、および 800 シリーズの ISR を含み、これらに限定されません。
3. 対応するインフラストラクチャの部分の間のレイヤ 3 ホップの数：レイヤ 3 ホップの数の判断は、導入をできるだけシンプルにするには重要なことです。 たとえば、CAS デバイスとクライアントをホスティングするインフラストラクチャ間に 5 つのレイヤ 3 ホップが存在する場合、管理オーバーヘッドを作成できます。

適切ではないソリューションの場合、次のようになります。

1. レイヤ 2 トランキングが、非常に最適ではないレイヤ 2 トポロジを作成します。
2. レイヤ 3 サブインターフェイスにおいて、数多くの追加インターフェイスを設定しなければならなくなります。 その結果、これが、追加の管理オーバーヘッドと潜在的な IP アドレス指定の問題を生み出すことになります。 これを図に示します。 インフラストラクチャに冗長性はないと想定する場合、示されているネットワークの各レイヤが入出力両方の物理インターフェイスを備えています。 サブインターフェイスの数の計算は (2 * ネットワーク内の層の数 * (VRF の数)) です。 この例には 2 つの VRF があるので、式は ((2*5)*2) で 20 個のサブインターフェイスになります。 冗長性が追加されると、この数値は 2 倍よりも多くなります。 これを GRE 拡張に比較すると、GRE 拡張で同一の最終結果に必要とされるのは 4 つのインターフェイスだけです。 これは、GRE がいかに設定の影響を大幅に減少させるかをわかりやすく示しています。

レイヤ 2 トランキング

レイヤ 2 トランキングは、レイヤ 3 クローゼットが導入されない場所またはネットワーク デバイスが GRE またはサブインターフェイスをサポートしない場所のシナリオで好まれます。 Catalyst 3560、3750、4500 プラットフォームがサブインターフェイスをサポートしないことに注意してください。 Catalyst 3560 と 3750 は GRE もサポートしません。 Catalyst 4500 はソフトウェアで GRE をサポートし、Catalyst 6500 はハードウェアで GRE をサポートします。

サブインターフェイスまたは GRE をサポートしないプラットフォームからサポートするプラットフォームに接続するレイヤ 3 クローゼット モデルでは、片方の側でレイヤ 2 トランキングだけを使用することと、もう一方の側でサブインターフェイスを使用することが好まれます。 これによって、レイヤ 3 クロゼット アーキテクチャのすべてのメリットを維持でき、さらに、いくつかのプラットフォームでの GRE またはサブインターフェイス サポートなしの制限を解消できます

。リンクの一方の側だけにレイヤ 2 トランキングの設定を行う主なメリットの 1 つは、スパニング ツリーがレイヤ 3 環境の後ろには導入されないということです。 3750 アクセス スイッチ（GRE とサブインターフェイス サポートなし）が 6500 ディストリビューション スイッチに接続される例を参照してください。6500 ディストリビューション スイッチでは GRE およびサブインターフェイスがサポートされます。

3750 関連の設定：

この設定では、FastEthernet 1/0/1 で、NATIVE VLAN 用のデフォルト設定が VLAN 1 であることに注目してください。 この設定は変更されていません。 ただし、VLAN 1 がリンクにわたってトランクされることは許可されていないことにも注目してください。 許可される VLAN は、タグ付きの VLAN だけに限定されています。 このレイヤ 3 トポロジではトランク ネゴシエーションの必要はなく、また、スイッチ間で VTP トラフィックが行き来する必要もないので、このリンクを通過するためのカプセル化されていないトラフィックの必要性もありません。 この設定は、不必要なレイヤ 2 セキュリティ ホールを開くことはないので、アーキテクチャのセキュリティ ポスチャを増やします。

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
!
interface FastEthernet1/0/1
description CONNECTION_TO_DISTRIBUTION_6504
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport mode trunk
speed 100
duplex full
!
!
interface Vlan10
description DIRTY_VRF_TRANSIT
ip vrf forwarding DIRTY
ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
description CLEAN_TRANSIT
ip address 192.168.20.2 255.255.255.252
!
interface Vlan30
description GUESTS_VRF_TRANSIT
ip vrf forwarding GUESTS
ip address 192.168.30.2 255.255.255.252
!
```

6500 関係のある構成:

この構成では、dot1q カプセル化が使用され、VLAN 10、20、30 のフレームにタグが付けられることに注目してください。 使用する VLAN タグを選択するとき、スイッチ上の VLAN データベースにローカルにすでに定義されている VLAN 番号は使用できません。

```
!
```

```
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface FastEthernet3/1.20
description CLEAN_TRANSIT
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
description GUESTS_VRF_TRANSIT
encapsulation dot1Q 30
ip vrf forwarding GUESTS
ip address 192.168.30.1 255.255.255.252
!
```

レイヤ 3 サブインターフェイス

レイヤ 3 サブインターフェイスは、ネットワーク内で 1 つのレイヤ 3 ホップ経由で VRF を拡張する必要があるだけの場合に格好のオプションです。 GRE またはサブインターフェイスのどちらも、各設定の快適さのレベルをベースにして選択できます。 これは、レイヤ 3 サブインターフェイスの設定例です。

```
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
```

GRE トンネル

GRE トンネルは、VRF へのアクセスが必要なクライアント間に複数のレイヤ 3 ホップが存在する場合に VRF-Lite VRF を拡張するときの推奨方式です。 このタイプの設計は、リモート クライ

アントが中央に配置された NAC サーバにアクセスすることを望んでいるリモート オフィスではさらに一般的です。 たとえば、典型的なコア、ディストリビューション、アクセス ネットワーク モデル クライアントは、ディストリビューションにもコアにも直接は接続されません。 そのため、ディストリビューション デバイスまたはコア デバイスに複雑な VRF 定義を追加する必要はありません。 GRE は、NAC サーバが接続されているネットワーク内のポイントに分離する必要があるトラフィックを単純に転送するために使用できます。 これは、GRE トンネル インターフェイスの例です。

```
!
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.254.1
!
```

VRF 用のルーティングの設定

このドキュメントで前述したように、VRF-Lite は BGP、OSPF、 EIGRP をサポートします。 この設定例では、一般に、EIGRP が高速コンバージェンスが必要なキャンパス ネットワーク上に実装されるシスコ推奨ルーティング プロトコルなので、EIGRP が選択されます。

OSPF が VRF-Lite と同等に良好に動作し、BGP も同様であることにも注目してください。

また、VRF 間でトラフィックがリークする必要がある設計の場合は、BGP が必要であることも注目してください。

これは、EIGRP を伴う VRF のルーティングの設定例です。

```
!
!--- As with any configuration this is base routing
protocol !--- configuration which handles the routing
for the Global Routing Table. router eigrp 1 network
192.168.20.0 0.0.0.3 network 192.168.21.0 network
192.168.22.0 network 192.168.28.0 0.0.0.3 network
192.168.29.0 0.0.0.3 network 192.168.254.1 0.0.0.0 no
auto-summary ! !--- An Address Family must be defined
for each VRF !--- that is to be routing through the
routing protocol. !--- Routing Protocol options such as
auto-summarization, !--- autonomous system number,
router id, and so forth are all !--- configured under
the address family. Note that EIGRP does not !---
neighbor without the autonomous system specified under
!--- the address family. Also note, that this autonomous
system !--- number should be unique for each VRF and
should not be !--- the same as the Global AS number. !
address-family ipv4 vrf GUESTS network 192.168.30.0
0.0.0.3 network 192.168.38.0 0.0.0.3 no auto-summary
autonomous-system 30 exit-address-family ! address-
family ipv4 vrf DIRTY network 192.168.10.0 0.0.0.3
network 192.168.11.0 no auto-summary autonomous-system
10 exit-address-family !
```

グローバル ルーティング テーブルとダーティ VRF との間のトラフィックのルーティング

ネットワークの信頼できない側またはダーティな側からネットワークの信頼できる側またはクリ

ーンな側にトラフィックを通過させる必要があるかどうかは、NAC 導入要件に依存します。 たとえば、修正サービスは、NAC アプライアンスの信頼できる側で動作中である可能性があります。 導入環境での Active Directory シングル サインオンの場合、対話型ログオン、Kerberos チケット交換などを許可するために、Active Directory へとトラフィックのサブセットを通過させる必要があります。 いずれにしても、グローバル ルーティング テーブルとダーティ VRF の間でデータを受け渡す必要がある場合は、グローバル ルーティング テーブルがダーティ VRF に到達する方法が確立されていること、そしてダーティ VRF がグローバル ルーティング テーブルに到達する方法が確立されていることが非常に重要です。 これは、通常、この方式で処理されます。

ダーティ VRF は、デフォルトで NAC アプライアンスの信頼できない インターフェイスまたはダーティ インターフェイスになります。 グローバルは、ダーティ VLAN とみなされるサブネットだけにスタティック ルートを持っています。

次の図を検討してみましょう。

NAC アプライアンスの信頼できない側またはダーティな側の最初のレイヤ 3 ホップは、NAC アプライアンスにポイントするルーティング プロセスのデフォルト ルートを再配布します。 NAC アプライアンスの信頼できる側またはクリーンな側の最初のレイヤ 3 ホップは、VLAN 100 に属しているサブセット、この場合 192.168.100.0/24 であるスタティック ルートを再配布します。

注: NAC アプライアンスの反対側にある最初のレイヤ 3 ホップは、同一の物理デバイス上、ただし、異なる VRF 上に存在できます。 次の例では、NAC サーバの信頼できない側またはダーティ側は VRF 内に存在し、一方で、NAC アプライアンスの信頼できる側またはクリーンな側はグローバル ルーティング テーブル内に留まります。

設定は次のようになります。

```
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
ip classless
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
```

```
!!
```

レイヤ 3 OOB 用の NAC 設定

CAS 設定

「概要」で説明した第一の原則を思い出してください。 成功する NAC 設計のテクニックは、ダーティと分類されたトラフィックが NAC サーバ（CAS）の信頼できない側に流れる*必要がある*ことを常に念頭に置くということです。

最初のスクリーン ショットでは、NAC サーバ ネットワーク設定に注意してください。 サーバがアウトオブバンド リアル IP ゲートウェイとして導入されています。 NAC サーバのデフォルト ルートは信頼できる（Trusted）側をポイントしています。

サーバは、信頼できない（Untrusted）側に存在するダーティ VLAN のそれぞれにスタティック ルートとともに設定する必要があります。 2 番目のスクリーン ショットを参照してください。

確認

ネットワークにログインしているユーザ NAC-Employee のドキュメント化されたプロセスを参照してください。 シスコは、アクセス スイッチ、ワークステーションからのアクティビティを把握しており、ディストリビューション スイッチのルーティング テーブルからの情報を表示します。

ここでは、設定が正常に動作していることを確認します。

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

ステージ 1：まだネットワークに接続しておらず、アクセス スイッチ上のスイッチポートはダウンしています。

```
! – Catalyst 3750 Access Switch
!--- Note: Client mahcine is off the network at this
point. ! 3750-Access#show int status | i Fa1/0/13
Fa1/0/13 CLIENT_CONNECTION notconnect 100 auto auto
10/100BaseTX ! ! 3750-Access#!Notice it is in the
"notconnect" state. !
```

ステージ 2：Windows クライアントは、ネットワークに接続し、スイッチの初期 VLAN は VLAN 100（ダーティ VLAN）です。 このスクリーン ショットでわかるように、IP アドレスがホストに割り当てられています。

```
! – Catalyst 3750 Access Switch
!--- Note: Client just connected to the network. 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100,
changed state to up 2w5d: %LINK-3-UPDOWN: Interface
FastEthernet1/0/13, changed state to up 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/13, changed state to up ! ! 3750-
Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 100 a-full a-100
10/100BaseTX !
```

ステージ 3：数秒で、NAC エージェントはログオン プロセスを開始します。 この例では、Active Directory シングル サインオンが設定されるので、ユーザ名とパスワードの入力は促されません。 その代わりに、シングル サインオンが発生するというメッセージのポップアップ ウィンドウが表示されます。

認証とポスチャ評価が完了した後、成功のメッセージが表示され、スイッチポートはダーティ VLAN から社員用 VLAN に移動され、NAC エージェントは PC の IP アドレスを更新します。

```
! – Catalyst 3750 Access Switch
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan100, changed state to down
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan200, changed state to up
!
!--- Note: As you can tell from the previous messages,
!--- the switchport was just moved from VLAN 100 to VLAN
200. ! 3750-Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 200 a-full a-100
10/100BaseTX ! !
```

このスクリーン ショットは、社員 VLAN（VLAN 200）内にある最終 IP アドレスを示しています。

このスクリーン ショットは、認定済みデバイス リスト（Certified Devices List）にある NAC-Employee ユーザのデバイスを示しています。 役割（Role）は *EMPLOYEES* に割り当てられ、VLAN は 200 です。

このスクリーン ショットは、NAC マネージャのオンライン ユーザ リストを示しています。

これは NAC マネージャ イベント ログであり、これはアウトオブバンド ユーザの正常なログインを示します。

このセクションでは、グローバル ルート テーブルのルーティング テーブルとダーティ VRF を調べます。 最初の画面では、**show ip route** コマンドに注目してください。 これは、グローバル ルート向けのルーティング テーブルが表示されることを示しています。

```
6504-DISTRIBUTION#show ip route Codes: C - connected, S
- static, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1
- OSPF external type 1, E2 - OSPF external type 2 i -
IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-
IS level-2 ia - IS-IS inter area, * - candidate default,
U - per-user static route o - ODR, P - periodic
downloaded static route Gateway of last resort is
192.168.28.2 to network 0.0.0.0 192.168.29.0/30 is
subnetted, 1 subnets D 192.168.29.0 [90/30720] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.28.0/30 is
subnetted, 1 subnets C 192.168.28.0 is directly
connected, FastEthernet3/48 D EX 192.168.31.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 D
EX 192.168.30.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D 192.168.200.0/24 [90/28416] via
192.168.20.2, 6d19h, FastEthernet3/1.20 D EX
192.168.38.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 C 192.168.21.0/24 is directly
connected, Vlan21 D EX 192.168.39.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.20.0/30 is
```

```
subnetted, 1 subnets C 192.168.20.0 is directly
connected, FastEthernet3/1.20 D EX 192.168.36.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.22.0/24 is directly connected, Vlan22 D EX
192.168.37.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.34.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.254.0/32 is
subnetted, 3 subnets D 192.168.254.2 [90/156160] via
192.168.20.2, 2w5d, FastEthernet3/1.20 D 192.168.254.3
[90/156160] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.254.1 is directly connected, Loopback0 D EX
192.168.35.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.32.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 S 192.168.100.0/24
[1/0] via 192.168.21.10 D EX 192.168.33.0/24 [170/30976]
via 192.168.28.2, 2w5d, FastEthernet3/48 D*EX 0.0.0.0/0
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48
```

注: 192.168.100.0/24 ネットワーク (ダーティ ネットワーク) は、スタティック ルートとしてルーティング テーブル内にあり、次のホップは NAC サーバの信頼できるインターフェイスになっています。

show ip route vrf DIRTY コマンドに注目してください。 これは、ダーティ仮想ネットワークだけのルーティング テーブルが確認できることを示しています。

```
6504-DISTRIBUTION#show ip route vrf DIRTY Routing Table:
DIRTY Codes: C - connected, S - static, R - RIP, M -
mobile, B - BGP D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area N1 - OSPF NSSA external type
1, N2 - OSPF NSSA external type 2 E1 - OSPF external
type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS
summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-
IS inter area, * - candidate default, U - per-user
static route o - ODR, P - periodic downloaded static
route Gateway of last resort is 192.168.11.2 to network
0.0.0.0 192.168.10.0/30 is subnetted, 1 subnets C
192.168.10.0 is directly connected, FastEthernet3/1.10 C
192.168.11.0/24 is directly connected, Vlan11 D
192.168.100.0/24 [90/28416] via 192.168.10.2, 01:03:19,
FastEthernet3/1.10 S* 0.0.0.0/0 [1/0] via 192.168.11.2
```

注: ダーティ VRF ルーティング テーブルだけにあるダーティ アクセス VLAN (192.168.100.0/24) が 3750 アクセス スイッチからの EIGRP 経由で、ディストリビューションで習得される点に注意してください。 このルートは、グローバル テーブルには存在しません。

付録 A： スイッチの設定

アクセス スイッチが動作している設定

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3750-Access
!
!
no aaa new-model
clock timezone EST -5
```

```
clock summer-time EST recurring
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
!
!
crypto pki trustpoint TP-self-signed-819048320
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-819048320
 revocation-check none
 rsakeypair TP-self-signed-819048320
!
!
crypto ca certificate chain TP-self-signed-819048320
 certificate self-signed 01
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Loopback0
 ip address 192.168.254.2 255.255.255.255
!

!
interface FastEthernet1/0/1
 description CONNECTION_TO_DISTRIBUTION_6504
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 speed 100
 duplex full
!
interface range FastEthernet1/0/2 - 24
 description CLIENT_CONNECTION
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!- SNIP -
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description DIRTY_VRF_TRANSMIT
 ip vrf forwarding DIRTY
 ip address 192.168.10.2 255.255.255.252
!
```

```
interface Vlan20
 description CLEAN_TRANSIT
 ip address 192.168.20.2 255.255.255.252
!
interface Vlan30
 description GUESTS_TRANSIT
 ip vrf forwarding GUESTS
 ip address 192.168.30.2 255.255.255.252
!
interface Vlan100
 description DIRTY_VLAN
 ip vrf forwarding DIRTY
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan200
 description EMPLOYEES_VLAN
 ip address 192.168.200.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan210
 description CONTRACTORS_VLAN
 ip address 192.168.210.1 255.255.255.0
 ip helper-address 192.168.22.11
!

!
interface Vlan300
 description GUESTS
 ip vrf forwarding GUESTS
 ip address 192.168.31.1 255.255.255.0
!
router eigrp 1
 network 192.168.20.0 0.0.0.3
 network 192.168.200.0
 network 192.168.254.2 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
 network 192.168.30.0 0.0.0.3
 network 192.168.31.0
 no auto-summary
 autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
 network 192.168.10.0 0.0.0.3
 network 192.168.100.0
 no auto-summary
 autonomous-system 10
 exit-address-family
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip http server
ip http secure-server
!
```

```
!
snmp-server community NIC-NAC-PADDYWHACK RW
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v1
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v2c
snmp-server trap-source Loopback0
snmp-server host 192.168.22.5 version 2c NIC-NAC-
PADDYWHACK
!
!- SNIP
!
ntp clock-period 36028450
ntp source Loopback0
ntp server 192.168.254.1 version 2 prefer
end
```

ディストリビューション スイッチが動作している設定

```
!– SNIP -
!
hostname 6504-DISTRIBUTION
!
boot-start-marker
boot system disk0:s72033-advipservicesk9_wan-mz.122-
33.SXH2a.bin
boot-end-marker
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
!
!- SNIP -
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
ipv6 mfib hardware-switching replication-mode ingress
vtp domain cmpd
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
```

```
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!

!
vlan 11
 name CAS_DIRTY
!
vlan 21
 name CAS_CLEAN
!
vlan 22
 name SERVER_VLAN
!
interface Tunnel0
 ip vrf forwarding GUESTS
 ip address 192.168.38.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 192.168.254.3
!
interface Loopback0
 ip address 192.168.254.1 255.255.255.255
!
!- SNIP -
!
interface FastEthernet3/1
 description CONNECTION_TO_3750_ACCESS
 no ip address
 speed 100
 duplex full
!
interface FastEthernet3/1.10
 description DIRTY_VRF_TRANSIT
 encapsulation dot1Q 10
 ip vrf forwarding DIRTY
 ip address 192.168.10.1 255.255.255.252
 ip verify unicast source reachable-via rx allow-default
!
interface FastEthernet3/1.20
 description CLEAN_TRANSIT
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
 description GUESTS_TRANSIT
 encapsulation dot1Q 30
 ip vrf forwarding GUESTS
 ip address 192.168.30.1 255.255.255.252
!
!
!
!

!
interface FastEthernet3/2
 description CAS1_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
```

```
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/3
 description CAS2_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/4
 description CAS1_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/5
 description CAS2_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/6
 description CAM
 switchport
 switchport access vlan 22
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!
!- SNIP -
!
!


!
interface FastEthernet3/48
 description CONNECTION_TO_THE_WORLD
 ip address 192.168.28.1 255.255.255.252
 speed 100
 duplex full
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan11
 description NAC_DIRTY
 ip vrf forwarding DIRTY
 ip address 192.168.11.1 255.255.255.0
```

```
!
interface Vlan21
 description NAC_CLEAN
 ip address 192.168.21.1 255.255.255.0
!
interface Vlan22
 description SERVER_VLAN
 ip address 192.168.22.1 255.255.255.0
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
!
!
!
!

!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
!
!- SNIP -
!
ntp source Loopback0
ntp master 2
!
end
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems