Guide de conception NAC couche 3 hors bande, qui utilise VRF-Lite pour l'isolation du trafic

Contenu

Introduction

Remarque: Les informations dans ce document peuvent modification sans préavis. Confirmez toutes les recommandations si possible.

Le but de ce document est de décrire une implémentation basée parLite de NAC dans une couche 3 sur le déploiement de la bande (OOB) où le serveur NAC (CAS) est configuré en vrai mode de passerelle IP (conduite). La couche 3 sur la bande a rapidement devenu des méthodologies de déploiement les plus populaires pour le NAC. Cette variation dans la popularité est basée sur des plusieurs dynamics. Le premier est une meilleure utilisation des ressources en matériel. Par le déploiement du NAC dans une méthodologie de la couche 3 OOB, une appliance simple NAC peut être faite pour mesurer pour rendre service à plus d'utilisateurs. Il permet également les appliances NAC à situer centralement plutôt que distribuées à travers le campus ou l'organisation. Ainsi, les déploiements de la couche 3 OOB sont beaucoup plus rentables chacun des deux d'un point de vue de capital et de frais d'exploitation. Il y a deux approches très utilisées pour déployer le NAC en architecture de la couche 3 OOB.

1. Approche basée parhôte — Emploie la capacité inhérente dans l'agent NAC afin d'atteindre le serveur NAC (CAS). ACLs s'est appliqué sur l'application du trafic de contrôle de commutateur d'accès sur le réseau modifié. Référez-vous à se connecter au serveur NAC (CAS) utilisant le pour en savoir plus SUISSE de Protocol.

2. Approche basée par VRF — Vrf d'utilisations pour conduire le trafic unauthenticated à CAS. Des stratégies de trafic configurées sur le serveur NAC (CAS) sont utilisées pour l'application sur le réseau modifié. Cette approche a deux sous-titre-approches. Dans la première approche, les vrf sont dominants dans toute l'infrastructure, dans ce cas tous les périphériques de la couche 3 participent à la commutation de balise. La deuxième approche utilise des tunnels de Vrf-Lite et GRE pour percer un tunnel les vrf par les périphériques de la couche 3 qui ne comprennent pas la commutation de balise. L'avantage à la deuxième approche est que des modifications de configuration minimale sont exigées à votre infrastructure principale.

Remarque: Tandis que la couche 3 OOB est l'une des méthodologies de déploiement les plus communes, ce ne peut pas toujours être la solution optimale pour chaque environnement. Il y a d'autres options de choisir de cela peut être une adaptation plus optimale pour vos conditions requises particulières. Référez-vous à prévoir votre déploiement pour plus d'informations sur ces autres options de conception NAC.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Une compréhension de base exécution et configuration de la couche 2 et de la couche 3 d'infrastructure
- Une compréhension de base de l'appliance de Cisco NAC, et les différences entre les diverses méthodologies d'implémentation qui sont associées avec elle
- Tous les déploiements et conceptions NAC devraient être basés sur des conditions requises claires d'affaires. Ce sont les suppositions de condition requise d'affaires pour cette installation de test :Des utilisateurs doivent être authentifiés avant d'être accordé l'accès au réseau dans son ensemble.Votre accès est limité basé sur qui les utilisateurs sont. Ces privilèges sont tracés à l'adhésion à des associations dans le Répertoire actif. Les groupes sont des invités, des sous-traitants, et des employés.Basé sur l'adhésion à des associations d'AD, des utilisateurs sont placés dans un VLAN qui a les privilèges d'accès au réseau qui sont appropriés pour chaque groupe.Le trafic d'utilisateur d'invité continue à être isolé dans le reste du réseau même après l'authentification.Après que l'utilisateur soit admis au réseau, l'appliance NAC doit plus n'être dans le chemin du trafic. Ceci empêche l'appliance NAC de devenir un étranglement et permet le réseau à utiliser à son plein potentiel par les utilisateurs validés.
- Le NAC a beaucoup de capacités qui ne sont pas couvertes par ce document. Le but de ce guide est d'explorer et documenter les directives de conception et la configuration exigées pour une couche basée 3 de Vrf-Lite sur le déploiement de la bande NAC. Ce guide ne se concentre pas sur l'estimation ou la correction de posture. Plus d'informations sur l'appliance NAC et ses pleines capacités peuvent être trouvées chez www.cisco.com/go/nac (clients enregistrés seulement).

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Configuration d'infrastructure

Introduction :

Quand vu un Vrf-Lite basé le déploiement de la couche 3 OOB NAC, là sont plusieurs conceptions de bases il est très importante considérer que. Ces principes sont répertoriés ici, et une brève discussion de leur importance est incluse.

1. **Classification du trafic et ingénierie** — Un concept clé à réaliser et se souvenir pour ce type de conception NAC est que le trafic classifié en tant qu'écoulement modifié de *nécessité* dans le côté non approuvé du serveur NAC (CAS). Gardez toujours ce dessus de principe d'esprit pendant la conception d'une implémentation NAC. Supplémentaire, on ne devrait pas permettre aux des réseaux propres et modifiés pour communiquer directement les uns avec les autres. Dans une conception de la couche 3 OOB avec des vrf, le serveur NAC (CAS) agit en tant que point ou contrôleur d'application qui assure la ségrégation et la communication protégée entre les réseaux propres et modifiés.
2. **La localisation du trafic** — Il est important d'être sûr qu'un mécanisme d'application approprié est sélectionné pour fournir l'isolation du trafic et de chemin pour tout le trafic originaire des hôtes non-authentifiés et non-autorisés. Vrf-Lite est utilisé ici pour réaliser l'isolation de solutions complètes de données et de contrôle-avion (VRF).
3. **Application centralisée** — Puisque la méthodologie de Vrf-Lite suit la sélection de chemin naturelle créée par l'acheminement : les modifications de topologie, les conditions requises de contrôle d'accès, et/ou les modifications d'adresse ne créent pas la nécessité de manipuler ACLs à travers l'infrastructure. Si vous utilisez un tunnel GRE en même temps que Vrf-Lite, ceci te donne la flexibilité de relâcher le juste modifié du trafic devant le serveur NAC sans nécessité de configurer de plusieurs sauts. Vrf-Lite en même temps que GRE exigent seulement la configuration sur des périphériques de la couche 3 de périphérie. Ceci réduit excessivement le nombre de périphériques qui doivent être touchés afin de fournir la condition requise d'isolation de chemin.
4. **Difficulté** — Difficulté d'implémentation aussi bien que de maintenance continue. Quand vous déterminez l'approche que vous êtes susceptible de utiliser pour la couche NAC 3 OOB dans votre réseau, il est important de considérer la facilité de l'implémentation et le coût d'exploitation et la complexité actuels de mettre en application cette technologie, en particulier dans un environnement dynamique.

Remarque: L'appliance NAC est inconsciente à la façon dont le trafic lui est présenté. En d'autres termes, l'appliance elle-même n'a aucune préférence si le trafic arrive par un tunnel GRE, ou a été réorientée par la stratégie basée conduisant la configuration, VRF conduit et ainsi de suite.

Remarque: Pour la meilleure expérience utilisateur possible, souvenez-vous pour utiliser les Certificats qui sont de confiance par le navigateur de l'utilisateur. L'utilisation des Certificats Auto-générés sur le serveur NAC n'est pas recommandée pour un environnement de production.

Remarque: Générez toujours le certificat pour le serveur NAC avec l'adresse IP de son interface NON APPROUVÉE.

Une illustration de virtualisation de périphérique avec des vrf peut être vue ici. Cette méthodologie fournit l'avion et le plan de données de contrôle pour l'isolation de chemin.

Topologie

Ce diagramme est représentant de la topologie utilisée pour la création de ce document. Le réseau interne conduit par le Tableau de routage global et n'a aucun VRF associé avec lui. Le VRF MODIFIÉ contient seulement le Dirty_VLAN et les réseaux associés de transit qui sont exigés pour forcer toutes les données originaires du DIRTY_VLAN pour traverser le côté modifié des appliances NAC. Le VRF d'invité contient le GUEST_VLAN et les réseaux associés de transit exigés pour terminer toutes les données originaires du GUEST_VLAN sur une sous-interface séparée sur le Pare-feu. Chacun des trois réseaux virtuels est porté sur la même infrastructure physique et fournit l'isolation complète du trafic et de chemin respectivement.

Écoulements de processus

Cette section affiche l'écoulement d'opération de base avec de ce qu'est prié de gagner l'accès au réseau chacun des deux, et sans agent installé. Ces écoulements de processus sont macroanalytiques en nature et contiennent seulement les étapes fonctionnelles de décision. Ils n'incluent pas chaque option ou font un pas qui se produit et n'incluent pas les décisions d'autorisation qui sont basées sur des critères d'estimation de point final.

Configuration

Les informations de configuration détaillent l'étape nécessaire pour configurer votre réseau pour l'isolation de chemin utilisant VRF-Lite/GRE et la configuration exigée pour la mise en place de l'appliance NAC dans votre réseau comme vraie passerelle IP de la couche 3 OOB.

Remarque: Vrf-lite est une caractéristique qui te permet de prendre en charge des réseaux deux ou plus virtuels. Vrf-lite tient compte également des adresses IP superposantes parmi les réseaux virtuels. Mais, la superposition d'adresse IP n'est pas recommandée pour une implémentation NAC parce que tandis que l'infrastructure elle-même prend en charge les adresses superposantes, elle peut créer des complexités de dépannage et l'enregistrement incorrect.

Vrf-lite emploie des interfaces d'entrée pour distinguer des artères pour différents réseaux virtuels et les tables virtuelles de transfert de paquet de formes en associant un ou plusieurs posent 3 interfaces avec chaque VRF. Les interfaces dans un VRF peuvent être l'un ou l'autre physique, comme des ports Ethernet ; ou logique, comme les sous-interfaces, les interfaces de tunnel ou le VLAN SVI. Veuillez noter une interface de la couche 3 ne peut pas appartenir à plus d'un VRF à tout moment.

Importantes considérations pour Vrf-Lite

- Vrf-Lite est seulement localement - significatif au commutateur où il est défini, et à l'adhésion de VRF est déterminé par l'interface d'entrée. Aucune manipulation d'en-tête ou de charge utile de paquet n'est exécutée.
- Un commutateur avec Vrf-lite est partagé par de plusieurs domaines de sécurité, et tous les

domaines de sécurité ont leurs propres seules tables de routage.

- Vrf-Lite permet de plusieurs domaines de sécurité de partager le même lien physique entre les périphériques de réseau. Les ports de joncteur réseau avec des VLAN multiples ou des tunnels GRE fournissent la localisation du trafic qui sépare des paquets de chaque domaine de sécurité différent.
- Tous les domaines de sécurité doivent avoir leurs propres VLAN.
- Vrf-lite ne prend en charge pas toute la fonctionnalité MPLS-VRF : étiquetez l'échange, la contiguïté LDP, ou les paquets étiquetés.
- La ressource en couche 3 TCAM est partagée entre tous les vrf. Afin de s'assurer que n'importe quel un VRF a le suffisamment d'espace de CAM, utilisez la commande de **maximum routes**.
- Un commutateur de Catalyst utilisant Vrf-Lite peut prendre en charge un réseau global et jusqu'à 64 vrf. Le nombre total d'artères prises en charge est limité par la taille du TCAM.
- La plupart des protocoles de routage (BGP, OSPF, EIGRP, RIP et routage statique) peuvent être utilisés entre les périphériques qui exécutent Vrf-Lite.
- Il n'y a aucun besoin d'exécuter le BGP avec Vrf-Lite à moins que vous deviez couler des artères entre les vrf.
- Vrf-Lite n'affecte pas le débit de commutation par paquets.
- La Multidiffusion et le Vrf-Lite ne peuvent pas être configurés sur la même interface de la couche 3 en même temps.
- La commande secondaire de **capability vrf-lite** sous le **router ospf** devrait être utilisée quand vous configurez l'OSPF comme protocole de routage entre les périphériques de réseau.

Définir un VRF

Dans l'exemple de projet, les conditions requises fournissent l'isolation de chemin pour les utilisateurs unauthenticated ou MODIFIÉS aussi bien que les INVITÉS. On permet au tout autre trafic pour utiliser le réseau interne. Ceci exige la définition de deux vrf. Voici la configuration :

```
!
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 !
```

Associez un VLAN ou une interface avec un VRF

Après que le VRF ait été défini sur le commutateur ou le routeur de la couche 3, les interfaces qui participent à la configuration de Vrf-Lite doivent être associées avec le VRF auquel elles appartiennent. Comme cité précédemment, l'examen médical ou les interfaces virtuelles peut être associé avec un VRF. Inclus sont les exemples d'une interface physique, d'une interface virtuelle commutée, d'une sous-interface et d'une interface de tunnel qui sont associés avec un VRF.

```
!
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
!
```

Étendez un VRF entre deux périphériques

Il y a plusieurs méthodologies acceptables pour l'extenion d'un VRF entre deux parties d'infrastructure. La méthode que vous choisissez devrait être basée sur le ce des critères :

1. Capacités de plate-forme — En vue de des capacités de plate-forme, tout le Cisco en cours support posent 3 d'entreprise Plateformes capables de commutation et de routage Vrf-Lite. Ceci inclut mais n'est pas limité 4500, 3750, et 3560 aux Plateformes de Catalyst 6500.
2. Toute plate-forme de routage qui exécute le Cisco IOS® approprié, qui incluent mais ne sont pas limités aux 7600, 3800, 2800, 1800, et gamme 800 ISR.
3. Le nombre d'une couche 3 saute à cloche-pied entre les parties appropriées d'infrastructure — la détermination du nombre de sauts de la couche 3 est essentielle de maintenir le déploiement aussi simple comme possible. Par exemple, s'il y avait cinq sauts de la couche 3 entre l'infrastructure qui hébergent les périphériques de CAS et les clients, il peut créer des frais d'administration.

Avec la solution incorrecte :

1. La jonction de la couche 2 crée une topologie très suboptimale de la couche 2.
2. Les sous-interfaces de la couche 3 créent beaucoup d'interfaces supplémentaires pour configurer. En conséquence ceci peut créer les questions supplémentaires d'adressage IP de temps système et de potentiel de Gestion. Ceci est illustré dans le diagramme. Si vous supposez qu'il n'y a aucune Redondance dans l'infrastructure, chaque couche du réseau représenté ont un d'entrée et l'interface physique de sortie. Le calcul pour le nombre de sous-interfaces est alors (2 * nombre de niveaux dans le réseau * (nombre de vrf)). Dans cet exemple il y a deux vrf ainsi la formule est ((2*5)*2) ou 20 sous-interfaces. Une fois que la Redondance est ajoutée ce nombre de plus que double. Comparez ceci à l'extension GRE, où seulement quatre interfaces sont exigées avec le même résultat final. Ceci illustre ordinairement comment GRE réduit excessivement l'incidence de configuration.

Jonction de la couche 2

La jonction de la couche 2 est préférée dans les scénarios où des locaux de la couche 3 ne sont

pas déployés ou où les périphériques de réseau ne prennent en charge pas GRE ou sous-interfaces. Il convient noter que 3750 et 4500 les Plateformes de Catalyst 3560, ne prennent en charge pas des sous-interfaces. Le Catalyst 3560, et 3750 également ne prennent en charge pas GRE. Le Catalyst 4500 prend en charge GRE en logiciel, et le Catalyst 6500 prend en charge GRE dans le matériel.

Dans un local de la couche 3 modèle où vous connectez une plate-forme qui ne prend en charge pas des sous-interfaces ou GRE à une plate-forme qui fait, il est préféré pour utiliser seulement la jonction de la couche 2 d'un côté, et pour utiliser des sous-interfaces de l'autre côté. Ceci te permet pour mettre à jour tous les avantages d'une architecture de local de la couche 3, et pour surmonter toujours la limite sans GRE ou la prise en charge de sous-interface sur quelques Plateformes. Un des avantages principaux de la configuration d'une jonction de la couche 2 seulement d'un côté du lien est que le spanning-tree n'est pas introduit de nouveau dans l'environnement de la couche 3. Voyez l'exemple où un commutateur d'accès de 3750 (Aucun GRE ou prise en charge de sous-interface) est connecté à un commutateur de distribution 6500, qui prend en charge GRE et sous-interfaces.

Configuration 3750 appropriée :

Dans cette configuration, notez que sur la valeur par défaut de FastEthernet 1/0/1 pour le VLAN INDIGÈNE est VLAN 1. Cette configuration n'a pas été changée. Vous notez également, cependant, qu'on ne permet pas au VLAN 1 pour être trunked à travers le lien. Les VLAN permis est limités seulement aux VLAN qui sont étiquetés. Puisque dans cette topologie de la couche 3 il n'y a aucun besoin de négociation de jonction, ou de trafic VTP d'aller du commutateur commuter, il n'y a également aucun besoin du trafic unencapsulated de transiter ce lien. Cette configuration augmente le choix de sécurité de l'architecture puisqu'il doesn pour ne pas ouvrir les failles de sécurité inutiles de la couche 2.

```
!
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
!
```

Configuration 6500 appropriée :

Dans cette configuration, notez que l'encapsulation dot1q est utilisée et les trames avec le VLAN 10, 20 et 30 sont étiquetés. Quand vous choisissez les balises VLAN pour utiliser, vous ne pouvez pas utiliser un nombre VLAN qui est déjà défini localement dans la base de données VLAN sur le commutateur.

```
!
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
!
```

Sous-interfaces de la couche 3

Les sous-interfaces de la couche 3 sont une bonne option quand vous devez seulement étendre le VRF plus d'un saut de la couche 3 dans le réseau. GRE ou sous-interfaces peut être choisi a basé à votre niveau de confort avec chaque configuration. C'est une configuration d'échantillon pour une sous-interface de la couche 3 :

```
!
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
!
```

Tunnels GRE

Les tunnels GRE sont la méthode préférée pour étendre un VRF de Vrf-Lite quand il y a de plusieurs sauts de la couche 3 entre les clients qui doivent accéder au VRF. Ce type de conception est plus commun avec la succursale distante NAC où les clients distants veulent accéder à un serveur centralement localisé NAC. Par exemple, dans un noyau typique, la distribution, des clients de modèle de réseau d'Access ne sont pas directement connectées aux distributions ou au noyau. Par conséquent, il n'y a aucun besoin d'ajouter la complexité du vrf definition sur la distribution ou les périphériques principaux. GRE peut être utilisé pour transporter simplement le trafic qui doit être localisé dans le point dans le réseau où les serveurs NAC sont connectés. C'est un exemple d'une interface de tunnel GRE.

```
!
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
!
```

Configurer le routage pour le VRF

Comme discuté plus tôt dans le document, Vrf-Lite prend en charge le BGP, l'OSPF, et l'EIGRP. Dans cet exemple de configuration, l'EIGRP est choisi parce que c'est typiquement Cisco protocole de routage recommandé mis en application sur des réseaux campus où la convergence rapide est exigée.

Il devrait noter, des travaux cet OSPF aussi bien avec Vrf-Lite, de même que fait BGP.

Il devrait également noter que si la conception exige que le trafic devrait être coulé entre les vrf, alors le BGP est exigé.

C'est un exemple de la configuration du routage pour un VRF avec l'EIGRP.

```
!
!--- 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 !
```

Acheminement du trafic entre le Tableau de routage global et le VRF modifié

Il dépend des conditions requises de déploiement NAC s'il peut être nécessaire de passer le trafic du côté non approuvé ou modifié du réseau à la faire confiance ou de nettoyer le côté du réseau. Par exemple, les services de correction peuvent potentiellement vivant du côté de confiance de l'appliance NAC. Dans le cas du Répertoire actif simple connectez-vous les déploiements, il est nécessaire pour passer un sous-ensemble du trafic au Répertoire actif pour permettre des connexions interactives, échange de ticket Kerberos, et ainsi de suite. Quoi qu'il arrive, il est très important que le Tableau de routage global sache atteindre le VRF modifié, et que le VRF MODIFIÉ sait atteindre le Tableau de routage global si n'importe quelles données doivent passer entre les deux. Ceci est typiquement manipulé par cette méthodologie.

Le VRF modifié se transfère sur l'interface non approuvée ou modifiée de l'appliance NAC. Le global a les artères statiques *seulement aux* sous-réseaux qui sont considérés des VLAN MODIFIÉS.

Considérez ce dessin.

Le premier saut de la couche 3 du côté non approuvé ou modifié de l'appliance NAC redistribue un default route dans le processus de routage ces points à l'appliance NAC. Le premier saut de la couche 3 du côté de confiance ou propre de l'appliance NAC redistribue une artère statique pour le sous-réseau qui appartient à VLAN 100, qui est dans ce cas 192.168.100.0/24.

Remarque: Le premier saut de la couche 3 des bords opposés de l'appliance NAC peut être sur le même périphérique physique, mais dans différents vrf. Dans l'exemple suivant, le côté non approuvé ou modifié du serveur NAC est dans un VRF, alors que le côté de confiance ou propre de l'appliance NAC demeure dans la table globale de routage.

La configuration est comme suit :

```
!
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
!
!!
```

Configuration du NAC pour la couche 3 OOB

Installation de CAS

Souvenez-vous notre principe du numéro un de la section d'introduction : L'astuce à une conception réussie NAC est de se souvenir toujours que le trafic classifié en tant qu'écoulement modifié de *nécessité* dans le côté non approuvé du serveur NAC (CAS).

Dans la première copie d'écran, attention de paiement à l'installation de réseau serveur NAC. Vous notez que le serveur est déployé comme passerelle Vrai-IP hors bande. Notez que le default route du serveur NAC est indiqué le côté DE CONFIANCE.

Le serveur doit être configuré avec les artères statiques pour chacun des VLAN MODIFIÉS qui existent du côté NON APPROUVÉ. Voyez la deuxième copie d'écran.

Vérifiez

Trouvez le processus documenté du NAC-`employé d'`utilisateur se connectant dans notre réseau. Cisco a capturé l'activité du commutateur d'accès, Le poste de travail, et affiche les informations des tables de routage des commutateurs de distribution.

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Étape 1 — Vous ne vous êtes pas connecté au réseau encore, et le switchport sur le commutateur d'accès Est vers le bas.

```
! – 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. !
```

Étape 2 — Le client Windows branche au réseau, et l'initiale VLAN sur le commutateur est VLAN 100 (le VLAN modifié). Une adresse IP est assignée à l'hôte, comme vous pouvez voir dans cette

copie d'écran.

```
! – 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 !
```

Étape 3 — Dans quelques secondes, l'agent NAC commence son processus de connexion. Dans cet exemple, le Répertoire actif Simple-Signe-sur est configuré, ainsi vous n'êtes pas incité pour un nom d'utilisateur et mot de passe. Au lieu de cela, vous voyez qu'une fenêtre externe qui décrit cela Simple-Signe-sur se produit.

Après l'authentification et la posture l'estimation a été terminée, un message de succès est affiché, le switchport est déplacé du VLAN modifié à l'employé VLAN et aux refreshs d'agent NAC l'adresse IP du PC.

```
! – 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 ! !
```

Cette copie d'écran affiche l'adresse IP finale, qui est dans l'employé VLAN (VLAN 200).

Cette copie d'écran affiche le périphérique de l'utilisateur de NAC-employé comme répertorié dans la liste de périphériques certifiée. Le rôle est assigné aux *EMPLOYÉS* et le VLAN est 200.

Cette copie d'écran affiche aux utilisateurs en ligne la liste sur le gestionnaire NAC.

C'est le journal d'événements de gestionnaire NAC, qui affiche la procédure de connexion réussie de l'utilisateur hors bande.

Dans cette section, les tables de routage de la table de routage globale et le VRF MODIFIÉ sont examinés. Dans la première capture d'écran, notez la commande de **show ip route**. Ceci indique que vous voyez la table de routage pour les artères globales.

```
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
```

Remarque: Le réseau 192.168.100.0/24 (le réseau modifié) est dans la table de routage comme artère statique, avec le prochain-saut étant l'interface de confiance du serveur NAC.

Notez la commande **MODIFIÉE de show ip route vrf**. Ceci indique que vous voyez la table de routage pour le réseau virtuel MODIFIÉ seulement.

```
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
```

Remarque: Notez Access modifié VLAN (192.168.100.0/24) est appris dans la distribution par l'EIGRP du commutateur d'accès de 3750, Seulement dans le Tableau de routage MODIFIÉ de VRF. Cette artère n'existe pas dans la table globale.

Annexe A : Configurations de commutateurs

Configuration en cours de commutateur d'accès

```
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
```

Configuration en cours de commutateur de distribution

```
!– 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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems