Camada 3 OOB de Cisco NAC usando VRF-Lite para o isolamento de tráfego

Índice

Introdução
Vista geral da solução
Sumário executivo
Descrição da solução
Definição simples do VRF
Arquitetura da solução
Camada de acesso
Camada de distribuição
Camada central
O centro de dados presta serviços de manutenção à camada
Componentes de solução
Gerente de Cisco NAC
Server de Cisco NAC
Agente de Cisco NAC
Considerações do projeto
Modo OOB
Classificação do valor-limite
Papéis do valor-limite
Isolamento do papel
Fluxo de tráfego
Modo de servidor de Cisco NAC
Experiência do usuário (com o agente de Cisco NAC)
Experiência do usuário (sem o agente de Cisco NAC)
Fluxos de processo de Cisco NAC
Implementação de solução de Cisco NAC
Topologia
Ordem de operação
Configuração de rede
Exemplo de configuração da camada 3 OOB VRF-Lite de Cisco NAC
Passo 1: Configurar o switch de ponta
Passo 2: Configurar o switch central
Passo 3: Configurar o interruptor de centro de dados
Passo 4: Execute a instalação inicial do Cisco NAC Manager and Server
Passo 5: Aplique uma licença ao gerente de Cisco NAC
Passo 6: Políticas da atualização de Cisco.com no gerente de Cisco NAC
Passo 7: Instale Certificados de um Certificate Authority (CA) da terceira

Passo 8: Instalação do server de Cisco NAC da revisão
Etapa 9: Adicionar o server de Cisco NAC ao gerente de Cisco NAC
Etapa 10: Configurar o server de Cisco NAC
Etapa 11: Permita o apoio da camada 3
Etapa 12: Configurar rotas estáticas
Passo 13: Perfis estabelecidos para o Switches no gerente de Cisco NAC
Passo 14: Configurar ajustes do receptor SNMP
Etapa 15: Adicionar o Switches como dispositivos no gerente de Cisco NAC
Passo 16: Configurar portas de switch para que os dispositivos sejam controlados pelo NAC
Etapa 17: Configurar papéis de usuário
Etapa 18: Adicionar usuários e atribua-os para apropriar o papel de usuário
Etapa 19: Personalize a página do login de usuário para o início de uma sessão da Web
Etapa 20: Personalize o agente de Cisco NAC para os papéis de usuário
Etapa 21: Distribua o host da descoberta para o agente de Cisco NAC
Etapa 22: Início de uma sessão da Web
Etapa 23: Início de uma sessão do agente
Apêndice
Alta Disponibilidade
Diretório ativo SingleSignOn (diretório ativo SSO)
Considerações do ambiente do domínio do Windows
Configurar a ferramenta NAC de Cisco para o início de uma sessão do agente e a avaliação da postura do cliente
Informações Relacionadas

Introdução

Este guia descreve uma implantação do Cisco Network Admission Control (NAC) em uma implementação de Camada 3 Out-of-Band (OOB) baseada no virtual route forwarding (VRF)-Lite.

Vista geral da solução

Esta seção dá uma breve introdução para mergulhar 3 OOB usando métodos de VRF-Lite a fim executar uma arquitetura NAC.

Sumário executivo

Cisco NAC reforça as políticas de segurança de rede de uma organização em todos os dispositivos que procuram o acesso de rede. Cisco NAC permite somente dispositivos de ponto final complacentes e confiados, tais como PC, server, e PDA, na rede. Cisco NAC restringe o acesso de dispositivos noncompliant, que limita o dano potencial das ameaças de segurança e dos riscos emergentes. Cisco NAC dá a organizações um método poderoso, papel-baseado a fim impedir o acesso não autorizado e melhorar a elasticidade de rede.

A solução de Cisco NAC fornece estes benefícios para os negócios:

- **Conformidade da política de segurança** — Assegura-se de que os valores-limite se conformem à política de segurança; protege a infraestrutura e a produtividade do funcionário;

fixa ativos controlados e unmanaged; ambientes internos dos apoios e acesso do convidado; costura políticas a seu nível de risco
- **Protege investimentos existentes** — É compatível com aplicativos de gerenciamento de terceira parte; as opções de distribuição flexíveis minimizam a necessidade para elevações da infraestrutura
- **Abranda riscos dos vírus, dos worms, e dos controles de acesso desautorizados** e reduz rompimentos em grande escala da infraestrutura; reduz despesas de funcionamento fazendo movimentos, adiciona, e muda dinâmico e automatizado, assim permitindo uma eficiência mais alta TI; integra com outros componentes da rede de auto-definição de Cisco a fim entregar a proteção de segurança detalhada

Descrição da solução

Cisco NAC é usado na infraestrutura de rede a fim reforçar a conformidade da política de segurança em todos os dispositivos que procuram o acesso aos recursos de rede. Cisco NAC permite que os administradores de rede autentiquem e autorizem usuários e avaliem-nos e remediate suas máquinas associadas antes que estejam concedidos o acesso de rede. Você pode usar diversos métodos de configuração para realizar esta tarefa. Este documento centra-se especificamente sobre a aplicação VRF-baseada de Cisco NAC em um desenvolvimento da camada 3 OOB onde o server de Cisco NAC (servidor de acesso limpo de Cisco) seja configurado no modo (roteado) real do IP gateway.

A camada 3 OOB é uma das metodologias as mais populares do desenvolvimento para o NAC. Esta SHIFT na popularidade é baseada em diversa dinâmica que inclui a melhor utilização dos recursos do hardware. Distribuindo Cisco NAC em uma metodologia da camada 3 OOB, uma única ferramenta NAC de Cisco pode escalar para acomodar mais usuários. Igualmente permite que as ferramentas NAC de Cisco sejam ficadas situadas centralmente um pouco do que distribuída através do terreno ou da organização. Consequentemente, as disposições da camada 3 OOB são mais eficazes na redução de custos ambos de um ponto de vista do capital e das despesas operacionais.

Este guia descreve uma aplicação de Cisco NAC em um desenvolvimento da camada 3 OOB que seja baseado em VRF-Lite.

Definição simples do VRF

Uma maneira de olhar a virtualização do dispositivo VRF é igualá-la ao advento dos VLAN. Os VLAN criaram virtuais switch fora de um único interruptor físico. Os VRF estendem essa virtualização após o limite da camada 2, e permitem a criação dos roteadores virtuais. Os roteadores virtuais preveem redes completo-virtualizadas de fim-a-fim.

Uma outra maneira de olhar o projeto VRF é que cada VRF atua apenas como um VPN ou um túnel. O tráfego que é colocado em um VRF não pode comunicar-se fora do VRF (túnel) até que o tráfego passe através do dispositivo que termina o túnel (o VPN Router do destino).

Nota: Estas definições são significadas ajudar a introduzir um novo conceito. Estas definições não são representações ou definições oficial exatas do VRF.

Figura 1 mostra uma ilustração da virtualização do dispositivo com VRF. Cada camada colorida no diagrama representa um roteador virtual diferente, ou o VRF. A metodologia VRF fornece o isolamento plano do plano do controle e do trajeto dos dados, junto com a capacidade para ter

planos isolados múltiplo dos dados. Ou seja fornece a possibilidade para um roteador virtual separado ou a rede para cada tipo de tráfego que é esperado em um ambiente que use Cisco NAC. Os tipos de tráfego típicos são:

- Tráfego de usuário não-autenticado
- Tráfego do usuário autenticado
- Tráfego do contratante
- Tráfego do convidado

Figura 1 – ***Virtualização do dispositivo***

Arquitetura da solução

Os server de Cisco NAC foram projetados inicialmente ser dispositivos da em-faixa. O uso de ferramentas NAC de Cisco em uma infraestrutura de rede Cisco permite que você tome um dispositivo que seja projetado ser em-faixa a todo o tráfego de rede, e distribui-o com uma metodologia OOB.

A arquitetura da solução (veja figura 2) identifica os componentes de solução e o ponto chaves da integração do server de Cisco NAC.

Nota: Neste documento, os termos “switch de ponta” e “switch de acesso” são usados permutavelmente.

Figura 2 – ***Arquitetura da solução***

As próximas seções descrevem o acesso, a distribuição, o núcleo, e as camadas do centro de dados que compõem uma arquitetura típica do terreno.

Camada de acesso

A solução da camada 3 OOB Cisco NAC é aplicável a um projeto de campus roteado do acesso. No modo de acesso roteado, as interfaces virtuais comutadas da camada 3 (SVI) são configuradas no switch de acesso. Como figura 3 mostra, o acesso VLAN da camada 3 (por exemplo, VLAN 100) é configurado no switch de ponta, mergulha 3 que o roteamento é apoiado do interruptor ao switch de distribuição ou ao roteador ascendente, e o gerente de Cisco NAC controla as portas no switch de acesso.

Figura 3 – ***Switch de acesso com camada 3 à borda***

Camada de distribuição

A camada de distribuição é responsável para o roteamento da camada 3 e a agregação dos switch de camada de acesso. Quando você puder colocar os server de Cisco NAC nesta camada em um projeto da camada 2 OOB, você não os encontra aqui em um projeto da camada 3 OOB. Em lugar de, coloque os server de Cisco NAC centralmente no bloco do serviço do centro de dados, como a arquitetura da solução mostra (figura 2).

Camada central

A camada central usa roteadores baseado em IOS de Cisco. A camada central é reservada para o roteamento de alta velocidade, sem nenhuns serviços. Coloque serviços em um interruptor do serviço no centro de dados.

O centro de dados presta serviços de manutenção à camada

O centro de dados presta serviços de manutenção a roteadores baseado em IOS e a Switches de Cisco dos usos da camada na rede do campus. O gerente de Cisco NAC e o server de Cisco NAC são ficados situado centralmente no bloco do serviço do centro de dados neste projeto da camada 3 OOB.

Componentes de solução

Gerente de Cisco NAC

O gerente de Cisco NAC é o servidor de administração e o base de dados que centraliza a configuração e a monitoração de todos os server, usuários, e políticas de Cisco NAC em um desenvolvimento da ferramenta NAC de Cisco. Para um desenvolvimento OOB Cisco NAC, o gerente de Cisco NAC fornece o Gerenciamento OOB a fim adicionar e o Switches de controle no domínio do gerente de Cisco NAC e configurar portas de switch.

Server de Cisco NAC

O server de Cisco NAC é o ponto da aplicação entre a rede (controlada) não confiável e a rede (interna) confiada. O server reforça policia definido no gerente de Cisco NAC, e os valores-limite comunicam-se com o server durante a autenticação. Neste projeto, o server separa logicamente o não-confiável e as redes confiável, e serve como o ponto centralizado da aplicação para todas as Listas de acesso (ACL) e restrições de largura de banda para dispositivos na rede não confiável. Veja a seção de modo OOB para mais informação.

Agente de Cisco NAC

O agente de Cisco NAC é um componente opcional da solução de Cisco NAC. Quando o agente é permitido para seu desenvolvimento de Cisco NAC, assegura-se de que os computadores que alcançam sua reunião da rede as exigências da postura do sistema você especifiquem. O agente é um de leitura apenas, fácil de usar, o programa da pequeno-pegada que reside em máquinas do usuário. Quando um usuário tenta alcançar a rede, o agente verifica o sistema de cliente para ver se há o software que você exige, e ajuda-o a adquirir todas as atualizações ou software faltante. Veja a etapa 6: Atualize políticas do cisco.com no gerente de Cisco NAC para mais informação.

Considerações do projeto

Quando você considera um desenvolvimento da camada 3 OOB NAC, reveja diversas considerações de projeto. Estas considerações são alistadas nestas subseções, junto com uma breve discussão de sua importância.

Modo OOB

No desenvolvimento da ferramenta NAC OOB de Cisco, o server NAC comunica-se com o host final somente durante o processo de autenticação, posture a avaliação, e a remediação. Depois que o host final é certificado, não se comunica com o server.

No modo OOB, o gerente de Cisco NAC usa o Switches de controle do Simple Network Management Protocol (SNMP) e as atribuições de VLAN do grupo para portas. Quando o Cisco NAC Manager and Server se estabelece para OOB, o gerente pode controlar as portas de switch do Switches apoiado. O controle das portas de switch é sabido como o plano do controle SNMP. Para uma lista de modelos de switch apoiados, refira a seção *apoiada OOB do Switches do* apoio do interruptor para a ferramenta NAC de Cisco.

O modo OOB é usado primeiramente para disposições prendidas. Quando o método VRF da camada 3 OOB é usado, todo o tráfego do não-confiável VLAN (sujos), incluindo o tráfego do agente, alcança o server centralizado de Cisco NAC onde toda a aplicação ocorre. A aplicação do tráfego no server é um diferenciador de tecla entre o método VRF e o método ACL da camada 3 OOB.

Nota: O server de Cisco NAC foi projetado originalmente para ser um dispositivo da em-faixa. Ou seja o server foi projetado mandar todo o tráfego correr através d, que permitiria que o server fosse o ponto de controle. Quando você usa o método VRF da camada 3 OOB, todo o tráfego de usuário não-autenticado corre através do server exatamente como se era um desenvolvimento da em-faixa. Este fluxo de tráfego permite um ambiente consistente, predizível.

Classificação do valor-limite

Diversos fatores contribuem à classificação do valor-limite, e incluem tipos de dispositivo e papéis de usuário. O tipo de dispositivo e o papel de usuário impactam o papel do valor-limite.

Estes são os tipos de dispositivo possíveis:

- Dispositivos corporativos
- dispositivos NON-corporativos
- Dispositivos NON-PC

Estes são os papéis de usuário possíveis:

- Empregado
- Contratante
- Convidados

Inicialmente, todos os valores-limite são atribuídos ao VLAN não-autenticado. O acesso aos outros papéis é permitido depois que o processo da identidade e da postura está completo.

Papéis do valor-limite

O papel de cada tipo de valor-limite deve inicialmente ser determinado. Um desenvolvimento típico do terreno inclui diversos papéis, tais como empregados, convidados, contratantes, e outros valores-limite tais como impressoras, pontos de acesso Wireless, e câmeras IP. Os papéis são traçados ao switch de ponta VLAN.

Nota: Um papel adicional é exigido para a autenticação a que todos os valores-limite pertencem inicialmente. Este papel traça a um VLAN “sujo” não-autenticado.

Isolamento do papel

Para este tipo de projeto NAC, o tráfego classificado como “sujo” deve fluir no lado “não confiável”

do server de Cisco NAC. Mantenha este princípio na mente quando você projetar uma aplicação de Cisco NAC. Adicionalmente, não permita “limpam” e redes “sujas” para comunicar-se diretamente um com o otro.

Figura 4 mostra que quando os usos VRF de um projeto da camada 3 OOB, o VRF se asseguram de que as sobras não-autenticados do tráfego isoladas em sua própria rede virtual. O server de Cisco NAC atua como o ponto da aplicação ou o controlador que assegura a segregação e a comunicação segura entre “limpa” e redes “sujas”.

Figura 4 – *O server de Cisco NAC conecta aos lados sujos e limpos*

Fluxo de tráfego

O processo NAC começa quando um valor-limite é conectado a um switchport NAC-controlado. O tráfego classificado como “sujo” ou “não-autenticado” está isolado do resto das redes enquanto está no VRF “sujo”. Este tráfego é isolado e enviado à interface não confiável no server de Cisco NAC. Veja a figura 4.

Nota: A ferramenta NAC de Cisco é alheado a como o tráfego lhe é apresentado. Ou seja o dispositivo próprio não tem nenhuma preferência se o tráfego chega através de um túnel de encapsulamento de roteamento genérico (GRE) ou está reorientado com uma configuração do roteamento baseado em política, VRF-roteado, ou outros métodos de redirecionamento.

Modo de servidor de Cisco NAC

Você pode distribuir um server de Cisco NAC em um destes dois modos:

- Modo virtual do gateway (ponte)
- Modo (roteado) real do IP gateway

Modo virtual do gateway (ponte)

O modo virtual do gateway (ponte) é usado tipicamente quando o server de Cisco NAC é a camada 2 junto aos valores-limite. Neste modo, o server atua como uma ponte e não é envolvido na decisão de roteamento do tráfego de rede.

Nota: Este modo não é aplicável para este projeto particular ACL.

Modo (roteado) do gateway Real-IP

O modo (roteado) do gateway real-IP é mais aplicável em um projeto onde o server de Cisco NAC seja saltos da camada múltipla 3 longe do valor-limite, tal como a camada 3 OOB. Quando você usa o server como um gateway real-IP, especifique os endereços IP de Um ou Mais Servidores Cisco ICM NT de suas duas relações: um para o lado confiado (Gerenciamento do server) e um para o lado (sujo) não confiável. Os dois endereços devem estar em sub-redes diferentes. O IP da interface não confiável é usado comunicando-se com o valor-limite na sub-rede não confiável. O modo que este guia usa é o gateway real-IP.

Experiência do usuário (com o agente de Cisco NAC)

Tipicamente, as entidades corporativas têm o agente de Cisco NAC distribuído adiantado aos

clientes da extremidade. A configuração de host da descoberta no agente provoca os pacotes de descoberta a ser enviados à interface não confiável do server de Cisco NAC, que continua automaticamente o valor-limite com o processo NAC.

Em uma camada 3 OOB com modelo VRF, o host da descoberta é ajustado tipicamente para ser o nome de DNS ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do gerente de Cisco NAC. O gerente existe na rede limpa. Porque todo o tráfego das redes “sujas” é distribuído à revelia através do server de Cisco NAC, os pacotes de descoberta correm através automaticamente do server. O fluxo de tráfego descrito aqui é um dos benefícios ao método VRF. Este fluxo de tráfego prevê uma experiência consistente, predizível. Veja fluxos de processo de Cisco NAC para mais informação.

Experiência do usuário (sem o agente de Cisco NAC)

A capacidade para operar-se sem um agente de Cisco NAC é um outro benefício do modelo VRF. Todo o tráfego das redes “sujas” é distribuído naturalmente através do server de Cisco NAC. Isto significa que um usuário em uma máquina sem um agente de Cisco NAC somente tem que abrir um navegador da Web e consultar a todo o Web site válido. O tráfego do navegador tenta passar através do server, que por sua vez captura a sessão de navegador e a reorienta a um portal prisioneiro. Veja fluxos de processo de Cisco NAC para mais informação.

Nota: Para a melhor experiência de usuário final possível, Certificados do uso que são confiados pelo navegador do utilizador final. os Certificados Auto-gerados no server de Cisco NAC e no gerente de Cisco NAC não são recomendados para um ambiente de produção.

Nota: Gerencia sempre o certificado para o server de Cisco NAC com o endereço IP de Um ou Mais Servidores Cisco ICM NT de sua interface não confiável.

Fluxos de processo de Cisco NAC

Esta seção explica o fluxo de processo básico para uma solução NAC OOB. As encenações são ambos descritos com e sem um agente de Cisco NAC instalado na máquina cliente. Esta seção mostra como o gerente de Cisco NAC controla as portas de switch usando o SNMP como o media do controle. Estes fluxos de processo são macroanalíticos na natureza e contêm somente etapas funcionais da decisão. Os fluxos de processo não incluem cada opção nem pisam que ocorre e não incluem as decisões de autorização que são baseadas em critérios de avaliação do valor-limite.

Refira o diagrama de fluxo de processo na figura 6 para as etapas circundadas que estão na figura 5.

Figura 5 – ***Fluxo de processo NAC para a solução da camada 3 OOB Cisco NAC*** **Figura 6 –** ***Diagrama de bloco do fluxo de processo de Cisco NAC***

Implementação de solução de Cisco NAC

Esta seção descreve como executar uma solução de Cisco NAC.

Topologia

A figura 7 mostra a topologia usada para a criação deste guia. A rede interna, que consiste em

VLAN 200 e 210, é distribuída usando a tabela de roteamento global. A rede interna não tem nenhum VRF associado com ela.

O VRF sujo contém somente o VLAN SUJO e as redes associadas do trânsito que são precisados a fim criar uma única rede virtual para que todo o tráfego sujo flua ao lado sujo do server centralizado de Cisco NAC.

O convidado VRF contém os CONVIDADOS VLAN e as redes associadas do trânsito que são precisados a fim terminar todos os dados de origem dos CONVIDADOS VLAN em uma secundário-relação separada no Firewall. Cada um das três redes virtuais (SUJAS, CONVIDADOS, e GLOBAL) é levada na mesma infraestrutura física e fornece o isolamento completo do tráfego e do trajeto.

Figura 7 – *Topologia usada neste guia*

Ordem de operação

O ordem de operação para o desenvolvimento de uma solução de Cisco NAC é facilmente acima para o debate. Você configura a parcela NAC da solução antes que a rede esteja preparada? Ou, você prepara a rede antes que você configure os dispositivos de Cisco NAC?

Para fins da organização, este guia centra-se sobre a configuração de rede primeiramente. Isto assegura-se de que a rede esteja pronta para o NAC, então a configuração do Produtos de Cisco NAC.

Configuração de rede

Este guia focaliza em VRF-Lite fim-a-fim para o isolamento do trajeto. É importante notar que você pode usar VRF com um túnel GRE a fim permitir o isolamento do trajeto através de uma distribuição e de uma camada central existentes, sem exigir nenhuma configuração naqueles dispositivos. Para obter mais informações sobre de quando e por que usar os túneis GRE comparados a um VRF fim-a-fim projete, veja que o alargamento que um VRF entre dois dispositivos seciona. Você pode igualmente referir a camada 3 NAC do Guia de Design da faixa que usa VRF-Lite para o isolamento de tráfego.

Este documento é um Guia de Design completo focalizado no VRF-Lite com método GRE.

Adicionalmente, o switching de caractere completo pode ser usado no lugar de VRF-Lite onde aplicável. O switching de caractere é considerado para fora--espaço para fins deste documento.

Considerações importantes para VRF-Lite

Nota: VRF-Lite é uma característica que o permita de apoiar dois ou mais redes virtuais. VRF-Lite igualmente permite endereços IP de Um ou Mais Servidores Cisco ICM NT de sobreposição entre as redes virtuais. Contudo, a sobreposição do endereço IP de Um ou Mais Servidores Cisco ICM NT não é recomendada para uma aplicação NAC, porque quando a infraestrutura própria apoiar os endereços de sobreposição, pode criar complexidades do Troubleshooting e o relatório incorreto.

Detalhes dados nas etapas fornecidas neste esboço da seção as etapas necessárias a fim configurar sua rede para o isolamento do trajeto usando VRF-Lite. A configuração exigida introduzindo a ferramenta NAC de Cisco em sua rede como um gateway real-IP da camada 3

OOB é fornecida igualmente.

As interfaces de entrada dos usos de VRF-Lite a fim distinguir rotas para redes virtuais e formulários diferentes separam tabelas de roteamento virtual associando uns ou vários relações da camada 3 com cada VRF. As relações em um VRF podem ser ou exame, tal como portas Ethernet, ou podem ser ou lógico, como subinterfaces, interfaces de túnel, ou interfaces virtuais do interruptor VLAN (SVI).

Nota: Uma relação da camada 3 não pode pertencer a mais de um VRF de cada vez.

Note estas considerações de VRF-Lite:

- VRF-Lite está localmente - significativo somente ao interruptor onde é definido, e à Associação de VRF é determinado pela interface de entrada. Nenhuma manipulação do cabeçalho de pacote de informação ou do payload é executada.
- Um interruptor com VRF-Lite é compartilhado por redes virtuais múltiplas (domínios de segurança), e todos os domínios de segurança têm suas próprias tabelas de roteamento originais.
- Todos os domínios de segurança devem ter seus próprios VLAN.
- VRF-Lite não apoia todo o Multiprotocol Label Switching (MPLS) - A funcionalidade VRF tal como a troca da etiqueta, a adjacência do protocolo de distribuição de rótulo (LDP), ou os pacotes rotulados que são igualmente sabem como o tag-switching).
- O recurso do Ternary Content Addressable Memory da camada 3 (TCAM) é compartilhado entre todos os VRF. A fim assegurar-se de que todo o um VRF tenha o suficiente espaço da memória endereçável satisfeita (CAM), use o **comando maximum routes**.
- Um Catalyst Switch que usa VRF-Lite pode apoiar uma rede global e até 64 VRF. O número total de rotas apoiadas é limitado pelo tamanho do TCAM.
- Você pode usar a maioria de protocolos de roteamento tais como o Border Gateway Protocol (BGP), o Open Shortest Path First (OSPF), o Enhanced Interior Gateway Routing Protocol (EIGRP), o Routing Information Protocol (RIP), e o roteamento estático entre os dispositivos que executam VRF-Lite.
- Na maioria dos casos, não há nenhuma necessidade de executar o BGP com VRF-Lite.
- VRF-Lite não afeta a taxa do packet switching.
- Você não pode configurar o Multicast e o VRF-Lite no mesmos relação da camada 3 ao mesmo tempo.
- Use o subcommand de VRF-**lite da capacidade** sob o roteador OSPF quando você configura o OSPF como o protocolo de roteamento entre dispositivos de rede.

Defina um VRF

Neste exemplo de design, o isolamento do trajeto deve ser fornecido para usuários e convidados não-autenticados ou sujos. Todo tráfego restante é permitido para usar a rede interna. Você deve definir dois VRF enquanto esta configuração mostra:

Exemplo da configuração de VRF

```
!--- This command creates a VRF for the DIRTY virtual
network: ! ip vrf DIRTY ! !--- This command 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
100:3 ! !--- 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). ! !--- This document uses
the Autonomous System number and a unique router-id in
that AS. !--- This example signifies AS 100:Router-ID 3
!
```

Nota: O distinguidor de rota não é uma configuração requerida para VRF-Lite. Contudo, considera-se um melhor prática configurar o distinguidor de rota para o futuro, de modo que trabalhe continuamente com switching de caractere.

```
! -- Here we create a VRF for the GUEST Virtual Network: ! ip vrf GUESTSdescription
GUESTS_VRF_FOR_VISITORSrd 600:3 !
```

Associe um VLAN ou conecte-o com um VRF

Depois que o VRF é definido no switch de camada 3 ou no roteador, você deve associar as relações que estão indo participar na configuração de VRF-Lite com o VRF onde pertencem. Você pode associar o exame ou as interfaces virtuais com um VRF. Esta seção fornecem exemplos de uma interface física, uma relação secundária, um Switched Virtual Interface, e uma interface de túnel que todos são associados com um VRF.

Nota: Os exemplos são amostras somente, e não foram usados na topologia deste documento.

Exemplo da configuração de interface física

```
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
```

Exemplo de configuração da Secundário-relação

```
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
```

Exemplo de configuração do Switched Virtual Interface

```
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
```

Exemplo de configuração da interface de túnel

```
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
```

Estenda um dispositivo VRF entre dois dispositivos

Há diversas metodologias que aceitáveis você pode se usar a fim estender um VRF entre duas partes de infraestrutura. Certifique-se de que o método que você escolhe está baseado nestes critérios:

- Considere as capacidades da plataforma. Todo o Cisco atual mergulha o apoio VRF-Lite da empresa 3-capable do interruptor e de plataformas de roteamento. Estas Plataformas incluem, mas não são limitadas a, 4500, 3750, e 3560 as Plataformas do Catalyst 6500.
- Uma plataforma de roteamento deve executar os IO apropriados. As Plataformas incluem, mas não são limitadas a, os 7600, os 3900, a 3800, 2900, 2800, 1900, 1800, e o Roteadores dos Serviços integrados do 800 Series (ISR).
- Considere o número de saltos da camada 3 entre partes relevantes de infraestrutura. A fim determinar o número de saltos da camada 3, mantenha o desenvolvimento tão simples quanto possível. Por exemplo, se cinco saltos da camada 3 existem entre a infraestrutura que hospeda os dispositivos da sinalização associada a canal (CAS) e os clientes, pode criar a carga adicional administrativa.

Com a solução incorreta:

- O entroncamento da camada 2 cria uma topologia muito secundário-ótima da camada 2.
- As subinterfaces da camada 3 criam muitas interfaces adicionais para configurar. Mais relações a configurar podem criar edições adicionais do endereçamento de IP da carga adicional de gerenciamento e do potencial. Com a suposição que não há nenhuma Redundância na infraestrutura, cada camada da rede tem um ingresso e a interface física da saída. A computação para o número de subi-nterfaces é então (2 * número de séries na rede * número de VRF). Nosso exemplo tem dois VRF, assim que a fórmula é (2 *5 * 2) ou 20 subinterfaces. Depois que a Redundância é adicionada, este número mais do que dobra. Compare isto à extensão GRE, onde somente quatro relações são exigidas com o mesmo resultado final. Esta comparação ilustra como o GRE reduz o impacto da configuração.

Entroncamento da camada 2

O entroncamento da camada 2 é preferido nas encenações onde os dispositivos da camada de acesso não apoiam subinterfaces. As 4500 Plataformas do catalizador 3560, 3750, e não apoiam subinterfaces.

Em uma camada 3 alcance o modelo que conecta a uma plataforma que não apoie subinterfaces a uma plataforma que faça, simplesmente entroncamento da camada 2 do uso em um lado e em subinterfaces do uso no outro lado. Esta configuração mantém todos os benefícios de uma arquitetura do armário da camada 3 e ainda supera a limitação de nenhum apoio da secundário-relação em algumas Plataformas.

Uma das vantagens preliminares de configurar o entroncamento da camada 2 em somente um lado do link é que medindo - a árvore não é introduzida de novo no ambiente da camada 3. Veja o exemplo de 3750 configurações relevantes onde um switch de acesso 3750. qual não apoia o GRE ou as subinterfaces, é conectado a um switch de distribuição 6500. O switch de distribuição 6500 apoia o GRE e as subinterfaces.

Configuração relevante 3750

Nesta configuração, a configuração padrão para o VLAN NATIVO é VLAN1 nos FastEthernet 1/0/1. Esta configuração não foi mudada. Contudo, o VLAN1 não é permitido ser em tronco através do link. Os VLAN permitidos são limitados somente aos VLAN que são etiquetados.

Não há nenhuma necessidade para a negociação de tronco do switch para switch ou o tráfego do protocolo VLAN Trunk (VTP) nesta topologia da camada 3. Consequentemente, não há igualmente nenhuma necessidade para que nenhum tráfego sem etiqueta seja transmitido neste

link. Esta configuração aumenta a postura de segurança da arquitetura porque não abre furos de segurança desnecessários da camada 2.

Exemplo de 3750 configurações relevantes

```
!--- 3750 Switch configuration, related to connecting it
to a !--- sub-interface capable switch (Catalyst 6500):
! ip vrf DIRTY rd 100:1 ! ip vrf GUEST rd 600:1 !
interface GigabitEthernet1/0/48 description Uplink to
Cat6k switchport trunk encapsulation dot1q switchport
trunk allowed vlan 901-903,906 switchport mode trunk
spanning-tree portfast trunk ! !--- Since the 3750 does
not support sub-interfaces, !--- you must configure one
SVI per transit network: ! interface Vlan901 description
DIRTY_TRANSIT ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 ! interface Vlan902
description GLOBAL_TRANSIT ip address 172.26.120.6
255.255.255.252 ! interface Vlan906 description
GUEST_TRANSIT ip vrf forwarding GUEST ip address
172.26.120.14 255.255.255.252 ! !--- This configuration
uses EIGRP as the routing protocol !--- of choice in
this document. !--- Each VRF is defined as a separate !-
-- Autonomous System under the Global AS. ! router eigrp
26 ! address-family ipv4 vrf DIRTY network 172.26.120.0
0.0.0.255 autonomous-system 100 no auto-summary exit-
address-family ! address-family ipv4 vrf GUEST
redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family network 172.26.0.0
```

Configuração relevante 6500

Nesta configuração, o encapsulamento do dot1q é usado a fim etiquetar os quadros com o VLAN 901, 902, e 906. Quando você seleciona o VLAN etiqueta para usar-se em uma secundário-relação, você não pode usar um número de VLAN que seja definido já localmente na base de dados de VLAN no interruptor.

Exemplo de 6500 configurações relevantes

```
!--- 6500 Switch configuration, related to connecting it
!--- to a non-sub-interface capable switch (Catalyst
3750): ! ip vrf DIRTY rd 100:26 ! ip vrf GUEST rd 600:26
! interface FastEthernet1/34 description NAC LAB - 3750
no ip address ! interface FastEthernet1/34.901
encapsulation dot1Q 901 ip vrf forwarding DIRTY ip
address 172.26.120.1 255.255.255.252 ! interface
FastEthernet1/34.902 encapsulation dot1Q 902 ip address
172.26.120.5 255.255.255.252 ! interface
FastEthernet1/34.906 encapsulation dot1Q 906 ip vrf
forwarding GUEST ip address 172.26.120.13
255.255.255.252 ! !--- EIGRP is the routing protocol of
choice in this document. !--- Each VRF is defined as a
!--- separate Autonomous System under the Global AS. !--
- See Configure Routing for the VRF for more
information. ! router eigrp 26 network 172.26.0.0
0.0.255.255 no auto-summary passive-interface Vlan1
redistribute static ! address-family ipv4 vrf DIRTY
autonomous-system 100 network 172.26.120.0 0.0.0.3
network 172.26.160.0 0.0.0.255 no auto-summary no
default-information out redistribute static route-map
```

```
gw-route exit-address-family ! address-family ipv4 vrf
GUEST redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family !
```

Configurar o roteamento para o VRF

Como discutido mais cedo nas considerações importantes para usar a seção de VRF-Lite, VRF-Lite apoia o BGP, o OSPF, e o EIGRP. Neste exemplo de configuração, o EIGRP é selecionado porque é o protocolo de roteamento que Cisco recomenda para a aplicação em redes do campus onde a convergência rápida é exigida.

Nota: O OSPF trabalha igualmente bem com VRF-Lite, como faz BGP.

Nota: O BGP é exigido se o projeto exige que o tráfego “esteja escapado” entre VRF.

Roteamento para um VRF com exemplo de configuração EIGRP

```
!
!--- This base routing protocol configuration handles
the routing !--- for the Global Routing Table. ! router
eigrp 26 network 172.26.50.0 0.0.0.255 network
172.26.51.0 0.0.0.255 network 172.26.52.0 0.0.0.255
network 172.26.55.0 0.0.0.255 network 172.26.60.0
0.0.0.255 network 172.26.61.0 0.0.0.255 network
172.26.62.0 0.0.0.255 network 172.26.120.4 0.0.0.3
network 172.26.176.0 0.0.0.255 network 172.26.254.1
0.0.0.0 no auto-summary passive-interface Vlan1
redistribute static ! !--- You must define an address
family for each VRF !--- that is to be routing using the
routing protocol. !--- Routing protocol options such as
auto-summarization, !--- AS number, and router id are
all configured under the !--- address family. EIGRP does
not form a neighbor !--- relationship without the AS
specified under the address family. !--- Also, this AS
number needs to be unique for !--- each VRF and cannot
be the same as the global AS number. ! address-family
ipv4 vrf DIRTY autonomous-system 100 network
172.26.120.0 0.0.0.3 network 172.26.160.0 0.0.0.255 no
auto-summary no default-information out redistribute
static route-map gw-route exit-address-family ! address-
family ipv4 vrf GUEST redistribute static network
172.26.120.0 0.0.0.255 autonomous-system 600 no auto-
summary exit-address-family !
```

Tráfego da rota entre a tabela de roteamento global e o VRF sujo

Segundo as exigências do desenvolvimento NAC, pode ser necessário passar o tráfego do lado não confiável ou sujo da rede à confiada ou limpar o lado da rede. Por exemplo, os serviços da remediação podem potencialmente viver no lado confiado da ferramenta NAC de Cisco. No caso do diretório ativo único sinal-em disposições, é necessário passar um subconjunto do tráfego ao diretório ativo a fim permitir a troca interativa do bilhete do Kerberos dos fazer logon, e assim por diante.

Em todos os casos, é muito importante que a tabela de roteamento global sabe alcançar o VRF sujo, e que o VRF sujo sabe alcançar a tabela de roteamento global se algum dados precisa de

passar entre os dois. Isto é segurado tipicamente pela metodologia em figura 8.

O VRF sujo opta a relação não confiável ou suja da ferramenta NAC de Cisco. O global tem rotas estáticas somente às sub-redes que são consideradas VLAN sujos. Aquelas rotas estáticas apontam à relação (confiada) limpa do server de Cisco NAC como o salto seguinte.

Figura 8 – ***Distribuindo fluxos***

O primeiro salto da camada 3 no lado não confiável ou sujo da ferramenta NAC de Cisco redistribui uma rota padrão em um processo de roteamento esses pontos à ferramenta NAC de Cisco. O primeiro salto da camada 3 no lado confiado ou limpo da ferramenta NAC de Cisco redistribui uma rota estática para as sub-redes que pertencem ao VLAN sujo na camada de acesso (neste caso 172.26.123.0/26).

Nota: O primeiro salto da camada 3 em lados opostos da ferramenta NAC de Cisco pode estar no mesmo dispositivo físico, mas em VRF diferentes.

Nota: Na topologia usada para este documento, o lado não confiável ou sujo do server de Cisco NAC está em um VRF, quando o lado confiado ou limpo da ferramenta NAC de Cisco permanecer na tabela de roteamento global. Contudo, ambas as relações são conectadas ao mesmo interruptor de centro de dados.

Exemplo de configuração da camada 3 OOB VRF-Lite de Cisco NAC

A fim distribuir com sucesso uma solução de Cisco NAC OOB, você precisa de configurar os componentes NAC a fim combinar a arquitetura desejada. A figura 9 é um diagrama de rede lógica de Cisco NAC OOB da camada 3 que seja usado nesta seção a fim mostrar a configuração relevante do gerente de Cisco NAC, do server de Cisco NAC, e do switch de ponta para uma camada 3 OOB NAC com desenvolvimento de VRF-Lite.

Figura 9 – ***Topologia lógica da camada 3 OOB de Cisco NAC***

Termine as etapas nestas seções a fim configurar um desenvolvimento real-IP OOB VRF Cisco NAC da camada 3:

Passo 1: Configurar o switch de ponta

Como estes exemplos de configuração mostram, crie dois mais VLAN (SUJOS e CONVIDADO) no switch de ponta.

A produção existente VLAN (VLAN 200) é usada para todos os sistemas corporativos. Este exemplo cria os VLAN, suas redes associadas do trânsito, e atribui ambos aos VRF corretos. A aplicação ocorre no server de Cisco NAC, assim que você não precisa de aplicar ACL a cada VLAN no interruptor.

Papel não autenticado: VLAN 100, exemplo sujo da configuração de VRF
`!--- Define the DIRTY VRF.` ip vrf DIRTY rd 100:3 `!--- Create the SVI for the DIRTY VLAN.` interface Vlan100 ip vrf forwarding DIRTY ip address 172.26.123.1 255.255.255.224 ip helper-address vrf DIRTY 172.26.51.11

```
!--- Create the SVI for the DIRTY_TRANSIT_NETWORK.
interface Vlan301 ip vrf forwarding DIRTY ip address
172.26.120.50 255.255.255.252 !--- Set the allowed VLAN
on the trunk. interface FastEthernet1/0/48 switchport
trunk allowed vlan add 301 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf DIRTY
network 172.26.0.0 autonomous-system 100 no auto-summary
exit-address-family
```

Papel de convidado: VLAN 600, exemplo da configuração de VRF do CONVIDADO

```
!--- Define the GUEST VRF. ip vrf GUEST rd 600:3 !---
Create the SVI for the GUEST VLAN. interface Vlan600 ip
vrf forwarding GUEST ip address 172.26.123.193
255.255.255.224 !--- Create the SVI for the
DIRTY_TRANSIT_NETWORK. interface Vlan306 ip vrf
forwarding GUEST ip address 172.26.120.62
255.255.255.252 !--- Set the allowed VLAN on the trunk.
interface FastEthernet1/0/48 switchport trunk allowed
vlan add 306 !--- Set up the routing for the VRF. router
eigrp 26 address-family ipv4 vrf GUEST network
172.26.0.0 autonomous-system 600 no auto-summary exit-
address-family
```

Passo 2: Configurar o switch central

Os exemplos de configuração nesta seção mostram a simulação de um centro falido com um Catalyst 3750-E Switch. Na maioria de ambientes, este não é um interruptor da borda-classe. Contudo, o interruptor foi construído no ambiente de laboratório usado para este documento.

Crie quatro mais VLAN para redes do trânsito, dois para o VLAN SUJO e dois para o CONVIDADO VLAN. Veja a figura 10.

- VLAN SUJOVLAN 301 SUJO da borda a retirar o núcleoVLAN 901 SUJO do núcleo ao centro de dados
- CONVIDADO VLANCONVIDADO VLAN 306 da borda a retirar o núcleoCONVIDADO VLAN 906 do núcleo ao centro de dados

Um transit network está sendo construído da borda ao núcleo, e de um segundo para o núcleo ao centro de dados. As redes do trânsito devem ser terminadas para que os SUJOS e o CONVIDADO VRF. Se o switching de caractere é permitido em vez de VRF-Lite, este não é necessário.

Nota: Este documento focaliza em VRF-Lite, e o switching de caractere é considerado para fora--espaço.

Figura 10 – *Redes do trânsito*
:

VLAN 301 SUJO da borda a retirar o núcleo; VLAN 901 SUJO do núcleo ao exemplo de configuração do centro de dados

```
!--- This is the core switch. !--- Define the DIRTY VRF.
ip vrf DIRTY rd 100:1 !--- Create the SVI for the DIRTY
VLANs. interface Vlan301 desc This is the Transit
```

```
Network between the Edge & Core ip vrf forwarding DIRTY
ip address 172.26.120.49 255.255.255.252 interface
Vlan901 desc This is the Transit Network between the
Core and the DC ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 !--- Set the allowed VLAN
on the trunks. interface GigabitEthernet1/0/3 switchport
trunk allowed vlan add 301 interface
GigabitEthernet1/0/48 switchport trunk allowed vlan add
901 !--- Set up the routing for the VRF. router eigrp 26
address-family ipv4 vrf DIRTY network 172.26.0.0
autonomous-system 100 no auto-summary exit-address-
family exit-address-family
```

CONVIDADO VLAN 306 da borda a retirar o núcleo; CONVIDADO VLAN 906 do núcleo ao exemplo de configuração do centro de dados

```
!--- This is the core switch. ! !--- Define the GUEST
VRF. ip vrf GUEST rd 600:1 !--- Create the SVI for the
GUEST VLANS. interface Vlan306 desc This is the transit
network between the Edge & Core ip vrf forwarding GUEST
ip address 172.26.120.61 255.255.255.252 interface
Vlan906 description Transit Network between Core & DC ip
vrf forwarding GUEST ip address 172.26.120.14
255.255.255.252 !--- Set the allowed VLAN on the trunks.
interface GigabitEthernet1/0/3 switchport trunk allowed
vlan add 306 interface GigabitEthernet1/0/48 switchport
trunk allowed vlan add 906 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf GUEST
network 172.26.0.0 autonomous-system 600 no auto-summary
exit-address-family
```

Passo 3: Configurar o interruptor de centro de dados

Enquanto o exemplo de configuração mostra, o server de Cisco NAC tem ambas as relações conectadas ao mesmo interruptor de centro de dados 6500. A relação confiada está em VLAN 60, e a interface não confiável está no VLAN 160, que está no VRF SUJO.

1. Crie quatro mais VLAN para a conexão ao núcleo:Um VLAN sujo (160)Um VLAN limpo (60)Um transit network sujo (901)Um transit network limpo (906)Adicionar o VLAN SUJO ao VRF SUJO.Termine o CONVIDADO VRF em um CONVIDADO DMZ (999) esse usos um Firewall de Cisco ASA (fora do espaço para este documento) a fim conectar usuários convidado ao Internet e executar funções do Network Address Translation (NAT).
2. Crie as subinterfaces SUJAS e do CONVIDADO do trânsito.Os comandos mostrados no exemplo da configuração de switch do centro de dados executam estas tarefas:Defina os SUJOS e o CONVIDADO VRF.Crie as redes SUJAS e LIMPAS para o server de Cisco NAC.

Exemplo da configuração de switch do centro de dados

```
!--- Define the DIRTY and GUEST VRFs. ip vrf DIRTY rd
100:26 ip vrf GUEST rd 600:26 !--- Create the sub-
interface and switched virtual interface (SVI) !--- for
the DIRTY and GUEST VLANs. interface
FastEthernet1/34.901 desc Transit Network from Core to
DC for DIRTY traffic encapsulation dot1Q 901 ip vrf
forwarding DIRTY ip address 172.26.120.1 255.255.255.252
interface FastEthernet1/34.906 desc Transit Network from
Core to DC for GUEST traffic encapsulation dot1Q 906 ip
```

```
vrf forwarding GUEST ip address 172.26.120.13
255.255.255.252 interface Vlan60 desc Trusted (CLEAN)
side of the NAC Server ip address 172.26.60.1
255.255.255.0 interface Vlan160 desc Untrusted (DIRTY)
side of the NAC Server ip vrf forwarding DIRTY ip
address 172.26.160.1 255.255.255.0 interface Vlan999
description GUEST VLAN SVI ip vrf forwarding GUEST ip
address 192.168.26.254 255.255.255.0 !--- Set up the
routing for the VRFs. router eigrp 26 network
172.26.60.0 0.0.0.255 no auto-summary redistribute
static address-family ipv4 vrf DIRTY autonomous-system
100 network 172.26.120.0 0.0.0.3 network 172.26.160.0
0.0.0.255 no auto-summary redistribute static exit-
address-family address-family ipv4 vrf GUEST network
172.26.0.0 network 192.168.26.0 autonomous-system 600 no
auto-summary redistribute static exit-address-family !--
- Set up the static routes for redistribution for the
VRFs. ip route 172.26.123.0 255.255.255.192 172.26.60.2
ip route vrf DIRTY 0.0.0.0 0.0.0.0 172.26.160.2 ip route
vrf GUEST 0.0.0.0 0.0.0.0 192.168.26.1
```

Passo 4: Execute a instalação inicial do Cisco NAC Manager and Server

A instalação do Cisco NAC Manager and Server é executada com o acesso de console. A instalação de serviço público guia-o com a configuração inicial para o gerente e o server. Vá a instalar o Access Manager limpo e o servidor de acesso limpo a fim executar a instalação inicial.

Passo 5: Aplique uma licença ao gerente de Cisco NAC

Depois que você executa a instalação inicial através do console, alcance o GUI de gerenciador de Cisco NAC a fim continuar a configurar o Cisco NAC Manager and Server. Transfira arquivos pela rede primeiramente o gerente e as licenças de servidor que vieram com os dispositivos. Para obter mais informações sobre de como transferir arquivos pela rede as licenças, vá ao *acesso a* seção do *console de web CAM de* instalar o Access Manager limpo e limpe o servidor de acesso.

Nota: Todas as licenças do Cisco NAC Manager and Server são baseadas no MAC address do eth0 do gerente. Em uma instalação do Failover, as licenças são baseadas no MAC address do eth0 de gerentes preliminares e secundários de Cisco NAC.

Passo 6: Políticas da atualização do cisco.com no gerente de Cisco NAC

O gerente de Cisco NAC deve ser configurado a fim recuperar atualizações periódicas do server central da atualização situado em Cisco. A lista apoiada ferramenta NAC do produto de Cisco AV/AS é um arquivo versioned XML distribuído de um server centralizado da atualização que forneça a matriz a mais atual de vendedores apoiados do antivirus e do antispyware e as versões do produto usadas para configurar regras do antivirus ou do antispyware e exigências da atualização da definição do antivirus ou do antispyware para a avaliação e a remediação da postura. Esta lista é atualizada regularmente para o antivirus e o Produtos e as versões do antispyware apoiados em cada agente de Cisco NAC liberam e incluem novos produtos para versões de agente novas. A lista fornece a informação de versão somente. Quando o gerente de Cisco NAC transfere a lista apoiada do produto do antivirus e do antispyware, está transferindo a informação sobre o que as versões as mais atrasadas são para o Produtos do antivirus e do antispyware. Não está transferindo arquivos de correção ou arquivos de definição de vírus reais. Baseado nesta informação, o agente pode então provocar o aplicativo nativo do antivirus ou do antispyware a fim executar atualizações. Para obter mais informações sobre de como as

atualizações são recuperadas, vá ao *início de uma sessão do agente da exigência para a* seção das *máquinas cliente de* configurar a ferramenta NAC de Cisco para o início de uma sessão do agente e a avaliação da postura do cliente.

Passo 7: Instale Certificados de um Certificate Authority (CA) da terceira

Durante a instalação, o script do utilitário de configuração para o gerente de Cisco NAC e o server de Cisco NAC exige-o gerar um certificado provisório SSL. Para o ambiente de laboratório, você pode continuar a usar os certificados auto-assinados. Contudo, não são recomendados para uma rede de produção.

Para obter mais informações sobre de instalar Certificados no gerente de Cisco NAC de CA da terceira, vá ao *tempo de sistema do grupo* e *limpe* seções *de acesso direto do console de web do servidor de acesso de* administrar o CAM.

Nota: Se você usa os Certificados do auto-sinal no ambiente de laboratório, no gerente de Cisco NAC e no server de Cisco NAC cada necessidade de confiar o certificado do outro. Isto exige que você transfere arquivos pela rede os Certificados para ambos como um Certificate Authority confiado sob **SSL > autoridades do certificado confiável**.

Passo 8: Instalação do server de Cisco NAC da revisão

A maioria de importante a recordar para um projeto bem sucedido NAC é que o tráfego classificado como o fluxo sujo da obrigação no lado não confiável do server NAC, como figura 11 mostra:

Figura 11 – ***Distribuição de servidor de Cisco NAC***

Etapa 9: Adicionar o server de Cisco NAC ao gerente de Cisco NAC

Termine estas etapas a fim adicionar o server de Cisco NAC ao gerente de Cisco NAC:

1. Clique **server CCA** sob a placa do Gerenciamento de dispositivos. Veja figura 12.
2. Clique a aba nova do server.
3. Use a caixa do endereço IP do servidor a fim adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação confiada do server de Cisco NAC.
4. Na caixa da localização do servidor, entre no **server OOB Cisco NAC** como a localização do servidor.
5. Escolha o Real-IP-**gateway fora da banda da** lista de drop-down do tipo de servidor.
6. O clique **adiciona o servidor de acesso limpo**.

Figura 12 – ***Adicionando o server de Cisco NAC ao gerente de Cisco NAC***

Nota: O gerente de Cisco NAC e o server de Cisco NAC têm que confiar CA de cada um para que o gerente adicione com sucesso o server.

Depois que você adiciona o server de Cisco NAC, aparece na lista sob a lista de aba dos server. Consulte a Figura 13.

Etapa 10: Configurar o server de Cisco NAC

Termine estas etapas a fim configurar o server de Cisco NAC:

1. Clique a lista de aba dos server.
2. Clique o ícone do controlo para o server de Cisco NAC a fim continuar a configuração.

Figura 13 – *Server de Cisco NAC controlado pelo gerente de Cisco NAC*

Depois que você clica o ícone do controlo, a tela mostrada em figura 14 aparece.

Etapa 11: Permita o apoio da camada 3

Termine estas etapas a fim permitir o apoio da camada 3:

1. Selecione a aba da rede.
2. Verifique a caixa de seleção do **apoio da possibilidade L3**.
3. Verifique o **modo restrito da possibilidade L3 para obstruir dispositivos NAT com a** caixa de seleção do **agente NAC**.
4. Clique em **Update**.
5. Recarregue o server de Cisco NAC como instruído.

Figura 14 – *Detalhes da rede de servidor de Cisco NAC*

Nota: Gerencia sempre o certificado para o server de Cisco NAC com o endereço IP de Um ou Mais Servidores Cisco ICM NT de sua interface não confiável. Para um certificado nome-baseado, o nome precisa de resolver ao endereço IP de Um ou Mais Servidores Cisco ICM NT da interface não confiável. Quando o ponto final se comunica com a interface não confiável do server a fim começar o processo NAC, o server reorienta o usuário ao hostname do certificado ou ao IP. Se o certificado aponta à relação confiada, o processo de login não funciona corretamente.

Etapa 12: Configurar rotas estáticas

Termine estas etapas a fim configurar rotas estáticas:

1. Depois que as repartições do server de Cisco NAC, retornam ao server e continuam com a configuração.O server de Cisco NAC deve usar a interface não confiável a fim comunicar-se com os pontos finais no VLAN não-autenticado.
2. **Avançado** seleto **> rotas estáticas** a fim adicionar rotas ao VLAN não-autenticado.
3. Preencha as sub-redes apropriadas para os VLAN não-autenticados.
4. O clique **adiciona a rota**.
5. Selecione a **interface não confiável [eth1]** para estas rotas.

Figura 15 – *Adicionar uma rota estática para alcançar a sub-rede de usuário Un-autenticada*

Passo 13: Perfis estabelecidos para o Switches no gerente de Cisco NAC

Termine estas etapas a fim estabelecer perfis para o Switches no gerente de Cisco NAC:

1. **O Gerenciamento** seleto **OOB > perfila > dispositivo > edita**.
2. Preencha a informação de perfil de dispositivo. Use figura 16 como guia.Cada interruptor é associado com um perfil. Adicionar um perfil para cada tipo de switch de ponta que o gerente de Cisco NAC controlará. Neste exemplo, um 3750 Switch é controlado.**Figura 16 –** *Perfil SNMP usado para controlar o interruptor*
3. Estabelecer a configuração de switch para o SNMP.Configurar o switch de ponta para os mesmos string de comunidade de leitura/gravação SNMP que são configurados no gerente

de Cisco NAC.`snmp-server community Cisco123 RO`
`snmp-server community Cisco1234 RW`

4. Selecione o **Gerenciamento** > os **perfis** > a **porta OOB** > **novo**. Veja figura 17.Para o controle da porta individual, configurar um perfil da porta sob o **Gerenciamento** > os **perfis** > a **porta OOB** que inclui o padrão o acesso não-autenticado VLAN VLAN e de padrão. Na seção do acesso VLAN, especifique o papel de usuário VLAN usando o acesso VLAN dropdown. O gerente de Cisco NAC muda o VLAN não-autenticado ao acesso VLAN baseado no VLAN definido no papel onde o usuário pertence.Defina o perfil da porta a fim controlar o VLAN da porta baseado nos papéis de usuário e nos VLAN executados.O AUTH VLAN é o VLAN NÃO-AUTENTICADO (VLAN 17) a que os dispositivos não-autenticados são atribuídos inicialmente.O acesso VLAN do padrão é os EMPREGADOS VLAN (VLAN14). Este VLAN é usado se o usuário autenticado não tem um VLAN papel-baseado definido.O acesso VLAN pode cancelar o VLAN padrão a um papel de usuário VLAN, que é definido sob o papel de usuário. Para obter mais informações sobre dos papéis de usuário da fundação, veja etapa 17: Configurar papéis de usuário. Os mapeamentos LDAP podem ser usados a fim traçar papéis de usuário no NAC aos grupos LDAP. Para mais informação, refira NAC(CCA) 4.x: Trace usuários a determinados papéis usando o exemplo da configuração ldap.**Figura 17 – *Perfil da porta para controlar a porta de switch*** **Nota:** Você pode igualmente definir nomes VLAN em vez dos ID. Se você define nomes VLAN, você pode ter VLAN ID no Switches diferente através do terreno. Contudo, o mesmo nome VLAN é anexado a um papel particular.As opções adicionais estão disponíveis sob o perfil da porta para a liberação IP e renovam opções. Enrole para baixo a página mostrada dentro a fim ver estas opções.Se o usuário é atrás de um telefone IP, desmarcar o **salto a porta depois que o VLAN é** caixa de seleção **mudada**. Se isto é verificado, pode possivelmente recarregar o telefone IP quando a porta é saltada.**Figura 18 – *Perfil inferior disponível da porta das várias opções***

Passo 14: Configurar ajustes do receptor SNMP

Além do que estabelecer a série de comunidade snmp para o Read/Write, você igualmente precisa de configurar o gerente de Cisco NAC a fim receber o SNMP traps do interruptor. Estas armadilhas são enviadas quando o usuário conecta e disconexões da porta. Quando o server de Cisco NAC envia a informação do endereço IP de Um ou Mais Servidores Cisco ICM NT MAC/de um ponto final particular ao gerente, o gerente pode construir internamente uma tabela de mapeamento para o MAC/IP e a porta de switch.

1. Selecione o **Gerenciamento OOB** > os **perfis** > o **receptor SNMP**.
2. Configurar os ajustes da armadilha de SNMP como esta figura mostra:**Figura 19 – *O ajuste do receptor do gerente SNMP de Cisco NAC para recolher o SNMP traps e informa***
3. A fim configurar as configurações de switch para o SNMP traps, aumente o temporizador limpo do resplendor do Access Manager do switch padrão (CAM) a 1 hora por recomendações da melhor prática de Cisco para NAC OOB. A amostra CLI mostra o conjunto de parâmetro do `tempo de envelhecimento do mac-address-table a` 3600.Ajustar o temporizador a 1 hora reduz a frequência das notificações MAC enviadas fora já dos dispositivos conectados ao gerente de Cisco NAC. Use o **comando trap da fonte** a fim especificar o endereço de origem que é usado para mandar as armadilhas.Opcionalmente, configurar a associação e as armadilhas de linkdown a fim enviar a Cisco NAC o gerente (não mostrado na amostra CLI). Estas armadilhas são usadas somente em um cenário de distribuição onde os host finais não sejam conectados atrás de um telefone IP.**Nota:** O

SNMP informa é recomendado porque são mais seguros do que o SNMP traps. Também, considere o Qualidade de Serviço (QoS) para o SNMP em um ambiente de rede do tráfego elevado.

Etapa 15: Adicionar o Switches como dispositivos no gerente de Cisco NAC

Termine estas etapas a fim adicionar o Switches como dispositivos no gerente de Cisco NAC:

1. Selecione o **Gerenciamento** > os **dispositivos** > os **dispositivos OOB** > **novo**.Use o perfil do interruptor criado em etapa 13 a fim adicionar o interruptor.
2. Sob o perfil de dispositivo, use o perfil que você criou. Não mude o valor do perfil da porta padrão quando você adiciona o interruptor.**Figura 20 –** ***Adicionar o switch de ponta no gerente de Cisco NAC para controlar através do SNMP***
3. Depois que o interruptor é adicionado ao gerente de Cisco NAC, você pode selecionar as portas que você quer controlar.

Passo 16: Configurar portas de switch para que os dispositivos sejam controlados pelo NAC

Termine estas etapas a fim configurar as portas de switch para que os dispositivos sejam controlados pelo NAC.

1. **O Gerenciamento** seleto **OOB** > o **[IP address] do interruptor de dispositivos** > **movem** > **lista** a fim considerar as portas de switch que disponíveis você pode controlar.**Figura 21 –** ***Seleção do controle da porta disponível para um interruptor controlado*** **Nota:** Não deixe o perfil padrão como “descontrolado” até que você possa marcar as relações apropriadas estaticamente como “descontrolado”. Após as portas de uplink, e qualquer outro -fora nas portas que precisam de permanecer descontroladas são ajustados; mude então o padrão a seu perfil controlado da porta. A falha fazer assim nesta ordem pode conduzir aos resultados menos do que desejáveis.
2. **O Gerenciamento** seleto **OOB** > o **[IP address]** > as **portas do interruptor de dispositivos** > **controlam** a fim controlar imediatamente diversas portas.

Figura 22 – ***Controle portas múltiplas com a opção da junta***

Etapa 17: Configurar papéis de usuário

Neste exemplo, os VLAN que correspondem a cada papel são criados já no switch de ponta.

1. **O gerenciamento de usuário** > os **papéis de usuário** seletos > **editam o papel** e criam um papel do empregado enquanto esta figura mostra:**Figura 23 –** ***Crie um papel do empregado e trace o VLAN DE DADOS***
2. **O gerenciamento de usuário** > os **papéis de usuário** seletos > **editam o papel** e criam um papel de convidado enquanto esta figura mostra:**Figura 24 –** ***Crie um papel de convidado e trace o CONVIDADO VLAN***

Etapa 18: Adicionar usuários e atribua-os para apropriar o papel de usuário

Em um ambiente de campus, você integrará com um servidor de autenticação externa e traçará o

usuário a um papel particular por meio do atributo LDAP. Este exemplo usa um usuário local e associados esse usuário local com um papel.

Etapa 19: Personalize a página do login de usuário para o início de uma sessão da Web

Uma página de login do padrão é criada já no gerente de Cisco NAC. Você pode opcionalmente personalizar a página de login a fim mudar a aparência do portal da web. Para uma solução da camada 3 OOB NAC, você deve transferir o componente de ActiveX ou de Javas ao cliente da extremidade a fim executar estas tarefas:

- Busque o MAC address da máquina cliente.
- Execute a liberação do endereço IP de Um ou Mais Servidores Cisco ICM NT e renove-a.

1. Selecione a **administração > páginas de usuário**.
2. Edite a página a fim permitir as opções como esta figura mostra:

Figura 25 – ***Composição do usuário para o início de uma sessão da Web***

Etapa 20: Personalize o agente de Cisco NAC para os papéis de usuário

Termine estas etapas a fim personalizar o agente de Cisco NAC para papéis de usuário:

1. Selecione o **Gerenciamento de dispositivos > acesso limpo > instalação > início de uma sessão gerais do agente**.Você pode configurar o gerente de Cisco NAC a fim fazer o agente imperativo para todo o papel de usuário. Neste exemplo, o agente é imperativo para o papel do empregado. O contratante e os papéis de convidado devem usar o início de uma sessão da Web.
2. Verifique o **uso da exigência da** caixa de seleção do **agente**.

Figura 26 – ***Início de uma sessão do agente exigido para o papel do empregado***

Etapa 21: Distribua o host da descoberta para o agente de Cisco NAC

A distribuição de agente de software de Cisco NAC, a instalação, e a configuração são cobertas dentro configuram a ferramenta NAC de Cisco para o início de uma sessão do agente e a avaliação da postura do cliente. Este exemplo configura o host da descoberta no gerente de Cisco NAC.

Selecione o **Gerenciamento de dispositivos > acesso limpo > agente >** a **instalação limpos do acesso**:

Figura 27 – ***Descubra o host para um agente de Cisco NAC***

O campo do host da descoberta PRE-é povoado se o agente de Cisco NAC é transferido do server de Cisco NAC. Consulte a figura 27.

Nota: Em uma camada 3 OOB com modelo VRF, o host da descoberta é ajustado tipicamente para ser o nome de DNS ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do gerente de Cisco NAC, que existe na rede limpa. Porque todo o tráfego das redes “sujas” é distribuído à revelia através do server de Cisco NAC, os pacotes de descoberta correm através automaticamente do server. O fluxo de tráfego descrito aqui é um dos benefícios ao método VRF. Prevê uma experiência consistente, predizível. Veja fluxos de processo de Cisco NAC para mais

informação.

Etapa 22: Início de uma sessão da Web

Termine estas etapas a fim entrar com a Web:

1. Conecte a máquina cliente que usa uma das portas de ponta controladas pelo gerente de Cisco NAC.A máquina cliente é colocada no VLAN não-autenticado. Certifique-se de que a máquina recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT da sub-rede não-autenticado VLAN.
2. Abra o navegador a fim executar o início de uma sessão.A suposição é que esta máquina cliente não tem um agente de Cisco NAC instalado já. Se todas as entradas de DNS são reorientadas à interface não confiável do server de Cisco NAC, o navegador reorienta automaticamente a uma página de login. Se não faz, para ir a uma URL específica tal como guest.nac.local a fim executar o início de uma sessão:

Figura 28 – *Página de login da Web*

Etapa 23: Início de uma sessão do agente

Você pode distribuir o agente de Cisco NAC apenas como todo o aplicativo de outro software aos utilizadores finais ou você pode forçá-lo que usa o server de Cisco NAC.

Nota: Mais informação detalhada na distribuição de agente e na instalação está disponível na ferramenta NAC de Cisco - manual de configuração limpo do Access Manager.

Esta figura mostra a tela que aparece quando o agente é ativado:

Figura 29 – *Início de uma sessão do agente*

1. Selecione o server da lista suspensa do server.
2. Incorpore o username.
3. Incorpore a senha.
4. Clique em login.Figuras 30 e 31 mostram as telas que aparecem:.Figura 30 – *O agente de Cisco NAC que executa a liberação IP ou renova* Figura 31 – *O agente de Cisco NAC que indica o acesso de rede completo após o IP refresca*
5. Clique em **OK**.

Apêndice

Alta Disponibilidade

Cada um dos gerentes de Cisco NAC e dos server individuais de Cisco NAC na solução pode ser configurado na Alta disponibilidade do modo, significando que há dois dispositivos que atuam em uma configuração ativo-à espera.

Gerente NAC

Você pode configurar o gerente de Cisco NAC na Alta disponibilidade do modo onde há dois gerentes NAC que atuam em uma configuração ativo-à espera. A configuração completa em um

gerente é armazenada em um base de dados. O gerente do apoio sincroniza seu base de dados com o base de dados no gerente ativo. Todas as alterações de configuração feitas ao gerente ativo são empurradas imediatamente para o gerente à espera. Estes pontos chaves fornecem um sumário de nível elevado da Alta disponibilidade da operação do gerente:

- A Alta disponibilidade do modo do gerente de Cisco NAC é uma configuração de dois-server ativa ou passiva em que um gerente à espera atua como um backup a um gerente ativo.
- O gerente ativo de Cisco NAC executa todas as tarefas para o sistema. O gerente do apoio monitora o gerente ativo e mantém seu base de dados sincronizado com o base de dados do gerente ativo.
- Ambos os gerentes de Cisco NAC compartilham de um IP virtual do serviço para a relação confiada eth0. Use este IP do serviço para o certificado SSL.
- Os gerentes preliminares e secundários de Cisco NAC trocam pacotes de heartbeat UDP cada 2 segundos. Se o temporizador ritmado expira, a comutação classificada ocorre.
- A fim assegurar um gerente ativo de Cisco NAC está sempre disponível, sua relação confiada (eth0) deve estar acima. Você deve evitar a situação onde um gerente é ativo mas não é direto acessível sua relação confiada. Esta circunstância ocorre se o gerente à espera recebe pacotes de heartbeat do gerente ativo, mas a relação do eth0 do gerente ativo falha. O mecanismo da link-detecção permite que o gerente à espera saiba quando a relação do eth0 do gerente ativo se torna não disponível.
- Você pode escolher “configura automaticamente” a relação Eth1 na página da **administração** > do **gerente** > do **Failover CCA**. Contudo, você deve manualmente configurar a outra (Eth2 ou Eth3) Alta disponibilidade das relações com um endereço IP de Um ou Mais Servidores Cisco ICM NT e um netmask antes que você configure a Alta disponibilidade no gerente de Cisco NAC.
- O eth0, as relações Eth1, e Eth2/Eth3 podem ser usados para pacotes de heartbeat e sincronização de base de dados. Além, toda a relação (COM) de série disponível pode igualmente ser usada para pacotes de heartbeat. Se você se está usando mais de uma destas relações, o Failover ocorre somente se todas as relações da pulsação do coração falham.

Nota: A Alta disponibilidade dos pares do gerente de Cisco NAC não pode ser separada por um link da camada 3.

Para mais detalhes, refira a documentação do gerente de Cisco NAC em configurar a Alta disponibilidade.

Server de Cisco NAC

A fim fornecer a proteção contra um ponto de falha único, você pode configurar o server de Cisco NAC na Alta disponibilidade do modo. A Alta disponibilidade do modo para o server de Cisco NAC é similar àquela do gerente de Cisco NAC e igualmente usa uma configuração ativo-à espera. Os server de Cisco NAC ainda compartilham de um endereço IP de Um ou Mais Servidores Cisco ICM NT virtual (chamado um IP do serviço), mas não compartilham de endereços MAC virtuais.

Estes pontos chaves fornecem uma visão geral de alto nível da Alta disponibilidade da operação de servidor de Cisco NAC:

- A Alta disponibilidade do modo do server de Cisco NAC é uma configuração de dois-server ativo-passiva em que uma máquina do servidor à espera de Cisco NAC atua como um

backup a um server ativo de Cisco NAC.

- O server ativo de Cisco NAC executa todas as tarefas para o sistema. Porque a maioria da configuração do servidor está armazenada no gerente de Cisco NAC, quando o Failover do server ocorre, o gerente empurra a configuração para o server novo-ativo.
- O server à espera de Cisco NAC não envia nenhuns pacotes entre suas relações.
- O server à espera de Cisco NAC monitora a saúde do servidor ativo através de uma relação da pulsação do coração (série e umas ou várias relações UDP). Os pacotes de heartbeat podem ser enviados na interface serial, na relação Eth2 dedicada, na relação Eth3 dedicada, ou na relação Eth0/Eth1 (se nenhuma relação Eth2 ou Eth3 está disponível).
- Os server preliminares e secundários de Cisco NAC trocam pacotes de heartbeat UDP cada dois segundos. Se o temporizador ritmado expira, a comutação classificada ocorre.
- Além do que o Failover pulsação do coração-baseado, o server de Cisco NAC igualmente fornece o Failover link-baseado baseado no eth0 ou na falha do link Eth1. O server envia pacotes do ping ICMP a um endereço IP externo através do eth0 e/ou da relação Eth1. O Failover ocorre somente se um server de Cisco NAC pode sibilar os endereços externos.

Para mais detalhes, refira a documentação de servidor de Cisco NAC em configurar a Alta disponibilidade.

Diretório ativo SingleSignOn (diretório ativo SSO)

O diretório ativo SSO de Windows é a capacidade para uma ferramenta NAC de Cisco automaticamente aos usuários de login já autenticada a um controlador de domínio backend do Kerberos (servidor ative directory). Esta capacidade elimina a necessidade de registrar em Cisco NAC o server depois que você é registrado já no domínio. Para mais detalhes sobre configurar o diretório ativo SSO em uma ferramenta NAC de Cisco, vá a configurar o diretório ativo único Sinal-em.

Considerações do ambiente do domínio do Windows

Àvista de um desenvolvimento NAC, as mudanças à política do script do início de uma sessão podem ser exigidas. Os scripts do início de uma sessão de Windows podem ser classificados como scripts da partida ou da parada programada e do fazer logon ou do fazer logoff. Windows executa a partida e a parada programada passa pelo processo de script da “em um contexto máquina.” Executar os scripts funciona somente se a ferramenta NAC de Cisco abre os recursos de rede apropriados exigidos pelo script para o papel particular quando estes scripts estão executados na bota PC acima ou na parada programada, que são tipicamente o papel não autenticado. Os scripts do fazer logon e do fazer logoff são executados do “em um contexto usuário,” que significa que o script de logon executa depois que o usuário entrou a calha Windows GINA. O script de logon pode não executa se a autenticação ou a avaliação da postura da máquina cliente não terminam e o acesso de rede não está concedido a tempo. Estes scripts podem igualmente ser interrompidos pelo endereço IP de Um ou Mais Servidores Cisco ICM NT refrescam iniciado pelo agente de Cisco NAC depois que um evento do fazer logon OOB. Para obter mais informações sobre das alterações necessárias aos scripts do início de uma sessão, vá aos scripts de Windows GPO e à Interoperabilidade de Cisco NAC.

Configurar a ferramenta NAC de Cisco para o início de uma sessão do agente e a avaliação da postura do cliente

O agente de Cisco NAC e o agente da Web de Cisco NAC fornecem a avaliação e a remediação

locais da postura para máquinas cliente. Os usuários transferem e instalam o agente de Cisco NAC ou o agente da Web de Cisco NAC (software do cliente de leitura apenas), que podem verificar o registro, os processos, os aplicativos, e os serviços do host. Para mais detalhes sobre o agente e a avaliação e a remediação da postura, vá a configurar a ferramenta NAC de Cisco para o início de uma sessão do agente e a avaliação da postura do cliente.

Informações Relacionadas

- Página de suporte da ferramenta NAC de Cisco
- Suporte Técnico e Documentação - Cisco Systems