Camada 3 NAC do Guia de Design da faixa que usa VRF-Lite para o isolamento de tráfego

Índice

Introdução

Nota: A informação neste documento pode mudar sem aviso prévio. Confirme todas as recomendações se possível.

A finalidade deste documento é descrever uma aplicação baseada VRF-Lite do NAC em uma camada 3 do desenvolvimento da faixa (OOB) onde o server NAC (CAS) é configurado no modo (roteado) real do IP gateway. A camada 3 da faixa tem rapidamente tornado das metodologias as mais populares do desenvolvimento para o NAC. Esta SHIFT na popularidade é baseada em diversa dinâmica. O primeiro é melhor utilização dos recursos do hardware. Pelo desenvolvimento do NAC em uma metodologia da camada 3 OOB, uma única ferramenta NAC pode ser feita para escalar para acomodar mais usuários. Igualmente permite que as ferramentas NAC sejam ficadas situadas centralmente um pouco do que distribuída através do terreno ou da organização. Assim, as disposições da camada 3 OOB são muito mais eficazes na redução de custos ambos de um ponto de vista do capital e das despesas operacionais. Há duas aproximações amplamente utilizadas para distribuir o NAC em uma arquitetura da camada 3 OOB.

1. Aproximação baseada Descoberta-host — Usa a capacidade inerente dentro do agente NAC a fim alcançar o server NAC (CAS). ACL aplicados na aplicação do tráfego de controle do switch de acesso na rede suja. Refira a conexão ao server NAC (CAS) que usa o protocolo suíço para mais informação.

2. O VRF baseou a aproximação — Usos VRF distribuir o tráfego não-autenticado a CAS. As políticas de tráfego configuradas no server NAC (CAS) são usadas para a aplicação na rede suja. Esta aproximação tem duas secundário-aproximações. Na primeira aproximação, os VRF são patentes durante todo a infraestrutura, neste caso todos mergulham 3 dispositivos participam no switching de caractere. A segunda aproximação usa VRF-Lite e túneis GRE para escavar um túnel os VRF através dos dispositivos da camada 3 que não compreendem o switching de caractere. O benefício à segunda aproximação é que as mudanças de configuração mínima estão exigidas a sua infraestrutura de centro.

Nota: Quando a camada 3 OOB for uma da maioria de metodologias da distribuição comum, não pode sempre ser a solução ótima para cada ambiente. Há umas outras opções escolher daquela pode estar mais situação ótima cabida para seus requisitos particulares. Refira planejar seu desenvolvimento para obter mais informações sobre destas outras opções do projeto NAC.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Uma compreensão básica operação e configuração da infraestrutura da camada 2 e da camada 3
- Uma compreensão básica da ferramenta NAC de Cisco, e as diferenças entre as várias metodologias da aplicação que são associadas com ela
- Todas as disposições e os projetos NAC devem ser baseados em exigências do negócio claras. Estas são as suposições da exigência do negócio para esta definição de teste:Os usuários devem ser autenticados antes de ser concedida o acesso à rede at large.Seu acesso é limitado baseado em quem os usuários são. Estes privilégios são traçados à membrasia do clube no diretório ativo. Os grupos são convidados, contratantes, e empregados.Baseado na membrasia do clube AD, os usuários são colocados em um VLAN que tenha os privilégios de acesso de rede que são apropriados para cada grupo.O tráfego do usuário convidado continua a ser isolado do resto da rede mesmo depois a autenticação.Depois que o usuário é admitido à rede, a ferramenta NAC deve já não estar no caminho de tráfego. Isto impede a ferramenta NAC se transforme um gargalo e permite que a rede seja usada a seu potencial completo por usuários validados.
- O NAC tem muitas capacidades que não são cobertas por este documento. A finalidade deste guia é explorar e documentar as diretrizes do projeto e a configuração exigidas para uma camada baseada 3 de VRF-Lite do desenvolvimento da faixa NAC. Este guia não se centra sobre a avaliação ou a remediação da postura. Mais informação sobre a ferramenta NAC e suas capacidades completas podem ser encontradas em www.cisco.com/go/nac (clientes registrados somente).

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Configuração da infraestrutura

Introdução:

Quando considerando um VRF-Lite baseado o desenvolvimento da camada 3 OOB NAC, lá for diversos princípios do design que são muito importantes de considerar. Estes princípios são alistados aqui, e uma breve discussão de sua importância é incluída.

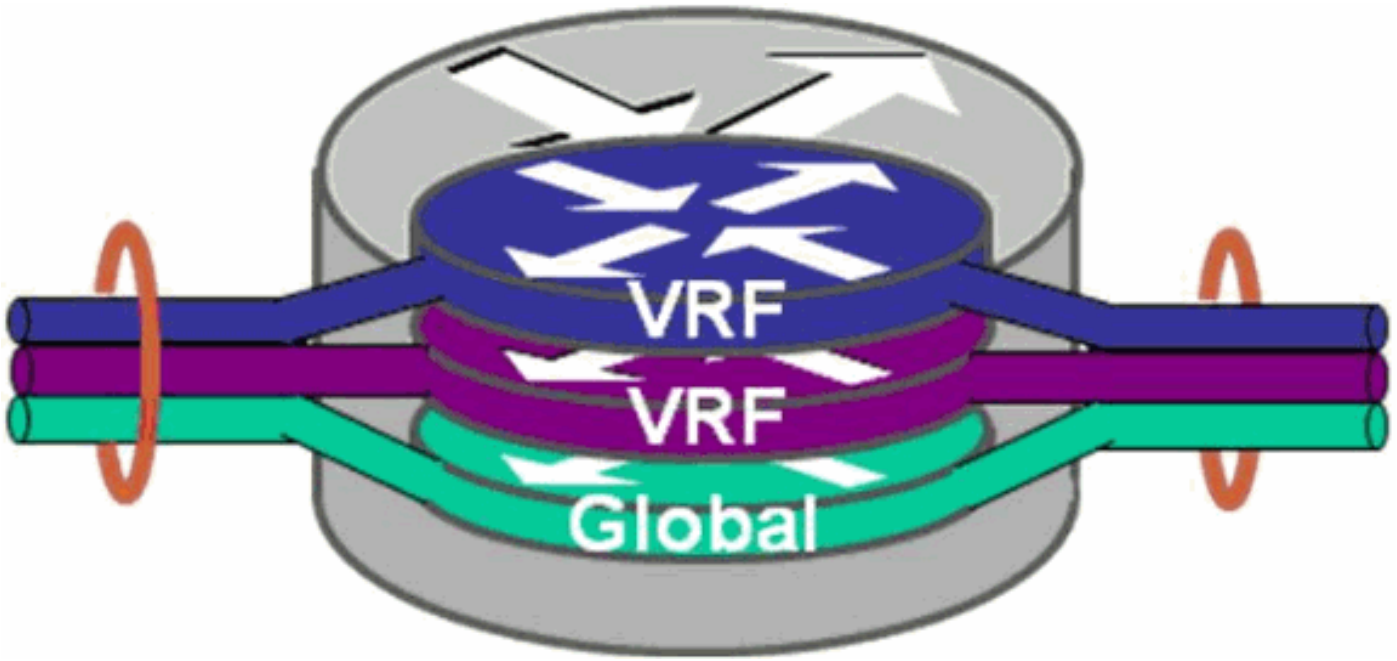
1. **Classificação de tráfego e engenharia** — Um conceito chave a realizar e recordar para este tipo de projeto NAC é que tráfego classificado como o fluxo sujo da *obrigação no* lado não confiável do server NAC (CAS). Mantenha sempre esta parte superior do princípio da mente durante o projeto de uma aplicação NAC. Adicionalmente, as redes limpas e sujas não devem ser permitidas comunicar-se diretamente um com o otro. Em um projeto da camada 3 OOB com VRF, o server NAC (CAS) atua como o ponto ou o controlador da aplicação que assegura a segregação e a comunicação segura entre as redes limpas e sujas.
2. **Isolamento de tráfego** — É importante para ter certeza que um mecanismo de aplicação apropriado está selecionado para fornecer o tráfego e o isolamento do trajeto para tudo tráfego originado dos anfitriões NON-autenticados e NON-autorizados. VRF-Lite é usado aqui para conseguir o isolamento completo dos dados e do controle plano (VRF).
3. **Aplicação centralizada** — Porque a metodologia de VRF-Lite segue a seleção de trajeto natural criada distribuindo: as alterações de topologia, as exigências do controle de acesso, e/ou as alterações de endereço não criam a necessidade de manipular ACL através da infraestrutura. Se você usa um túnel GRE conjuntamente com VRF-Lite, este dá-lhe a flexibilidade deixar cair o direito sujo do tráfego na frente do server NAC sem a necessidade de configurar saltos múltiplos. VRF-Lite conjuntamente com o GRE exige somente a configuração em dispositivos da camada 3 da borda. Isto reduz dramaticamente o número de dispositivos que devem ser tocados a fim fornecer a exigência do isolamento do trajeto.
4. **Dificuldade** — Dificuldade da aplicação assim como da manutenção contínua. Quando você determina a aproximação que você é provável se usar para a camada 3 OOB NAC em sua rede, é importante considerar a facilidade da aplicação e custos operacionais e complexidade em curso de executar essa tecnologia, particularmente em um ambiente dinâmico.

Nota: A ferramenta NAC 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 GRE, nem foi reorientado com a configuração de roteamento baseada política, VRF distribuído e assim por diante.

Nota: Para a melhor experiência de usuário final possível, recorde usar os Certificados que são confiados pelo navegador do utilizador final. O uso de Certificados Auto-gerados no server NAC não é recomendado para um ambiente de produção.

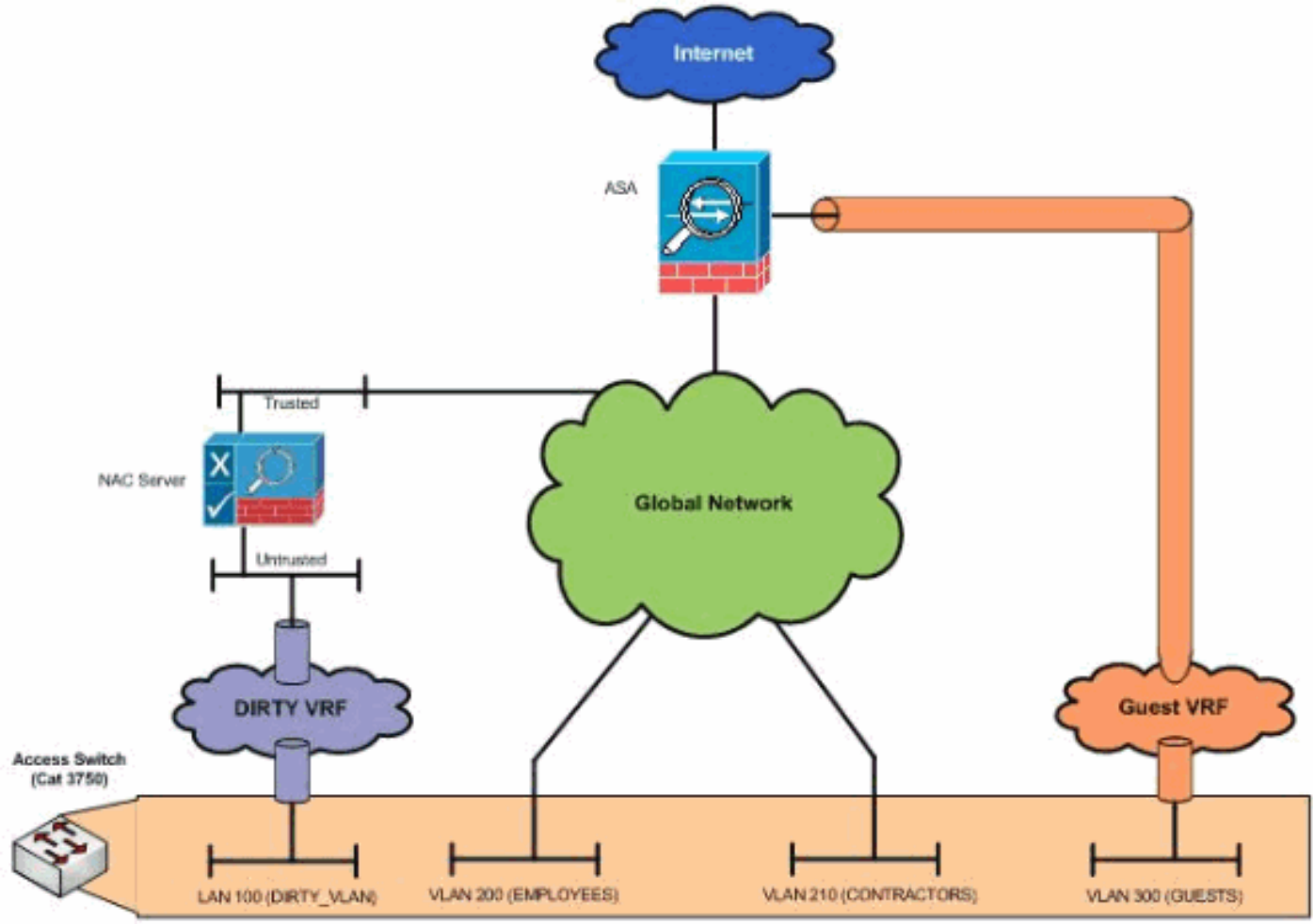
Nota: Gerencia sempre o certificado para o server NAC com o endereço IP de Um ou Mais Servidores Cisco ICM NT de sua interface não confiável.

Uma ilustração da virtualização do dispositivo com VRF pode ser considerada aqui. Esta metodologia fornece o plano do controle e os dados aplanam para o isolamento do trajeto.



Topologia

Este diagrama é representante da topologia usada para a criação deste papel. A rede interna está distribuindo através da tabela de roteamento global e não tem nenhum VRF associado com ela. O VRF SUJO contém somente o Dirty_VLAN e as redes associadas do trânsito que são exigidos para forçar todos os dados de origem do DIRTY_VLAN para correr através do lado sujo das ferramentas NAC. O convidado VRF contém o GUEST_VLAN e as redes associadas do trânsito exigidos para terminar todos os dados de origem do GUEST_VLAN em uma Secundário-relação separada no Firewall. Cada um das três redes virtuais é levada na mesma infraestrutura física e fornece o isolamento completo do tráfego e do trajeto respectivamente.



Fluxos de processo

Esta seção mostra o fluxo de processo básico do o que é exigido para ganhar o acesso de rede ambos com, e sem um agente instalado. Estes fluxos de processo são macroanalíticos na natureza e contêm somente etapas funcionais da decisão. 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.