Exemplo fora da banda da configuração sem fio NAC (OOB)

Índice

Introdução

Este documento fornece orientações de design para implementar a segurança de ponto de extremidade de um dispositivo Cisco Network Admission Control (NAC) fora de banda (OOB) em uma implementação de uma Cisco Unified Wireless Network. Estas recomendações da melhor prática supõem que uma rede de Cisco Unified Wireless esteve distribuída de acordo com as diretrizes fornecidas no 3.0 do Guia de Design da mobilidade da empresa.

O projeto recomendado é o gateway virtual (modo de Bridge) e solução central do desenvolvimento OOB com o RAIO único Sinal-em. O controlador do Wireless LAN (WLC) deve ser L2 colocado junto ao server NAC. O cliente associa ao WLC, e o WLC autentica o usuário. Uma vez que a autenticação é terminada, o tráfego de usuário atravessa a quarentena VLAN do WLC ao server NAC. O processo da avaliação e da remediação da postura ocorre. Uma vez que

o usuário é certificado, o VLAN de usuário muda da quarentena para alcançar o VLAN no WLC. O tráfego contorneia o server NAC quando movido para alcançar o VLAN.

Pré-requisitos

Requisitos

Esta configuração do documento é específica à liberação NAC 4.5 e WLC 5.1

Componentes Utilizados

Este documento é t restringido à versão de software e hardware específica.

- Server 3350 4.5 NAC
- Gerente 3350 NAC 4.5
- WLC 2106 5.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

Vista geral de Cisco NAC

Cisco NAC usa a infraestrutura de rede para reforçar a conformidade da política de segurança em todos os dispositivos que procuram aos recursos de computação da rede de acesso. Com a ferramenta NAC de Cisco, os administradores de rede podem autenticar, autorizam, avaliam, e remediate prendido, Sem fio, e usuários remotos e suas máquinas antes do acesso de rede. A ferramenta NAC de Cisco identifica se os dispositivos em rede tais como portáteis, Telefones IP, ou consoles do jogo são complacentes com políticas de segurança de rede, e repara todas as vulnerabilidades antes que permita o acesso à rede.

A terminologia do projeto recomendado é discutida:

Modo de gateway virtual (modo de Bridge)

Quando a ferramenta NAC é configurada como um gateway virtual, atua como uma ponte entre os utilizadores finais e o gateway padrão (roteador) para a sub-rede de cliente que é controlado. Para um cliente dado VLAN, a ferramenta NAC constrói uma ponte sobre o tráfego de sua interface não confiável a sua relação confiada. Quando atua como uma ponte do lado não confiável ao lado confiado do dispositivo, dois VLAN estão usados. Por exemplo, o cliente VLAN 110 é definido entre o controlador do Wireless LAN (WLC) e a interface não confiável da

ferramenta NAC. Não há nenhuma interface roteada ou Switched Virtual Interface (SVI) associada com o VLAN 110 no switch de distribuição. O VLAN10 é configurado entre a relação confiada da ferramenta NAC e o roteador de próximo salto interface/SVI para a sub-rede de cliente. Uma regra do mapeamento é feita na ferramenta NAC que para a frente os pacotes que chegam em VLAN 110 para fora VLAN10 quando troca a informação da etiqueta VLAN segundo as indicações do figo 1-1. O processo é invertido para os pacotes que retornam ao cliente. Note que, neste modo, os BPDU não estão passados do não-confiável-lado VLAN a suas contrapartes do confiar-lado. A opção do mapeamento VLAN é escolhida geralmente quando a ferramenta NAC é posicionada logicamente inline entre os clientes e as redes que estão protegidos. Esta opção de construção de uma ponte sobre deve ser usada se a ferramenta NAC deve ser distribuída no modo de gateway virtual com um desenvolvimento wireless unificado. Porque o server NAC está ciente dos *protocolos de camada superior*, à revelia permite explicitamente os protocolos que o exigem conectar à rede no papel autenticado, por exemplo, no DNS e no DHCP.

Figura gateway virtual de 1-1 com mapeamento VLAN

Modo fora da banda

As disposições fora da banda exigem o tráfego de usuário atravessar através da ferramenta NAC somente dentro da autenticação, da avaliação da postura, e da remediação. Quando um usuário é autenticado e passa todas as verificações da política, o tráfego está comutado normalmente através da rede e contorneia o server NAC. Para mais informações, refira o capítulo 4 da instalação e do Guia de Administração Dispositivo-limpos do Access Manager de Cisco NAC.

Quando a ferramenta NAC é configurada desse modo, o WLC é um dispositivo gerenciado no gerente NAC, a mesma maneira que um switch Cisco está controlado pelo gerente NAC. Depois que o usuário é autenticado e passa a avaliação da postura, o gerente NAC instrui o WLC para etiquetar o tráfego de usuário do NAC VLAN para alcançar o VLAN que oferece privilégios de acesso.

Figura ferramenta NAC de 1-2 no modo fora da banda com modo de gateway virtual

Escolha Sinal-em

Escolha sinal-em (SSO) é uma opção que não exija a intervenção de usuário e é relativamente direto executar. Utiliza a capacidade VPN SSO da solução NAC, acoplada com o agente de software limpo do acesso que é executado no PC cliente. O VPN SSO usa registros de contabilidade do RAIO para notificar a ferramenta NAC sobre os usuários de acesso remotos autenticados que conectam à rede. Da mesma forma, esta característica pode ser usada conjuntamente com o controlador de WLAN para informar automaticamente o server NAC sobre os clientes Wireless autenticados que conectam à rede.

Veja figuras 1-3 a 1-6 para exemplos de um cliente Wireless que execute a autenticação SSO, a avaliação da postura, a remediação, e o acesso de rede através da ferramenta NAC.

Esta sequência é mostrada em figura 1-3:

1. O usuário Wireless executa a autenticação 802.1x/EAP através do controlador de WLAN a um servidor AAA ascendente.
2. O cliente obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT do AAA ou de um servidor DHCP.

3. Depois que o cliente recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT, o WLC para a frente um registro da contabilidade do RAIO (começo) à ferramenta NAC, que inclui o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente Wireless.**Nota:** O controlador WLC usa um único registro de contabilidade do RAIO (começo) para a authenticação do cliente do 802.1x e a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT, quando o Switches do Cisco catalyst enviar dois registros de contabilidade: um começo da contabilidade é enviado após a authenticação do cliente do 802.1x, e uma atualização provisória é enviada depois que o cliente é atribuído um endereço IP de Um ou Mais Servidores Cisco ICM NT.
4. Depois que detecta a conectividade de rede, o agente NAC tenta conectar ao CAM (com o protocolo suíço). O tráfego é interceptado pelo server NAC, que, por sua vez, pergunta o gerente NAC para determinar se o usuário está na lista de usuário on-line. Somente os clientes que são autenticados estão na lista de usuário on-line, que é o caso no exemplo acima em consequência da atualização do RAIO em etapa 3.
5. O agente NAC executa uma avaliação local da postura da Segurança/risco da máquina cliente e para a frente a avaliação ao server NAC para a determinação da admissão da rede.**Figura processo de authenticação do cliente de 1-3 e avaliação da postura**

Esta sequência ocorre em figura 1-4:

1. A ferramenta NAC para a frente a avaliação do agente ao gerente da ferramenta NAC (CAM).
2. Neste exemplo, o CAM determina que o cliente não está na conformidade e instrui a ferramenta NAC para pôr o usuário em um papel da quarentena.
3. A ferramenta NAC envia então a informação da remediação ao agente do cliente.**Figura informação da avaliação da postura de 1-4 de CAS ao CAM**

Esta sequência ocorre em figura 1-5:

1. O agente do cliente indica o tempo que permanece realizar a remediação.
2. O agente guia o usuário ponto por ponto com o processo da remediação; por exemplo, na atualização do arquivo de definição anti-vírus.
3. Após a conclusão da remediação, o agente atualiza o server NAC.
4. O CAM indica uma indicação da política de uso aceitável (AUP) ao usuário.**Figura processo da remediação do cliente de 1-5 com CAS como o dispositivo da aplicação**

Esta sequência ocorre em figura 1-6:

1. Depois que aceita o AUP, a ferramenta NAC comuta o usuário a um papel (autorizado) em linha.
2. A funcionalidade SSO povoa a lista de usuário on-line com o endereço IP cliente. Após a remediação, uma entrada para o host é adicionada à lista certificada. Both of these tabelas (junto com a tabela descoberta dos clientes) são mantidas pelo CAM (gerente da ferramenta NAC).
3. O gerente NAC envia um SNMP escreve a notificação ao WLC para mudar o VLAN de usuário da quarentena para alcançar o VLAN.
4. O tráfego de usuário começa deixar o WLC com a etiqueta do acesso VLAN. O server NAC já não está no trajeto para este tráfego do usuário particular.**Figura 1-6 certificou o desvio do cliente CAS comutando sobre para alcançar o VLAN**

O método o mais transparente para facilitar a autenticação de usuário Wireless é permitir a autenticação VPN-SSO no server NAC e configurar os WLC para enviar o RAIO que explica ao

server NAC. Caso os registros de contabilidade precisarem de ser enviados a um servidor Radius rio acima na rede, o server NAC pode ser configurado para enviar o pacote da contabilidade ao servidor Radius.

Nota: Se a autenticação VPN-SSO é permitida sem o agente limpo do acesso instalado no PC cliente, o usuário está autenticado ainda automaticamente. Contudo, não estão conectados automaticamente através da ferramenta NAC até que seu navegador da Web esteja aberto e uma tentativa de conexão estiver feita. Neste caso, quando o usuário abre seu navegador da Web, são reorientados momentaneamente (sem uma alerta de fazer logon) dentro da fase do "agente-menos". Quando o processo SSO está completo, estão conectados a sua URL originalmente pedida.

Configurar a solução Wireless NAC OOB

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Na aplicação atual NAC O WLC integra com a ferramenta NAC de Cisco no modo da em-faixa somente, onde a ferramenta NAC tem que permanecer no trajeto de dados mesmo depois que o usuário é certificado. Uma vez que a ferramenta NAC termina sua validação da postura, o empregado/convidado recebe o acesso do baseado na rede em seu papel.

Com a liberação NAC 4.5 e WLC 5.1, a integração dos apoios OOB da solução do Sem fio NAC com ferramenta NAC. Quando o cliente associa e termina L2Auth, verifica-se se a relação da quarentena esteja associada ao WLAN/SSID. Se sim, o tráfego inicial é enviado na relação da quarentena. Os fluxos de tráfego do cliente na quarentena VLAN, que é em tronco à ferramenta NAC. Uma vez que a validação da postura é feita, o gerente NAC envia a um SNMP a mensagem ajustada que atualiza o ID de VLAN do acesso; o controlador atualiza-se com o ID de VLAN do acesso, e o tráfego de dados começa comutar do controlador diretamente à rede sem o server NAC.

Figura exemplo de 2-1 de CAS autônomo no modo de Bridge conectado ao WLC através do interruptor

Em figura 2-1, o WLC é conectado a uma porta de tronco que leve a quarentena VLAN e o acesso VLAN (176 e 175). No interruptor, o tráfego de VLAN da quarentena é em tronco à ferramenta NAC, e o tráfego de VLAN do acesso é em tronco diretamente ao interruptor Layer3. Trafique que alcança a quarentena VLAN na ferramenta NAC é traçado para alcançar o VLAN baseado na configuração do mapeamento estático. Quando os associados do cliente terminam o AUTH L2, verifica se a relação da quarentena é associada; se sim, os dados são enviados na relação da quarentena. Os fluxos de tráfego do cliente na quarentena VLAN, que é em tronco à ferramenta NAC. Uma vez que a validação da postura é feita, o server NAC (CAS) envia a um SNMP a mensagem ajustada que atualiza o ID de VLAN do acesso ao controlador, e aos começos do tráfego de dados para comutar do WLC diretamente à rede sem o server NAC.

Restrições

- Nenhum perfil da porta associado
- Nenhum ID de VLAN especificado no gerente NAC: definido no WLC

- O apoio do filtro MAC não pode usar o ID de VLAN dos ajustes do papel
- Apoio virtual fora da banda do modo de servidor do gateway NAC somente
- Associação da camada 2 entre o server WLC e NAC
- O NAC ISR e o WLC NM não podem estabelecer-se para fazer o Sem fio OOB NAC

Nota: Refira o mapeamento VLAN na seção dos modos de gateway virtual da ferramenta NAC de Cisco - o guia de configuração do servidor de acesso limpo, libera 4.8(1) para obter mais informações sobre de como configurar com segurança VLAN nos modos de gateway virtual.

Configuração de Catalyst switch

```
interface GigabitEthernet2/21
 description NAC SERVER UNTRUSTED INTERFACE switchport switchport trunk native vlan 998
switchport trunk allowed vlan 176 switchport mode trunk no ip address ! interface
GigabitEthernet2/22 description NAC SERVER TRUSTED INTERFACE switchport switchport trunk native
vlan 999 switchport trunk allowed vlan 11,175 switchport mode trunk no ip address ! interface
GigabitEthernet2/23 description NAC MANAGER INTERFACE switchport switchport access vlan 10 no ip
address spanning-tree portfast ! interface GigabitEthernet2/1 description WLC switchport
switchport trunk allowed vlan 75,175,176 switchport trunk native vlan 75 switchport mode trunk
no ip address ! interface Vlan75 Description WLC Management VLAN ip address 10.10.75.1
255.255.255.0 ! interface Vlan175 Description Client Subnet Access VLAN ip address 10.10.175.1
255.255.255.0 end
```

Etapas para configurar NAC OOB no gerente WLC e NAC

Siga estas etapas para configurar NAC OOB no gerente WLC e NAC:

1. Permita o modo SNMP v2 no controlador.
2. Crie um perfil para o WLC no gerente CAM. Clique o **perfil > o dispositivo do Gerenciamento OOB > novo**.
3. Uma vez que o perfil é criado no CAM, adicionar o WLC no perfil; vá ao **Gerenciamento > aos dispositivos OOB > novo** e incorpore o endereço IP de gerenciamento do WLC.O controlador é adicionado agora no gerente CAM.
4. Adicionar o CAM como o receptor de armadilha de SNMP do WLC. Use o nome exato do receptor de armadilha no CAM como o receptor SNMP.
5. Configurar o receptor de armadilha de SNMP no CAM com o mesmo nome, que é especificado no controlador; clique perfis sob o **Gerenciamento OOB > o receptor SNMP**.Nesta fase, o WLC e o CAM podem falar entre si para atualizações do estado da validação e do acesso/quarentena da postura do cliente.
6. No controlador, crie uma interface dinâmica com o acesso e a quarentena VLAN.
7. Crie o WLAN, e associe-o com a interface dinâmica.
8. Finalmente, permita o NAC no WLAN.
9. Adicionar a sub-rede de cliente no server de CAS como a sub-rede controlada; clique o **server de CAS > selecionam seus server de CAS > endereço IP de Um ou Mais Servidores Cisco ICM NT não utilizado >Advanced > controlado Manage das sub-redes do >Add da sub-rede de cliente** e põem a quarentena VLAN (não-confiável VLAN) para a sub-rede controlada.
10. Crie mapeamentos VLAN em CAS. Escolha o **server de CAS > selecionam seu server de CAS > controlam > avançou > mapeamento VLAN**. Adicionar o acesso VLAN como confiado e a quarentena VLAN como o não-confiável.

Configurar único Sinal-em (SSO) com a solução Wireless OOB

Estas são as exigências permitir o Sem fio SSO:

1. Permita a autenticação VPN no server NAC — o WLC é definido como o “concentrador VPN” na ferramenta NAC.
2. Permita a contabilidade do RAIO no WLC — o controlador que é definido na ferramenta NAC deve ser configurado para enviar registros de contabilidade do RAIO à ferramenta NAC para cada 802.1x/EAP WLAN que é uma sub-rede controlada no NAC.

Etapas para configurar o SSO no gerente NAC

Siga estas etapas para configurar o SSO no gerente NAC:

1. Do menu da mão esquerda CAM, sob o Gerenciamento de dispositivos, escolha o **server CCA**, e clique então o link do **server NAC**.
2. Da página do status de servidor, escolha a aba da **autenticação** e então o secundário-menu do **AUTH VPN**. Veja figura 3-1.**Figura 3-1 permitindo o único Sinal-no server NAC**
3. Escolha os **concentradores VPN que ajustam-se** (figura 3-2) para adicionar uma entrada nova do WLC. Povoe os campos de entrada para o endereço IP de gerenciamento WLC e o segredo que compartilhado você quer se usar entre o server WLC e NAC.**Figura 3-2 adiciona o WLC como um cliente RADIUS sob a seção do concentrador VPN**
4. Para o mapeamento do papel, adicionar o Authentication Server novo com tipo **sso do vpn** sob o **gerenciamento de usuário > os servidores de autenticação**.
5. Clique o ícone do **mapeamento** e adicionar então a **regra do mapeamento**. O mapeamento varia o dependente em cima do valor do atributo de classe 25 que o WLC envia no pacote da contabilidade. Este valor de atributo é configurado no servidor Radius e varia baseado na autorização de usuário. Neste exemplo, o valor de atributo é **ALLOWALL**, e é colocado no papel **AllowAll**.

Etapas para configurar o SSO no controlador do Wireless LAN

A contabilidade do RAIO precisa de ser configurada no WLC para conseguir único Sinal-na capacidade com o server NAC.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Comandos CLI de CISCO WLC para a verificação

```
(Cisco Controller) >show interface summary

Interface Name    Port Vlan Id    IP Address      Type    Ap Mgr Guest
------------------------------------------------ ---- -------- ------
ap-manager        1    untagged   10.10.75.3      Static  Yes    No
management        1    untagged   10.10.75.2      Static  No     No
nac-vlan          1    175        10.10.175.2     Dynamic No     No
service-port      N/A  N/A        192.168.1.1     Static  No     No
```

```
virtual          N/A  N/A        1.1.1.1         Static  No     No


(Cisco Controller) >show interface detailed management

Interface Name................................. management
MAC Address.................................... 00:18:73:34:b2:60
IP Address..................................... 10.10.75.2
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.10.75.1
VLAN........................................... untagged
Quarantine-vlan................................ 0
Active Physical Port........................... 1
Primary Physical Port.......................... 1
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.10.75.1
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ Unconfigured
AP Manager..................................... No
Guest Interface................................ No

(Cisco Controller) >show interface detailed nac-vlan

Interface Name................................. nac-vlan
MAC Address.................................... 00:18:73:34:b2:63
IP Address..................................... 10.10.175.2
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.10.175.1
VLAN........................................... 175 Quarantine-
vlan.............................. 176 Active Physical Port.......................... 1
Primary Physical Port.......................... 1 Backup Physical
Port........................... Unconfigured Primary DHCP Server.............................
10.10.175.1 Secondary DHCP Server.......................... Unconfigured DHCP Option
82............................... Disabled ACL.....................................
Unconfigured AP Manager..................................... No Guest
Interface.............................. No
```

Verificação do estado do cliente de WLC GUI

Inicialmente a corrente está em um estado da quarentena até que a análise da postura esteja feita na ferramenta NAC.

O estado NAC do cliente deve ser **acesso** depois que a análise da postura é terminada.

Verificação de único Sinal-no server NAC com WLC

Sob o AUTH VPN, vá à subseção do **cliente ativo** verificar se o pacote de início de contabilidade chegou do WLC. Esta entrada aparece com o agente CCA instalado na máquina cliente.

Você precisa de abrir um navegador para terminar o único Sinal-no processo sem um agente. Quando o usuário abre o navegador, o processo SSO ocorre, e o usuário aparece na lista de usuário on-line (OUL). Com o pacote de fim de relatório do RAIO, o usuário é removido da lista do cliente ativo.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Informações Relacionadas

- Remote Authentication Dial-In User Service (RADIUS)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems