Configurando a URL integrada que registra e relatório do tráfego do convidado em uma rede Cisco

Índice

Introdução

Este documento descreve como integrar um servidor convidado NAC (NGS) com controladores de LAN Wireless (WLCs) e um mecanismo de segurança adaptável (ASA) para fornecer a geração de registros e relatórios de URL do tráfego de convidado. Muitas empresas exigem a monitoração do tráfego do convidado e este artigo fornece as informações sobre como configurar componentes Cisco para cumprir essa exigência.

Note que há umas soluções da Cisco múltiplas para configurar o acesso do convidado em uma rede Cisco. Este artigo centra-se sobre o método que usa o WLC como a tecnologia de possibilidade. O WLC tem a capacidade original ao tráfego de túnel da margem de rede ao Internet com EoIP. Esta característica elimina a necessidade de distribuir VPN ou ACL dentro da infraestrutura de rede para restringir o tráfego do convidado do escape na rede interna da empresa.

O volume deste artigo cobre “integrou a URL que registra e que relata” em uma rede do “Sem fio-convidado”, mas esta característica pode ser configurada em uma rede do “prender-convidado”, também. O apêndice A fornece detalhes para uma rede do “prender-convidado”.

Pré-requisitos

Requisitos

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

- ASA que executa a versão 8.0.4.24 ou mais recente
- Dois controladores da série do WLC-4400 que executam a versão 4.2.130 ou mais recente
- Server do convidado NAC que executa a versão 2.0 ou mais recente

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA que corridas 8.0.4.26
- Dois controladores do WLC-44xx que executam o código 4.2.130
- Server do convidado NAC que executa o código 2.0.0
- Catalyst 6500

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

O acesso wireless do convidado fornece benefícios para os negócios significativos aos clientes. Estes benefícios incluem custos operacionais reduzidos, produtividade melhorada, e Gerenciamento e abastecimento simplificados do acesso do convidado. Além, o server do convidado NAC permite clientes de indicar seu Acceptable Use Policy e de exigir a aceitação desta política antes de conceder o acesso ao Internet. Agora, com a adição de URL integrada que registra e que relata, os clientes podem registrar o uso do convidado e a conformidade da trilha contra seu Acceptable Use Policy.

Configurar

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Topologia de lab do Sem fio-convidado

O Catalyst 6500 é usado para simular a rede de empreendimento. O convidado SSID, mostrado no vermelho, traça ao VLAN nativo no ASA, igualmente mostrado no vermelho. Fluxos de tráfego do convidado do PC no Access point, através do túnel LWAPP ao controlador estrangeiro WLC, e então através do túnel de EoIP ao controlador da âncora WLC. O controlador da âncora proporciona o DHCP e os serviços de autenticação para a rede de convidado. O serviço DHCP fornece o convidado um endereço IP de Um ou Mais Servidores Cisco ICM NT, um gateway padrão, e um servidor DNS. O gateway padrão é o ASA, e o servidor DNS é um server público situado no Internet. O serviço de autenticação no controlador da âncora comunica-se com os NG através do RAIO para autenticar usuários contra o base de dados de usuário convidado nos NG. O fazer logon do convidado é iniciado quando o convidado abre um navegador da Web, e o controlador da âncora reorienta o tráfego à página da autenticação. Todo o tráfego dentro e fora da sub-rede do convidado é filtrado com o ASA para o controle de política e o exame.

URL integrada que registra do ASA aos NG

O registro integrado URL é ativado quando você permite estes:

- Contabilidade do RAIO do controlador da âncora WLC aos NG
- O registro do HTTP obtém pedidos no ASA
- Emissão dos mensagens do syslog do ASA aos NG

A contabilidade do RAIO fornece os NG um mapeamento entre o endereço IP de Um ou Mais Servidores Cisco ICM NT do convidado e o usuário convidado - identificação por um período de tempo específico. O registro do HTTP obtém pedidos fornece os NG um log de que URL foi visitada pelo endereço IP de Um ou Mais Servidores Cisco ICM NT do convidado quando. Os NG podem então correlacionar esta informação para produzir um relatório que mostre as URL visitadas por um convidado particular por um período de tempo particular.

Note que o tempo precisa está exigido para que esta correlação trabalhe corretamente. Por este motivo, a configuração dos servidores de NTP é altamente recomendado no ASA, no WLC, e nos NG.

Configurações

Este documento utiliza as seguintes configurações:

- Configuração ASA
- Configuração de WLC
- Configuração NG

Configuração ASA

As tarefas de configuração chaves no ASA incluem estes:

- NTP
- Inspeção HTTP
- Syslog

O NTP é exigido para segurar a correlação apropriada das mensagens pelos NG. A inspeção HTTP permite o registro URL. O Syslog é o método usado para enviar os logs URL aos NG.

Neste exemplo, este comando é usado permitir o NTP no ASA:

```
ntp server 192.168.215.62
```

A inspeção HTTP permite o ASA de registrar URL. Especificamente, o comando **HTTP da inspeção** permite ou desabilita o registro do pedido GET com mensagem do syslog 304001.

O comando **HTTP da inspeção** é colocado sob um mapa de classe dentro de um mapa de política. Quando permitidos com o **comando service-policy**, os logs de inspeção HTTP obtêm pedidos com mensagem do syslog 304001. O código é exigido 8.0.4.24 ASA ou mais tarde para o mensagem do syslog 304001 para mostrar o hostname como parte da URL.

Neste exemplo, estes são os comandos relevant:

```
policy-map global_policy
 class inspection_default
  inspect http
!
service-policy global_policy global
```

O Syslog é o método usado para comunicar a URL que registra aos NG. Nesta configuração, somente o mensagem do syslog 304001 é enviado aos NG com esta configuração:

```
logging enable
logging timestamp
logging list WebLogging message 304001
logging trap WebLogging
logging facility 21
logging host inside 192.168.215.16
```

Configuração de WLC

As etapas de configuração chaves para os controladores do Wireless LAN incluem estes:

- Acesso básico do convidado
- NTP
- Contabilidade RADIUS

A configuração básica do acesso do convidado envolve a configuração de um controlador estrangeiro do controlador WLC e da âncora WLC de modo que o tráfego do convidado seja escavado um túnel através da rede de empreendimento ao Internet DMZ. A configuração do acesso básico do convidado é coberta na documentação separada. As ilustrações que mostram a configuração para a instalação são cobertas no apêndice.

Os servidores de NTP são adicionados na tela Controller/NTP.

Configuração de NTP no WLC

Um servidor de contabilidade do RAIO é exigido de modo que o server NG possa traçar o endereço IP de origem recebido nos mensagens do syslog ASA ao convidado que usa esse endereço nesse tempo particular.

Estas duas telas mostram a configuração da contabilidade da autenticação RADIUS e do RAIO no controlador da âncora WLC. A configuração RADIUS não é exigida no controlador estrangeiro.

Autenticação RADIUS Contabilidade RADIUS

Configuração NG

- NTP
- Clientes RADIUS
- Syslog

O server NG é configurado do página da web de https://(ip_address)/admin. O nome de usuário/senha padrão é admin/admin.

Os servidores de NTP são adicionados na tela do server/ajustes. Recomenda-se que o fuso horário do sistema esteja ajustado ao fuso horário onde o server é encontrado fisicamente. Quando o NTP é sincronizado, você vê uma mensagem na parte inferior desta tela que diz, “estado: Servidores de NTP ativos” junto com o endereço IP de Um ou Mais Servidores Cisco ICM NT que mostra “a fonte das horas atual.”

Configuração de NTP NG

O server NG precisa de ser configurado com o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador da âncora como um cliente RADIUS. Esta tela é ficada situada na página Devices/RADIUS-Clients. Certifique-se de que o segredo compartilhado é o mesmo que foi entrado no controlador da âncora. Clique o **botão Restart Button** depois que você faz mudanças para reiniciar o serviço de raio no server NG.

Clientes RADIUS

Àrevelia, o server NG aceita mensagens do syslog de todo o endereço IP de Um ou Mais Servidores Cisco ICM NT. Em consequência, não há nenhuma etapa adicional exigida para receber os mensagens do syslog do ASA.

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.

Siga estas etapas para verificar que trabalhos de registro URL corretamente.

1. De um PC cliente, conecte à rede de convidado wireless. O PC recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT, um gateway padrão, e um servidor DNS do servidor DHCP no controlador da âncora.
2. Abra um navegador da Web. Você é reorientado a uma tela de login. Incorpore um nome de usuário e senha do convidado. Em cima da autenticação bem sucedida, você é reorientado a uma página padrão no Internet.
3. Consulte aos vários página da web no Internet.
4. Conecte um Gerenciamento PC aos NG em https://(ip_address) e o início de uma sessão como um patrocinador.
5. Clique o **Gerenciamento de conta**. Você vê uma lista de contas do convidado. (Se sua conta

do convidado não aparece, clique o botão da **pesquisa avançada** e cancele o filtro que especifica que este patrocinador pode somente ver as contas que criaram.)

6. Encontre a conta de usuário convidado da lista. Enrole a direita até que você ver o ícone dos detalhes. Clique o ícone dos **detalhes**.
7. Clique a aba do **log de atividade**. Você vê uma lista das URL que o convidado visitou.**Relatório de registro URL para o usuário**

O relatório mostra que o usuário convidado visitou http://www.cisco.com o 1º de abril de 2009 em 2:51 PM. O endereço de dispositivo de 192.168.59.49 é o endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA que enviou o mensagem do syslog que contém o log URL. O endereço IP de origem para os usuários convidado é 192.168.0.10. O endereço de destino é 192.168.219.25 para http://www.cisco.com.

Apêndices

Apêndice A – Opção do Prender-convidado

Até este ponto, este artigo cobriu “URL integrada que registra e que relata do tráfego do convidado” para o uso em uma rede do “Sem fio-convidado”. Esta seção fornece detalhes para configurar também um “prender-convidado,”. os Prender-convidados e os Sem fio-convidados podem ser permitidos no mesmo controlador estrangeiro WLC.

Este é o diagrama da rede para o laboratório da rede do Prender-convidado.

Topologia de lab do Prender-convidado

A topologia de lab do prender-convidado é similar à topologia de lab do Sem fio-convidado, mostrada mais cedo, à exceção da adição de um prender-convidado VLAN. O prender-convidado VLAN, mostrado no vermelho, é uma conexão da camada 2 entre o prender-convidado PC e o controlador estrangeiro WLC. O tráfego do prender-convidado é recebido pelo controlador estrangeiro WLC e enviado por EoIP ao controlador da âncora WLC. O controlador da âncora WLC proporciona o DHCP e os serviços de autenticação para o usuário do prender-convidado da mesma forma que proporcionou estes serviços para o usuário do Sem fio-convidado. O gateway padrão é o ASA, e o servidor DNS é um server público no Internet. Logicamente, todo o tráfego dentro e fora da sub-rede é protegido pelo ASA.

Recomenda-se não configurar uma relação da camada 3 no Prender-convidado VLAN desde que este pode permitir um ponto da desconexão para que o tráfego escape fora do prender-convidado VLAN na rede corporativa.

Apêndice B – Configurações detalhadas para os WLC

Controlador da âncora WLC

Relações do controlador da âncora

A configuração das relações no controlador da âncora é mostrada:

O ap-gerente e as interfaces de gerenciamento estão no VLAN nativo da porta física 1 do WLC. A porta 1 conecta ao Catalyst Switch e recebe o tráfego da rede cliente. O tráfego do convidado é recebido através do túnel de EoIP do controlador estrangeiro e termina através desta porta.

A relação do convidado está no VLAN nativo da porta 2, e a relação prendida está em VLAN 9 da porta 2 da porta 2. conecta ao ASA e é usada para enviar para fora o tráfego ao Internet.

Grupos de mobilidade do controlador da âncora

Para este exemplo, um grupo da mobilidade é configurado para o controlador estrangeiro (prendido) e um grupo separado da mobilidade para o controlador da âncora (âncora). A configuração no controlador da âncora é mostrada.

Controlador WLAN da âncora

Controlador da âncora - Ajuste a âncora para o convidado WLAN

A fim configurar ou mostrar âncoras da mobilidade para um WLAN, mova seu rato para a seta da gota-para baixo no direito, e escolha **âncoras da mobilidade**, como mostrado.

Controlador da âncora - Seajuste- a âncora Controlador da âncora - WLAN para usuários do Sem fio-convidado Controlador da âncora - WLAN para os usuários do prender-convidado (opcionais) Controlador da âncora - Escopos de DHCP Controlador da âncora - Escopo de DHCP para Sem fio-convidados: Controlador da âncora - DHCP para os Prender-convidados (opcionais):

Controlador estrangeiro WLC

Relações

A configuração das relações no controlador estrangeiro é mostrada.

O ap-gerente e as interfaces de gerenciamento estão no VLAN nativo da porta física 1 do WLC.

A relação prendida é *opcional* e é exigida somente se você quer fornecer o acesso do prender-convidado. A relação prendida está em VLAN 8 da porta física 1. Esta relação recebe o tráfego do convidado VLAN do Catalyst Switch e envia-lhe para fora o túnel de EoIP, com o VLAN nativo, ao controlador da âncora.

Controlador estrangeiro - Grupos de mobilidade

A configuração no controlador estrangeiro é mostrada.

Controlador estrangeiro - WLAN

A fim configurar ou mostrar âncoras da mobilidade para um WLAN, movem seu rato sobre a seta da gota-para baixo no direito e escolhem **âncoras da mobilidade**, como mostrado.

Âncora da mobilidade ajustada para ancorar o controlador Controlador estrangeiro - Convidado WLAN para usuários do Sem fio-convidado

s

Controlador estrangeiro - WLAN para os usuários do Prender-convidado (opcionais) – continuado

C do apêndice – Configuração ASA

```
ASA-5520# show run
:
ASA Version 8.0(4)26
!
hostname ASA-5520
```

```
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.59.49 255.255.255.240
!
interface GigabitEthernet0/2
   <- Guest traffic enters this interface
 nameif wireless_guest
 security-level 50
 ip address 192.168.0.254 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.99.1 255.255.255.0
 management-only
!
boot system disk0:/asa804-26-k8.bin
clock timezone CST -6
clock summer-time CDT recurring
logging enable
logging timestamp
   <- provide a timestamp in each syslog message
logging list WebLogging message 304001
   <- list includes URL Log message (304001)
logging console errors
logging buffered notifications
logging trap WebLogging
   <- Send this list of Log messages to syslog servers
logging asdm informational
logging facility 21
logging host inside 192.168.215.16
   <- NGS is the syslog server
asdm image disk0:/asdm-61551.bin
route inside 10.10.10.0 255.255.255.0 192.168.59.62 1
route inside 192.168.215.0 255.255.255.0 192.168.59.62 1
route inside 198.168.1.15 255.255.255.255 192.168.59.62 1
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.99.0 255.255.255.0 management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 198.168.1.15 <- Configure ntp server
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect http
   <- Enable http inspection on the global policy
!
service-policy global_policy global
   <- Apply the policy
prompt hostname context
Cryptochecksum:b43ff809eacf50f0c9ef0ae2a9abbc1d
: end
```

Informações Relacionadas

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