Autenticação de usuário ASA VPN contra o server de Windows 2008 NP (diretório ativo) com exemplo da configuração RADIUS

Índice

Introdução

Este documento explica como configurar uma ferramenta de segurança adaptável (ASA) para comunicar-se com um server da política de rede de Microsoft Windows 2008 (NP) com o protocolo de raio de modo que os usuários do Cisco VPN Client/AnyConnect/sem clientes WebVPN do legado sejam autenticados contra o diretório ativo. Os NP são um dos papéis do servidor oferecidos pelo server de Windows 2008. É equivalente ao server de Windows 2003, IAS (Internet Authentication Service), que é a aplicação de um servidor Radius para fornecer a autenticação de usuário de discagem remota. Similarmente, no server de Windows 2008, os NP são a aplicação de um servidor Radius. Basicamente, o ASA é um cliente RADIUS a um servidor Radius NP. O ASA envia pedidos da autenticação RADIUS em nome dos usuários VPN e os NP autenticam-nos contra o diretório ativo.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- ASA que executa a versão 9.1(4)
- Server R2 de Windows 2008 com serviços de diretório ativo e papel NP instalado

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.

Configurar

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

Diagrama de Rede

Configurações

Configuração ASDM

1. Escolha o grupo de túneis para que a autenticação NP é exigida.
2. O clique **edita** e escolhe **básico**.
3. Na seção da autenticação, o clique **controla**.
4. Nos Grupos de servidores AAA secione, clique **adicionam**.
5. No campo do Grupo de servidores AAA, dê entrada com o nome do grupo de servidor (por exemplo, NP).
6. Da lista de drop-down do protocolo, escolha o **RAIO**.
7. Clique em **OK**.
8. Nos server na seção de grupo selecionada, escolha o Grupo de servidores AAA adicionado e o clique **adiciona**.
9. No campo do nome do servidor ou do endereço IP de Um ou Mais Servidores Cisco ICM NT, incorpore o endereço IP do servidor.
10. No campo chave do segredo de servidor, incorpore a chave secreta.
11. Saa da porta da autenticação de servidor e dos campos de porta de relatório do server no valor padrão a menos que o server escutar em uma porta diferente.
12. Clique em **OK**.
13. Clique em **OK**.
14. Da lista de drop-down do Grupo de servidores AAA, escolha o grupo (NP neste exemplo) adicionado nas etapas precedentes.
15. Clique em **OK**.

Configuração de CLI

```
aaa-server NPS protocol radius
aaa-server NPS (inside) host 10.105.130.51
 key *****

tunnel-group TEST type remote-access
tunnel-group TEST general-attributes
 address-pool test
 authentication-server-group (inside) NPS
tunnel-group TEST webvpn-attributes
 group-alias TEST enable

ip local pool test 192.168.1.1-192.168.1.10 mask 255.255.255.0
```

Àrevelia, o ASA usa o tipo do autenticação do protocolo de autenticação da senha não criptografada (PAP). Isto não significa que o ASA envia a senha no texto simples quando envia o pacote de REQUISIÇÃO RADIUS. Um pouco, a senha de texto simples é cifrada com o segredo compartilhado RAIO.

Se o gerenciamento de senha é permitido sob o grupo de túneis, a seguir o ASA usa o tipo do autenticação MSCHAP-v2 a fim cifrar a senha de texto simples. Em tal caso, assegure-se de que a caixa de verificação **capaz de Microsoft CHAPv2** esteja verificada dentro o indicador do servidor AAA da edição configurado na seção de configuração ASDM.

```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> Nota: **O comando authentication do AAA-server do teste** usa sempre o PAP. Somente quando um usuário inicia uma conexão ao grupo de túneis com o gerenciamento de senha permitido faz o uso MSCHAP-v2 ASA. Também, do “a opção do [password-expire-in-days days] gerenciamento de senha” é apoiada somente com Lightweight Directory Access Protocol (LDAP). O RAIO não fornece esta característica. Você verá a senha expirar opção quando a senha é expirada já no diretório ativo.

Server de Windows 2008 com configuração NP

O papel do servidor NP deve ser instalado e sendo executado no server de Windows 2008. Se não, escolha o **Iniciar > Ferramentas Administrativas > do > Add os papéis do servidor dos serviços do papel**. Escolha o server da política de rede e instale o software. Uma vez que o papel do servidor NP é instalado, termine estas etapas a fim configurar os NP para aceitar e processar pedidos da autenticação RADIUS do ASA:

1. Adicionar o ASA como um cliente RADIUS no server NP. Escolha **ferramentas administrativas > server da política de rede.**Clicar com o botão direito **clientes RADIUS** e escolha **novo**.Incorpore um nome amigável, um endereço (IP ou DNS), e um segredo compartilhado configurado no ASA.Clique na guia Advanced.Da lista de drop-down do nome de fornecedor, escolha o **padrão RADIUS**.Clique em **OK**.
2. Crie uma política do pedido de nova conexão para usuários VPN. A finalidade da política do pedido de conexão é especificar se os pedidos dos clientes RADIUS devem ser processado localmente ou enviada aos servidores de raio remotos. Sob os NP > as políticas, clicam com o botão direito **políticas do pedido de conexão** e criam uma política nova.Da lista de drop-

down do servidor de acesso do tipo de rede, escolha **não especificado**.Clique a aba das **circunstâncias**.Clique em Add.Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA como do “uma condição dos endereços do IPv4 cliente.Clique a aba dos **ajustes**.Sob o pedido de conexão da transmissão, escolha a **autenticação**. Assegure-se de que os pedidos da autenticação neste botão de rádio do server estejam escolhidos.Clique em **OK**.

3. Adicionar uma política de rede onde você possa especificar são permitidos a que usuários autenticar.Por exemplo, você pode adicionar grupos de usuário do diretório ativo como uma circunstância. Somente aqueles usuários que pertencem a um grupo especificado de Windows são autenticados sob esta política.Sob NP, escolha **políticas**.Clicar com o botão direito a **política de rede** e crie uma política nova.Assegure-se de que o botão de rádio do acesso de Grant esteja escolhido.Da lista de drop-down do servidor de acesso do tipo de rede, escolha **não especificado**.Clique a aba das **circunstâncias**.Clique em Add.Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA como uma condição do endereço do IPv4 do cliente.Incorpore o grupo de usuário do diretório ativo que contém usuários VPN.Clique a aba das **limitações**.Escolha **métodos de autenticação**.Assegure-se de que a caixa de verificação da autenticação não criptografada (PAP, SPAP) esteja verificada.Clique em **OK**.

Passe o atributo da Grupo-política (atributo 25) do servidor Radius NP

Se a grupo-política precisa de ser atribuída dinamicamente ao usuário com o servidor Radius NP, o atributo RADIUS da grupo-política (atributo 25) pode ser usado.

Termine estas etapas a fim enviar o atributo RADIUS 25 para a atribuição dinâmica de uma grupo-política ao usuário.

1. Depois que a política de rede é adicionada, clicar com o botão direito a política da rede obrigatória e clique a aba dos **ajustes**.
2. Escolha **atributos RADIUS > padrão**. Clique em Add. Deixe o tipo de acesso como tudo.
3. Nos atributos encaixote, escolha a **classe** e o clique **adiciona**. Incorpore o valor de atributo, isto é, o nome da grupo-política como uma corda. Recorde que uma grupo-política com este nome tem que ser configurada no ASA. Isto é de modo que o ASA o atribua à sessão de VPN depois que recebe este atributo na resposta do RAIO.

Verificar

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

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

O ASA debuga

Enable **debuga o raio todo no** ASA.

```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password
add_req 0x787a6424 session 0x80000001 id 8
RADIUS_REQUEST
radius.c: rad_mkpkt

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 65).....
01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f    |  ...A.....~m...
40 50 a8 36 01 09 76 70 6e 75 73 65 72 02 12 28    |  @P.6..vpnuser..(
c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04    |  .h.........Z.oC.
06 0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00    |  ..i........=....
05                                                 |  .

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 8 (0x08)
Radius: Length = 65 (0x0041)
Radius: Vector: C41BAB1AE37E6D12DA876F7F4050A836
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
76 70 6e 75 73 65 72                               |  vpnuser
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
28 c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43    |  (.h.........Z.oC
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.105.130.52 (0x0A6982DE)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
send pkt 10.105.130.51/1645
rip 0x787a6424 state 7 id 8
rad_vrfy() : response message verified
rip 0x787a6424
 : chall_state ''
 : state 0x7
 : reqauth:
    c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 40 50 a8 36
 : info 0x787a655c
    session_id 0x80000001
    request_id 0x8
    user 'vpnuser'
    response '***'
    app 0
    reason 0
    skey 'cisco'
    sip 10.105.130.51
    type 1

RADIUS packet decode (response)
```

```
------------------------------------
Raw packet data (length = 78).....
02 08 00 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37    |  ...N..Kv ....+.7
bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 00 02    |  ..lL............
19 2e 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a    |  .........7.....j
2c bf 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf    |  ,.....<..n...@..
1e 3a 18 6f 05 81 00 00 00 00 00 00 00 03          |  .:.o..........

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 8 (0x08)
Radius: Length = 78 (0x004E)
Radius: Vector: E8884B7620B6AAD30D2B9437BF9A6C4C
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 25 (0x19) Class
Radius: Length = 46 (0x2E)
Radius: Value (String) =
9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a 2c bf    |  .......7.....j,.
00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a    |  ....<..n...@...:
18 6f 05 81 00 00 00 00 00 00 00 03                |  .o..........
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x787a6424 session 0x80000001 id 8
free_rip 0x787a6424
radius: send queue empty
INFO: Authentication Successful
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Assegure-se de que a Conectividade entre o ASA e o server NP seja boa.Aplique capturas de pacote de informação para assegurar-se de que o pedido de autenticação saa da relação ASA (de onde o server é alcançável). Confirme que os dispositivos no trajeto não obstruem a porta 1645 UDP (porta de autenticação do raio padrão) a fim a assegurar alcançam o server NP. Mais informação em capturas de pacote de informação no ASA pode ser encontrada em ASA/PIX/FWSM: Pacote que captura usando o CLI e o exemplo da configuração ASDM.
- Se a autenticação ainda falha, olhe no visualizador de eventos nos indicadores NP. Sob o visualizador de eventos > os logs de Windows, escolha a **Segurança.** Procure os eventos associados com os NP em torno da época do pedido de autenticação.Uma vez que você abre propriedades do evento, você deve poder ver a razão para a falha segundo as indicações do exemplo. Neste exemplo, o PAP não foi escolhido como o tipo do autenticação sob a política de rede. Daqui, o pedido de autenticação falha. `Log Name:  Security`
  `Source:  Microsoft-Windows-Security-Auditing`
  `Date:  2/10/2014 1:35:47 PM`
  `Event ID:  6273`
  `Task Category: Network Policy Server`
  `Level:  Information`
  `Keywords:  Audit Failure`
  `User:  N/A`

Computer: win2k8.skp.com
Description:
Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
   Security ID: SKP\vpnuser
   Account Name: vpnuser
   Account Domain: SKP
   Fully Qualified Account Name: skp.com/Users/vpnuser

Client Machine:
   Security ID: NULL SID
   Account Name: -
   Fully Qualified Account Name: -
   OS-Version: -
   Called Station Identifier: -
   Calling Station Identifier: -

NAS:
   NAS IPv4 Address: 10.105.130.69
   NAS IPv6 Address: -
   NAS Identifier: -
   NAS Port-Type: Virtual
   NAS Port: 0

RADIUS Client:
   Client Friendly Name: vpn
   Client IP Address: 10.105.130.69

Authentication Details:
   Connection Request Policy Name: vpn
   Network Policy Name: vpn
   Authentication Provider: Windows
   Authentication Server: win2k8.skp.com
   Authentication Type: PAP
   EAP Type: -
   Account Session Identifier: -
   Logging Results: Accounting information was written to the local log file.
   Reason Code: 66
   Reason: **The user attempted to use an authentication method that is not enabled on the matching network policy.**