AnyConnect SSL sobre IPv4+IPv6 à configuração ASA

Índice

Introdução

Este documento fornece uma configuração de exemplo para a ferramenta de segurança adaptável de Cisco (ASA) para permitir que o Cliente de mobilidade Cisco AnyConnect Secure (referido como “AnyConnect” no restante deste documento) estabeleça um túnel SSL VPN sobre uma rede do IPv4 ou do IPv6.

Além, esta configuração permite que o cliente passe o tráfego do IPv4 e do IPv6 sobre o túnel.

Pré-requisitos

Requisitos

A fim estabelecer com sucesso um túnel SSLVPN sobre o IPv6, cumpra estas exigências:

- A Conectividade fim-a-fim do IPv6 é exigida
- A versão de AnyConnect precisa de estar 3.1 ou mais atrasada
- A versão de software ASA precisa de estar 9.0 ou mais atrasada

Contudo, se qualqueras um exigências não são cumpridas, a configuração discutida neste documento ainda permitirá que o cliente conecte sobre o IPv4.

Componentes Utilizados

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

- ASA-5505 com versão de software 9.0(1)
- Cliente seguro 3.1.00495 da mobilidade de AnyConnect no profissional do Microsoft Windows XP (sem apoio do IPv6)

- Cliente seguro 3.1.00495 da mobilidade de AnyConnect na empresa de Microsoft Windows 7 de 32 bits

Convenções

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

Configuração

Primeiramente fora, defina um pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT de que você atribuirá um a cada cliente que conecta.

Se você quer o cliente levar igualmente o tráfego do IPv6 sobre o túnel, você precisará um pool de endereços do IPv6. Ambas as associações são providas mais tarde na grupo-política.

```
ip local pool pool4 172.16.2.100-172.16.2.199 mask 255.255.255.0
ipv6 local pool pool6 fcfe:2222::64/64 128
```

Para a Conectividade do IPv6 ao ASA, você precisa um endereço do IPv6 na relação a que os clientes conectarão (tipicamente a interface externa).

Para a Conectividade do IPv6 sobre o túnel aos host internos, você precisa o IPv6 na interface interna também.

```
interface Vlan90
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0
 ipv6 address 2001:db8:90::2/64
!
interface Vlan102
 nameif inside
 security-level 100
 ip address 192.168.102.2 255.255.255.0
 ipv6 address fcfe:102::2/64
```

Para o IPv6, você igualmente precisa uma rota padrão que aponta ao roteador de próximo salto para o Internet.

```
ipv6 route outside ::/0 2001:db8:90::5
route outside 0.0.0.0 0.0.0.0 203.0.113.5 1
```

A fim autenticar-se aos clientes, o ASA precisa de ter um certificado de identidade. As instruções em como criar ou importar tal certificado são além do alcance deste documento, mas podem facilmente ser encontradas em outros documentos como

/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98596-asa-8-x-3rdpartyvendorcert.html

A configuração resultante deve olhar similar ao seguinte:

```
crypto ca trustpoint testCA
```

```
 keypair testCA
 crl configure
...
crypto ca certificate chain testCA
 certificate ca 00
  30820312 308201fa a0030201 02020100 300d0609 2a864886 f70d0101 05050030
  ...
  quit
 certificate 04
  3082032c 30820214 a0030201 02020104 300d0609 2a864886 f70d0101 05050030
  ...
  quit
```

Então, instrua o ASA para usar este certificado para o SSL:

```
ssl trust-point testCA
```

Está em seguida a configuração básica do webvpn (SSLVPN) onde a característica é permitida na interface externa. Os pacotes do cliente que estão disponíveis para a transferência são definidos, e nós definem um perfil são definidos (mais nisto mais tarde):

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
 anyconnect profiles asa9-ssl-ipv4v6 disk0:/asa9-ssl-ipv4v6.xml
 anyconnect enable
```

Neste exemplo básico, o IPv4 e conjuntos de endereços do IPv6 é configurado, a informação de servidor de DNS (de que será empurrado para o cliente) e um perfil na grupo-política do padrão (DfltGrpPolicy). Muito mais atributos podem ser configurados aqui, e opcionalmente você pode definir grupo-políticas diferentes para grupos diferentes de usuários.

Note: O atributo “gateway-FQDN” é novo na versão 9.0 e define o FQDN do ASA porque se sabe no DNS. O cliente aprende este FQDN do ASA e usá-lo-á ao vaguear de um IPv4 a uma rede do IPv6 ou vice versa.

```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

Em seguida, configurar uns ou vários grupos de túneis. O padrão um (DefaultWEBVPNGroup) é usado para este exemplo, e configurar-lo para exigir o usuário autenticar usando um certificado:

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

Àrevelia, o cliente de AnyConnect tenta conectar sobre o IPv4 e, simplesmente se este falha, tenta conectar sobre o IPv6. Contudo, este comportamento pode ser mudado por um ajuste no perfil XML. O perfil "asa9-SSL-ipv4v6.xml" de AnyConnect que é provido na configuração acima, foi gerado usando o editor do perfil em ASDM (configuração - acesso remoto VPN - rede (cliente) perfil do cliente de Acccess - de AnyConnect).

O perfil resultante XML (com as a maioria da peça do padrão omitida para a brevidade):

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
 <ClientInitialization>
 ...


 <IPProtocolSupport>IPv6,IPv4</IPProtocolSupport>
 ...
</ClientInitialization>
 <ServerList>
 <HostEntry>
 <HostName>SSL to ASA9 (IPv4,IPv6)</HostName>
 <HostAddress>asa9.example.net</HostAddress> </HostEntry> </ServerList>
</AnyConnectProfile>
```

No perfil acima um hostname é definido igualmente (que podem ser qualquer coisa, não precisa de combinar o nome de host real do ASA), e um host address (que é tipicamente o FQDN do ASA).

Note: O campo do host address pode ser saido vazio, mas o campo do hostname deve conter o FQDN do ASA.

Note: A menos que o perfil PRE-for distribuído, a primeira conexão exige o usuário datilografar dentro o FQDN do ASA. Esta conexão inicial preferirá o IPv4. Após a conexão bem sucedida, o perfil será transferido. De lá, os ajustes do perfil serão aplicados.

Verificar

A fim verificar se um cliente está conectado sobre o IPv4 ou o IPv6, verifique o cliente GUI ou a sessão de VPN DB no ASA:

- No cliente, abra o indicador avançado, vá às estatísticas aba e verifique o endereço IP de Um ou Mais Servidores Cisco ICM NT do “server”.Este primeiro usuário está conectando de um sistema de Windows XP sem o apoio do IPv6:Este segundo usuário conecta de um host de Windows 7 com a Conectividade do IPv6 ao ASA:
- No ASA, da verificação CLI do “IP público” da “na saída do anyconnect mostra VPN-sessiondb”. Neste exemplo você pode ver as mesmas duas conexões que acima: um do XP sobre o IPv4 e um de Windows 7 sobre o IPv6:

```
asa9# show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username : Nanashi no Gombei Index : 45
Assigned IP : 172.16.2.101 Public IP : 192.0.2.95
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 13138 Bytes Rx : 22656
Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time : 11:14:29 UTC Fri Oct 12 2012
Duration : 1h:45m:14s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
Username : Uno Who Index : 48
Assigned IP : 172.16.2.100 Public IP : 2001:db8:91::7
```

```
Assigned IPv6: fcfe:2222::64
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11068 Bytes Rx : 10355
Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time : 12:55:45 UTC Fri Oct 12 2012
Duration : 0h:03m:58s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems