Ejemplo de Configuración de VPN Client y AnyConnect Client Access to Local LAN

Contenido

Introducción prerrequisitos Requisitos **Componentes Utilizados** Diagrama de la red Antecedentes Configuración del acceso LAN local para clientes VPN o AnyConnect Secure Mobility Client Configure el ASA a través del ASDM Configure el ASA a través de la CLI Configuración de Cisco AnyConnect Secure Mobility Client Preferencias de usuario Ejemplo de perfil XML Verificación **Cisco AnyConnect Secure Mobility Client** Probar el acceso LAN local con Ping Troubleshoot No se puede imprimir ni examinar por nombre Información Relacionada

Introducción

Este documento describe cómo permitir que Cisco VPN Client o Cisco AnyConnect Secure Mobility Client **sólo** accedan a su LAN local mientras se tunelizan en un Cisco Adaptive Security Appliance (ASA) 5500 Series o ASA 5500-X Series. Esta configuración permite a los clientes VPN de Cisco o a Cisco AnyConnect Secure Mobility Client acceder de forma segura a los recursos corporativos a través de IPsec, Secure Sockets Layer (SSL) o Internet Key Exchange versión 2 (IKEv2) y, aun así, ofrece al cliente la posibilidad de llevar a cabo actividades como la impresión en la ubicación del cliente. Si se permite, el tráfico destinado a Internet sigue tunelizado al ASA.

Nota: Esta no es una configuración para la tunelización dividida, donde el cliente tiene acceso no cifrado a Internet mientras está conectado al ASA o PIX. Consulte PIX/ASA 7.x: <u>Permita la Tunelización Dividida para Clientes VPN en el Ejemplo de Configuración de ASA</u> para obtener información sobre cómo configurar la tunelización dividida en el ASA.

prerrequisitos

Requisitos

Este documento asume que ya existe una configuración de VPN de acceso remoto funcional en el

ASA.

Consulte <u>Ejemplo de Configuración de PIX/ASA 7.x como Servidor VPN Remoto con ASDM</u> para Cisco VPN Client si uno no está configurado todavía.

Consulte <u>Ejemplo de Configuración de ASA 8.x VPN Access con AnyConnect SSL VPN Client</u> para Cisco AnyConnect Secure Mobility Client si no se ha configurado todavía.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA serie 5500 versión 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) versión 7.1(6)
- Cliente Cisco VPN versión 5.0.07.0440
- Cisco AnyConnect Secure Mobility Client versión 3.1.05152

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

El cliente se encuentra en una red típica de oficinas pequeñas/oficinas domésticas (SOHO) y se conecta a través de Internet a la oficina principal.



Antecedentes

A diferencia de un escenario clásico de tunelización dividida en el que todo el tráfico de Internet se envía sin cifrar, cuando habilita el acceso LAN local para los clientes VPN, permite que esos clientes se comuniquen sin cifrar con sólo los dispositivos de la red en la que se encuentran. Por ejemplo, un cliente al que se le permite el acceso LAN local mientras está conectado al ASA desde casa puede imprimir a su propia impresora pero no acceder a Internet sin enviar primero el tráfico a través del túnel.

Se utiliza una lista de acceso para permitir el acceso LAN local de la misma manera que se configura la tunelización dividida en el ASA. Sin embargo, en lugar de definir qué redes *deben* cifrarse, la lista de acceso en este caso define qué redes *no deben* cifrarse. Además, a diferencia del escenario de tunelización dividida, no es necesario conocer las redes reales de la lista. En su lugar, ASA proporciona una red predeterminada de 0.0.0/255.255.255.255, lo que se entiende como la LAN local del cliente.

Nota: Cuando el cliente está conectado y configurado para acceso LAN local, *no puede imprimir ni navegar por el nombre* en la LAN local. Sin embargo, puede examinar o imprimir por dirección IP. Consulte la sección <u>Solución de problemas</u> de este documento para obtener más información y soluciones para esta situación.

Configuración del acceso LAN local para clientes VPN o AnyConnect Secure Mobility Client

Complete estas tareas para permitir que los clientes de Cisco VPN o Cisco AnyConnect Secure Mobility Client accedan a su LAN local mientras están conectados al ASA:

- Configure el ASA a través del ASDM o Configure el ASA a través de la CLI
- <u>Configuración de Cisco AnyConnect Secure Mobility Client</u>

Configure el ASA a través del ASDM

Complete estos pasos en el ASDM para permitir que los clientes VPN tengan acceso LAN local mientras están conectados al ASA:

1. Elija Configuration > Remote Access VPN > Network (Client) Access > Group Policy y seleccione la política de grupo en la que desea habilitar el acceso LAN local. A continuación, haga clic en Editar.

File View Tools Witzerds Window Help					
Hone Configuration 🕞 Monitoring 🔓	🖥 Save 🔕 Refresh 🔿 Back 🕥 Forward 🦻	Help			
Device List a P ×	Configuration > Remote Access VPN > Network	(Client) Access > Group Policies			
	Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADOLG/LDAP server To enforce authorization attributes from an IDAP server you must use an IDAP attribute rise.				
	Name	Туре	Tunneling Protocol		
	Dft:GrpPolicy (System Default) Histology opt	Internal	ikev1;ikev2;isi+clentiess;i2tp-ipsec ikev1		
Remoto Access VPN © Q Prinduction Pathwork (Clent) Access Pathwork (Clent) Access Pathwork (Clent) Access Pathwork Clent Software Path Connect Clent Software Pathwork (Clent) S					

2. Vaya a Avanzado > Tunelización dividida.

General Servers Servers Solit Turneling Browser Proxy Browser Prox Browser Prox Brows	The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing DNS Names: Inherit Policy: Inherit Network List: Inherit
	Pressing this button to set up split exlusion for Web Security proxies. Set up Split Exclusion for Web Security Intercept DHCP Configuration Message from Microsoft Clients

3. Desmarque la casilla Heredar para Política y elija Excluir lista de red a continuación.

General Servers	The VPN client makes split tunneling decisions on the basis of a network list that can be specified l	volec
Solt Tuppeling	DNS Names: V Inherit	
Browser Proxy	Policy: Inherit Exclude Network List Below	
	Network List: 📝 Inherit	al di ji
	Pressing this button to set up split exlusion for Web Security proxies.	
	Intercent DHCP Configuration Message from Microsoft Clients	

4. Desmarque la casilla **Heredar** para la lista de red y, a continuación, haga clic en **Administrar** para iniciar el administrador de la lista de control de acceso (ACL).



5. Dentro del Administrador de ACL, elija Add > Add ACL... para crear una nueva lista de acceso.

Standard	ACL Extended ACL		
🛧 Add	🕶 🛒 Edit 📋 Delete 🕈 🗲	🄉 🐂 🛍	*
No	Address	Action	Description

6. Asigne un nombre al ACL y haga clic en OK.

ACL Name: Local	Lan_Access	
ОК	Cancel	Help

7. Una vez que se crea la ACL, elija Add > Add ACE... para agregar una entrada de control de acceso (ACE).



8. Defina la ACE que corresponde a la LAN local del cliente.

Elija **Permit**.Elija una dirección IP de **0.0.0.0**Elija una máscara de red de */***32**.(*Opcional*) Proporcione una descripción.Click OK.

	Address	Action	Description	
.ocal_Lar I	_Access	🖌 🎺 Permit		
	🔁 Edit	ACE		
	Action:	💿 Permit 📀) Deny	
	Addres	s: 0.0.0.0/32		
	Descrip	tion:		

9. Haga clic en OK para salir del Administrador de ACL.

ACCINICIA					
itandard AC	Extended ACL				
🗣 Add 🗕 (🛃 Edit 👔 Delete 🕈	4 👗 🖻 🏙 -			
Notation	Address	Action	Description	anna an tha an	
Local_Lar	_Access				
1	🖳 0.0.0.0	🥜 Permit			
			OK Cencel	Help	

10. Asegúrese de que la ACL que acaba de crear esté seleccionada para la Lista de Red de Túnel Dividido.

-Advanced Split Tunneling Browser Proxy	DN5 Names: 🔽 Inherit	
	Policy: Inherit Exclude Network List Below	
⊕-AnyConnect Client ⊞-IPsec(IKE∨1) Client	Network List: Inherit Local_Lan_Access	
	Pressing this button to set up split exlusion for Web Security proxies. Set up Split Exclusion for Web Security Intercept DHCP Configuration Message from Microsoft Clients	

11. Haga clic en OK para volver a la configuración de la Política de Grupo.

The VPN client makes split	cunneling decisions on the basis of a network list that can be specified below by providing the proper parameter				
DNS Names: 👿 Inherit					
Policy: 📄 Inherit	Exclude Network List Below Local_Lan_Access				
Network List: 📄 Inherit					
Pressing this button to set	up split exlusion for Web Security proxies.				
Set up Split Exclusion fo	r Web Security				
Intercent DHCP Confi	uration Message from Microsoft Clients				
Intercept Drier Com					
Ne	xt 🙆 Previous				
	OK Cancel Help				

12. Haga clic en **Aplicar** y luego **Enviar** (si es necesario) para enviar los comandos al ASA.

add - mit cate 🗢 patents 1993 aurism		
• Hod • 🔄 Eat 🚺 Delete 🞇 Assign		
lame	Туре	Tunneing Protocol
fltGrpPolicy (System Default)	Internal	kev1;kev2;ssi-clentiess;l2tp-lpsec
ihaleyopo	Internal	dev1
find: 🛛 🖓 🎦 Match Cas	•	

Configure el ASA a través de la CLI

En lugar de utilizar el ASDM, puede completar estos pasos en la CLI de ASA para permitir que los clientes VPN tengan acceso LAN local mientras están conectados al ASA:

1. Ingrese al modo de configuración.

```
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#
```

2. Cree la lista de acceso para permitir el acceso LAN local.

```
ciscoasa(config)#access-list Local_LAN_Access remark Client Local LAN Access
ciscoasa(config)#access-list Local_LAN_Access standard permit host 0.0.0.0
```

Precaución: Debido a los cambios en la sintaxis de ACL entre las versiones 8.x a 9.x del software ASA, esta ACL ya no está permitida y los administradores verán este mensaje de

error cuando intenten configurarla:

```
rtpvpnoutbound6(config)# access-list test standard permit host
0.0.0.0
ERROR: dirección IP no válida
```

Lo único permitido es:

rtpvpnoutbound6(config)# access-list test standard permit any4

Este es un problema conocido y ha sido abordado por el ID de bug de Cisco <u>CSCut3131</u>. Actualice a una versión con la corrección de este error para poder configurar el acceso LAN local.

3. Ingrese el modo de configuración de directiva de grupo para la política que desea modificar.

ciscoasa(config)#group-policy hillvalleyvpn attributes
ciscoasa(config-group-policy)#

4. Especifique la política de túnel dividido. En este caso, se excluye la política.

ciscoasa(config-group-policy)#split-tunnel-policy excludespecified

5. Especifique la lista de acceso al túnel dividido. En este caso, la lista es Local_LAN_Access.

ciscoasa(config-group-policy)#split-tunnel-network-list value Local_LAN_Access

6. Ejecutar este comando:

ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes

7. Asocie la política del grupo al grupo de túnel

ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn

8. Salga de los dos modos de configuración.

```
ciscoasa(config-group-policy)#exit
ciscoasa(config)#exit
ciscoasa#
```

9. Guarde la configuración en la memoria RAM no volátil (NVRAM) y presione **Enter** cuando se le pida que especifique el nombre del archivo de origen.

ciscoasa#copy running-config startup-config

Source filename [running-config]? Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

Configuración de Cisco AnyConnect Secure Mobility Client

Para configurar Cisco AnyConnect Secure Mobility Client, refiérase a la sección <u>Establecimiento</u> <u>de la Conexión SSL VPN con SVC</u> de ASA 8.x : Permita la Tunelización Dividida para AnyConnect VPN Client en el Ejemplo de Configuración de ASA.

La tunelización dividida-excluida requiere que habilite **AllowLocalLanAccess** en AnyConnect Client. Toda la tunelización dividida excluida se considera acceso LAN local. Para utilizar la función de exclusión de la tunelización dividida, debe habilitar la preferencia **AllowLocalLan Access** en las **preferencias de AnyConnect VPN Client**. De forma predeterminada, el acceso LAN local está desactivado.

Para permitir el acceso LAN local y, por lo tanto, la tunelización dividida-excluida, un administrador de red puede habilitarlo en el perfil o los usuarios pueden habilitarlo en sus preferencias de configuración (consulte la imagen en la siguiente sección). Para permitir el acceso LAN local, un usuario selecciona la casilla de verificación **Permitir acceso LAN local** si la tunelización dividida está habilitada en el gateway seguro y se configura con la política **de exclusión de política de túnel dividido**. Además, puede configurar el perfil de cliente VPN si se permite el acceso LAN local con **<LocalLanAccess** UserControablaba="true">true

Preferencias de usuario

Estas son las selecciones que debe realizar en la ficha Preferencias de Cisco AnyConnect Secure Mobility Client para permitir el acceso local a LAN. S Cisco AnyConnect Secure Mobility Client

cisco	AnyC	Connect	Seci	ure Mobili	ity Client	(
Virtual P	rivate Ne	twork (VPN	I)			Diagnostics
Preferences	Statistics	Route Details	Firewall	Message History		
Start VPN before user logon to computer						
🔽 Enable	e automatic c	ertificate selecti	on			
🔽 Use Sa	afeWord Sof	Foken PIN to gel	: passwor(Ь		
Start 🛛	Start VPN when AnyConnect is started					
🔽 Minimi	Minimize AnyConnect on VPN connect					
🔽 Allow I	Allow local (LAN) access when using VPN (if configured)					
🔽 Do no	On not remember SmartCard PIN					
🔄 Enable	Enable automatic VPN server selection					
Block (Block connections to untrusted servers					
			Constant States		and the line was seen and	

23

-

Ejemplo de perfil XML

Este es un ejemplo de cómo configurar el perfil de cliente VPN con XML.

<?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> <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon> <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection> <ShowPreConnectMessage>false</ShowPreConnectMessage> <CertificateStore>All</CertificateStore> <CertificateStoreOverride>false</CertificateStoreOverride> <ProxySettings>Native</ProxySettings> <AllowLocalProxyConnections>true</AllowLocalProxyConnections> <AuthenticationTimeout>12</AuthenticationTimeout> <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart> <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect> <LocalLanAccess UserControllable="true">true</LocalLanAccess> <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin> <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>

```
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>
```

Verificación

Complete los pasos de estas secciones para verificar su configuración.

- Ver el DART
- Probar el acceso LAN local con Ping

Conecte Cisco AnyConnect Secure Mobility Client al ASA para verificar su configuración.

1. Elija la entrada de conexión de la lista de servidores y haga clic en Conectar.

🕥 Cisco AnyCo	nnect Secure Mobility Client	
	VPN: Ready to connect. 172.22.1.160 ▼	Connect
\$ ()		nd talk cisco

2. Elija Ventana Avanzada para Todos los Componentes > Estadísticas... para mostrar el modo de túnel.



Statistics	Route Details	Firewall Message Hist	ory
Connection Information		Address Information	
State:	Connected	Client (IPv4):	192.168.11.
Tunnel Mode (IPv4):	Split Exclude	Client (IPv6):	Not Available
Tunnel Mode (IPv6):	Drop All Traffic	Server:	64.102.156.82
Duration:	00:01:11	Transport Information	
Bytes		Protocol:	DTL
Sent:	49749	Cipher:	RSA_3DES_168_SHA
Received:	9298	Compression:	LZ
Frames		Proxy Address:	No Prox
Sent:	710	Feature Configuration	
Received:	3	FIPS Mode:	Disable
Control Frames		Trusted Network Detection	: Disable
Sent:	7	Always On:	Disable
Received:	5	Secure Mobility Solution	
Client Management		Status:	Unconfirme
Profile Name:	pro_locallan.xml	Appliance:	Not Availabl
Administrative Domain:	Undefined		

3. Haga clic en la pestaña **Detalles de ruta** para ver las rutas a las que Cisco AnyConnect Secure Mobility Client todavía tiene acceso local.

En este ejemplo, se permite al cliente acceso LAN local a 10.150.52.0/22 y 169.254.0.0/16 mientras que el resto del tráfico se cifra y se envía a través del túnel.

Sta	tistics Route D	etails Firewal	I Message H	listory
Route Details				
▼Non-Secured R	outes (IPv4)	nde Baser		
10.150.52.0	/22			
169.254.0.0	/16			
* Secured Routes	(IPV4)			
Non-Secured R	outes (IBv6)			
Secured Routes	(IPv6)	·····		
Secured Routes	(

Cisco AnyConnect Secure Mobility Client

Al examinar los registros de AnyConnect desde el paquete Diagnostics and Reporting Tool (DART), puede determinar si se ha establecido o no el parámetro que permite el acceso local a la LAN.

LocalLanAccess: true AutoReconnect: true AutoReconnectBehavior: DisconnectOnSuspend UseStartBeforeLogon: false AutoUpdate: true RSASecurIDIntegration: Automatic WindowsLogonEnforcement: SingleLocalLogon WindowsVPNEstablishment: LocalUsersOnly ProxySettings: Native AllowLocalProxyConnections: true PPPExclusion: Disable PPPExclusionServerIP: AutomaticVPNPolicy: false TrustedNetworkPolicy: Disconnect UntrustedNetworkPolicy: Connect TrustedDNSDomains: TrustedDNSServers: AlwaysOn: false ConnectFailurePolicy: Closed AllowCaptivePortalRemediation: false CaptivePortalRemediationTimeout: 5 ApplyLastVPNLocalResourceRules: false AllowVPNDisconnect: true EnableScripting: false TerminateScriptOnNextEvent: false EnablePostSBLOnConnectScript: true AutomaticCertSelection: true RetainVpnOnLogoff: false UserEnforcement: SameUserOnly EnableAutomaticServerSelection: false AutoServerSelectionImprovement: 20 AutoServerSelectionSuspendTime: 4 AuthenticationTimeout: 12 SafeWordSofTokenIntegration: false AllowIPsecOverSSL: false ClearSmartcardPin: true

Probar el acceso LAN local con Ping

Una manera adicional de probar que VPN Client todavía tiene acceso LAN local mientras se tuneliza al centro distribuidor VPN es utilizar el comando **ping** en la línea de comandos de Microsoft Windows. Aquí hay un ejemplo donde la LAN local del cliente es 192.168.0.0/24 y otro host está presente en la red con una dirección IP de 192.168.0.3.

C:\>ping 192.168.0.3 Pinging 192.168.0.3 with 32 bytes of data: Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 Ping statistics for 192.168.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

No se puede imprimir ni examinar por nombre

Cuando el VPN Client está conectado y configurado para el acceso LAN local, *no puede imprimir ni navegar por el nombre* en la LAN local. Hay dos opciones disponibles para solucionar esta situación:

• Busque o imprima por dirección IP.

Para navegar, en lugar de la sintaxis **\\sharename**, utilice la sintaxis **\\x.x.x.x** donde *x.x.x.x* es la dirección IP del equipo host.

Para imprimir, cambie las propiedades de la impresora de red para utilizar una dirección IP en lugar de un nombre. Por ejemplo, en lugar de la sintaxis **\\sharename\printername**, utilice **\\x.x.x.\printername**, donde *x.x.x.x* es una dirección IP.

 Cree o modifique el archivo VPN Client LMHOSTS. Un archivo LMHOSTS en un equipo Microsoft Windows permite crear asignaciones estáticas entre nombres de host y direcciones IP. Por ejemplo, un archivo LMHOSTS podría tener el siguiente aspecto:

192.168.0.3 SERVER1 192.168.0.4 SERVER2 192.168.0.5 SERVER3

En Microsoft Windows XP Professional Edition, el archivo LMHOSTS se encuentra en **%SystemRoot%\System32\Drivers\Etc**. Refiérase a su documentación de Microsoft o al artículo <u>314108 de</u> Microsoft para obtener más información.

Información Relacionada

- Ejemplo de Configuración de PIX/ASA 7.x como Servidor VPN Remoto Usando ASDM
- Ejemplo de Configuración de SSL VPN Client (SVC) en IOS con SDM
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- Soporte Técnico y Documentación Cisco Systems