Configurando un túnel IPsec - Concentrador del Cisco VPN 5000 al Firewall del punto de verificación 4.1

Contenido

Introducción

Este documento demuestra cómo formar un túnel IPsec con las claves previamente compartidas para unirse a dos redes privadas. Se une a una red privada dentro del concentrador del Cisco VPN 5000 (192.168.1.x) a una red privada dentro del Firewall del punto de verificación 4.1 (10.32.50.x). Se asume que fluye el tráfico por dentro del concentrador VPN y del interior el punto de verificación a Internet (representado en este documento por las redes 172.18.124.x) antes de que usted comience esta configuración.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Concentrador Cisco VPN 5000
- Versión concentrador software 5.2.19.0001 del Cisco VPN 5000
- Escudo de protección de punto de control 4.1

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

Este documento utiliza esta configuración.

Concentrador Cisco VPN 5000

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
```

```
Peer                        = "10.32.50.0/24"
BindTo                      = "ethernet 1:0"
SharedKey                   = "ciscorules"
KeyManage                   = Auto
Transform                   = esp(sha,des)
Partner                     = 172.18.124.157
Mode                        = Main

[ IP VPN 1 ]
Numbered                    = Off
Mode                        = Routed

[ IP Ethernet 1:0 ]
IPAddress                   = 172.18.124.35
SubnetMask                  = 255.255.255.240
Mode                        = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Escudo de protección de punto de control 4.1

Complete estos pasos para configurar el Firewall del punto de verificación 4.1.

1. Propiedades Select **> cifrado** para fijar las vidas útiles de IPSec del punto de verificación para estar de acuerdo con el **KeyLifeSecs =** comando vpn concentrator **28800**.**Note**: Deje los cursos de la vida del Internet Key Exchange (IKE) del punto de verificación en el valor por defecto.
2. Seleccione Manage (Administración) > Network Objects (Objetos de red) > New (o Edit) Nuevo (o Editar) > Network (Red) para configurar el objeto para la red interna ("cpinside") detrás del punto de control. Esto debe estar de acuerdo con el **par del =** comando vpn concentrator **"10.32.50.0/24"**.
3. Seleccione **Manage > Network Objects > Edit** para editar el objeto para el punto final del gateway (punto de verificación “RTPCPVPN”) ese las puntas del concentrador VPN en al **comando Partner = <ip>**.Seleccione la ubicación inferior **interna**.Seleccione el **gateway** para el tipo.Marque el **VPN-1 y FireWall-1** y **estación de administración** bajo los módulos instalados.
4. Seleccione **Manage > Network Objects > nuevo (o edite) > red** para configurar el objeto para (“inside_cisco”) la red externa detrás del concentrador VPN.Esto debe estar de acuerdo con el **LocalAccess = el** comando vpn concentrator **<192.168.1.0/24>**.
5. Seleccione **Manage > Network Objects > New > Workstation** para agregar un objeto para (“cisco_endpoint”) el gateway externo del concentrador VPN.Ésta es la interfaz del “exterior” del concentrador VPN con la Conectividad al punto de verificación (en este documento, 172.18.124.35 es la dirección IP en el **comando IPAddress = <ip>**).Seleccione el **externo** bajo ubicación. Seleccione el **gateway** para el tipo.**Note**: No marque VPN-1/FireWall-1.
6. Seleccione Manage (Administración) > Network objects (Objetos de red) > Edit (Editar) para editar la ficha VPN del punto final del punto de control Gateway (denominado"RTPCPVPN"). En Domain (Dominio), seleccione Other (Otro) y luego, seleccione el interior de la red de Punto de control (denominado "cpinside") en la lista desplegable. Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit (Editar).
7. Cambie las propiedades IKE a la **encripción de DES** y al picado **SHA1** para estar de acuerdo

con **SHA_DES_G2 el** comando vpn concentrator.**Note**: El "G2" refiere al grupo Diffie-Hellman 1 o 2. En la prueba, fue descubierto que el punto de verificación valida el "G2" o el "G1."Cambie estas configuraciones:Cancelar la selección del modo agresivoEl control **soporta las subredes**.**Secreto previamente compartido del** control bajo método de autentificación.

8. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con el **SharedKey = <key>** comando vpn concentrator.
9. Seleccione Manage (Administración) > Network Objects (Objetos de red) > Edit (Editar) para editar la ficha VPN de "cisco_endpoint". Bajo dominio, seleccione **otro**, y después seleccione el interior de la red del concentrador VPN (llamada “inside_cisco”). Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit (Editar).
10. Cambie las propiedades IKE a la **encripción de DES** y al picado **SHA1** para estar de acuerdo con **SHA_DES_G2 el** comando vpn concentrator.**Note**: El "G2" refiere al grupo Diffie-Hellman 1 o 2. En la prueba, fue encontrado que el punto de verificación valida el "G2" o el "G1."Cambie estas configuraciones:Cancelar la selección del modo agresivoEl control **soporta las subredes**.**Secreto previamente compartido del** control bajo método de autentificación.
11. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con el **SharedKey = <key>** comando vpn concentrator.
12. En la ventana del editor de políticas, ingrese una ventana tanto con el origen como con el destino, como en "inside_cisco" y "cpinside" (bidireccional). Set Service=Any, Action=Encrypt, y Track=Long.
13. Bajo título de la acción, haga clic el verde **cifran el** icono y lo seleccionan **Edit Properties** para configurar las políticas de encripción.
14. Seleccione el **IKE**, y el tecleo **edita**.
15. En la ventana de las propiedades IKE, cambie estas propiedades para estar de acuerdo con la **transformación = especialmente (sha, DES)** comando vpn concentrator.En Transform (Transformar), seleccione Encryption (Encriptación) + Data Integrity (ESP) (Integridad de datos (ESP)). El algoritmo de encripción debe ser **DES**, integridad de los datos debe ser **SHA1**, y el gateway de peer permitido debe ser el gateway externo del concentrador VPN (llamado “cisco_endpoint”). Click OK.
16. Después de que usted configure el punto de verificación, la **directiva** selecta **> instala** en el menú de punto de control para hacer que los cambios tomen el efecto.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Comandos de resolución de problemas del concentrador de la VPN 5000

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- vpn trace dump all - Muestra información acerca de todas las conexiones de VPN concordantes, incluida la información acerca de la hora, el número VPN, la dirección IP real del par, las secuencias de comandos que se ejecutaron y, en caso de algún error, la rutina y el número de línea del código de software en el que se produjo el error.
- **show system log buffer** — Muestra el contenido del búfer del registro interno.
- **show vpn statistics** — Muestra esta información para los usuarios, los Partners, y el total para ambos. (Para los modelos modulares, la visualización incluye una sección para cada slot del módulo. Refiera a la sección del ejemplo de salida del debug.)Activas actualmente: Las conexiones que están activas actualmente.In Negot – Las conexiones que están siendo negociadas actualmente.Agua alta - Cantidad máxima de conexiones activas al mismo tiempo desde el último reinicio.Total en ejecución - Cantidad total de conexiones correctas desde el último reinicio.Túneles correctos – Cantidad de túneles que no presentan errores.Comienzo del túnel - El número de túneles comienza.Error de túnel – El número de túneles con errores.
- show vpn statistics verbose – Muestra las estadísticas de negociación ISAKMP y muchas otras estadísticas de conexión activa.

Resumen de la red

Cuando las redes internas adyacentes del múltiplo se configuran en el dominio del cifrado en el punto de verificación, el dispositivo pudo resumirlas automáticamente con respecto al tráfico interesante. Si el concentrador VPN no se configura para hacer juego, el túnel es probable fallar. Por ejemplo, si las redes internas de 10.0.0.0 /24 y de 10.0.1.0 /24 se configuran para ser incluidas en el túnel, puede ser que sean resumidas a 10.0.0.0 /23.

Depuración del Checkpoint 4.1 Firewall

Esto era una instalación del Microsoft Windows NT. Porque el seguimiento fue fijado para `de largo` adentro la ventana de editor de políticas (como se ve en el paso 12), el tráfico denegado debe aparecer en el rojo en el Log Viewer. Un debug más prolijo se puede obtener por:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

y en otra ventana.

```
C:\WINNT\FW1\4.1\fwstart
```

Publique estos comandos de borrar las asociaciones de seguridad (SA) en el punto de verificación:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

¿La respuesta en `es` **sí** `usted seguro?` mensaje

Ejemplo de resultado del comando debug

```
cisco_endpoint#vpn trac dump all
```

```
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
```

```
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped               13
Unwrapped              9
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP                  9
rx IPX                 0
rx Other               0
tx IP                 13
tx IPX                 0
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:
```

```
          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
```

```
New conn limited        0
```

Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems