Configuration d'IPSec entre un serveur Microsoft Windows 2000 et un périphérique Cisco

Contenu

Introduction Avant de commencer **Conventions** Conditions préalables **Components Used** Diagramme du réseau Configuration du serveur Microsoft Windows 2000 pour qu'il fonctionne avec les périphériques Cisco Tâches effectuées Step-by-Step Instructions Configuration des périphériques Cisco Configuration du routeur Cisco 3640 Configuration de PIX Configuration du concentrateur VPN 3000 Configuration du concentrateur VPN 5000 Vérification Dépannage Dépannage des commandes Informations connexes

Introduction

Ce document explique comment créer un tunnel IPSec avec des clés prépartagées afin de joindre deux réseaux privés : un réseau privé (192.168.I.X) au sein d'un périphérique Cisco et un réseau privé (10.32.50.X) au sein d'un serveur Microsoft 2000. Nous supposons que le trafic allant du périphérique Cisco et du serveur 2000 vers Internet (représenté ici par les réseaux 172.18.124.X) circule déjà avant le début de la configuration.

Vous trouverez des informations détaillées sur la configuration du serveur Microsoft Windows 2000 sur le site Web de Microsoft : <u>http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP</u>

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions

utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ces configurations ont été développées et testées à l'aide des versions logicielles et matérielles ci-dessous.

- Microsoft Windows 2000 Server 5.00.2195
- Routeur Cisco 3640 avec logiciel Cisco IOS® version c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall avec logiciel PIX version 5.2.1
- Concentrateur Cisco VPN 3000 avec concentrateur VPN 3000 Version 2.5.2.F
- Concentrateur VPN Cisco 5000 avec concentrateur VPN 5000 Version 5.2.19

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configuration du serveur Microsoft Windows 2000 pour qu'il fonctionne avec les périphériques Cisco

Tâches effectuées

Ce diagramme montre les tâches effectuées dans la configuration du serveur Microsoft Windows 2000 :



Step-by-Step Instructions

Une fois que vous avez suivi les <u>instructions</u> de configuration sur le site Web de Microsoft, procédez comme suit pour vérifier que votre configuration peut fonctionner avec les périphériques Cisco. Les commentaires et les modifications sont notés avec les captures d'écran.

 Cliquez sur Démarrer > Exécuter > secpol.msc sur Microsoft Windows 2000 Server, puis vérifiez les informations sur les écrans suivants.Une fois que les instructions du site Web de Microsoft ont été utilisées pour configurer un serveur 2000, les informations de tunnel suivantes ont été affichées.Remarque : la règle d'exemple est appelée « to_cisco

📑 Local Security Settings				- - ×
Action ⊻iew ← →	· 🗈 📧 🗙 🗗 🗔	🔮] 🛍 🏦 🗍 🖺 🚨		
Tree	Name 🛆	Description	Policy Assigned	
Security Settings	Client (Respond Only) Secure Server (Requir Server (Request Secu	Communicate normally (uns For all IP traffic, always req For all IP traffic, always req	Policy Assigned No No Yes	

2. Cette règle d'exemple contient deux filtres : Microsoft-Cisco et Cisco-

to_cis	sco Properties		Ľ
Rule	es General		
ĺ	Security rules	for communicating with ot	her computers
ĪP	Security Rules:		
	P Filter List	Filter Action	Authentication Tu
6	Z Microsoft-Cisco	Permit	Preshared Key 17
	Z Cisco-Microsoft	Permit	Preshared Key 17
	Oynamic>	Default Response	Preshared Key No
	A <u>d</u> d <u>E</u> di	t <u>R</u> emove	Use Add <u>W</u> izard
		Close	Cancel <u>A</u> pply

3. Sélectionnez la règle de sécurité IP Cisco-Microsoft, puis cliquez sur **Modifier** pour afficher/ajouter/modifier les listes de filtres

Edit Rule Properties	? ×
Authentication Methods Tu IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter lis secured with this rule.	st specifies which network traffic will be
IP Filter Lists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
O Cisco-Microsoft	
O Microsoft-Cisco	
I	
Add Edit	Remove
0	K Cancel Apply

 IP.
 IP.

 4. L'onglet Général > Avancé de la règle a la durée de vie IKE (480 minutes = 28800 secondes)

to_cisco Properties ?X
Rules General
Key Exchange Settings ? 🗙
Master key Perfect Forward Secrecy
Authenticate and generate a new key after every:
480 minutes
Authenticate and generate a new key after every:
0 session(s)
Protect identities with these security methods:
Methods
Internet Key Eyehange (IKE) for) (indexe 2000
Jointly developed by Microsoft and Cisco Systems, Inc.
Advanced
OK Cancel Apply

5. L'onglet Général > Avancé > Méthodes de la règle comporte la méthode de chiffrement IKE (DES), le hachage IKE (SHA1) et le groupe Diffie-Helman (Low(1)



6. Chaque filtre comporte 5 onglets :**Méthodes d'authentification** (clés prépartagées pour l'échange de clés Internet [IKE])

IP Filter List Filter Action Authentication Methods Tunnel Setting Connection Type Image: Second	IP Filter List Filter Action Authentication Methods Tunnel Setting Connection Type Image: Second	t Rule Properties		? ×
Image: Second system The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer. Authentication Method preference order: Add Method Details Add Preshared Key ciscol 23 Edit Move up Image: Security up the security up the security with another computer. Image: Security up the secure security up the security up the security up the secur	Image: Second system The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer. Authentication Method preference order: Add Method Details Add Preshared Key Cisco123 Edit Move up Move down	IP Filter List Authentication Methods	Tunnel Setting	Filter Action
Authentication Method preference order: Method Details Add Preshared Key cisco123 Edit Remove Move up	Authentication Method preference order: Add Method Details Add Preshared Key cisco123 Edit Remove Move up Move down	The authenticat between the cor authentication m another compute	ion method specifies ho mputers. Offer and acce nethods when negotiatir er.	ow trust is established ept these ng security with
Method Details Add Preshared Key cisco123 Edit Remove Move up	Method Details Add Preshared Key cisco123 Edit Remove Move up Move down Move down	Authentication Method prefere	ence order:	
Preshared Key cisco123 Edit Remove Move up	Preshared Key cisco123 Edit Remove Move up Move down	Method	Details	Add
	Move down	Preshared Key	cisco123	Edit Remove Move up
			OK Ca	ncel Apply

connexion (LAN)

dit Rule Prope	rties			? ×
IP	Filter List	1	Filter Action	1
Authenticatio	n Methods	Tunnel Setting	Connect	tion Type
	This rule only appl he selected type.	ies to network traff	ic over connec	tions of
C All network	connections			
 Local area 	network (LAN)			
O Remote ad	cess			
		OK	Cancel	Apply

(IPSec)

Rule Properties	? ×
Authentication Methods Tun IP Filter List	nnel Setting Connection Type Filter Action
The selected filter action for secure network traffic	n specifies whether this rule negotiates c, and how it will secure the traffic.
Filter Actions:	Description
Name IPSec tunnel	Description
O Permit O Request Security (Optional) O Require Security	Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat
Add Edit	Remove 🔲 Use Add Wizard
OK	Cancel Apply

Action de filtre > tunnel IPSec > Modifier > Modifier, puis cliquez sur Personnalisé

Modify Security Method	
Security Method	
 High (ESP) Data will be encrypted, authentic and unmodified Medium (AH) 	
Data will be authentic and unmodified, but will not be encrypted	
Custom (for expert users) Settings	
OK Cancel Apply	

Paramètres - IPSec transforme et durée de vie IPSec

Custom Security Method Settings	? ×	
Specify the settings for this custom sec	urity method.	
Data and address integrity without a Integrity algorithm:	encryption (AH) :	
MD5 💌		
Data integrity and encryption (ESP) Integrity algorithm:	:	
Encryption algorithm:		
Session Key Settings:		
Generate a new key every:	🔽 Generate a new key every	
100000 Kbytes	3600 seconds	
	OK Cancel	

les réseaux source et de destination doivent être chiffrés :Pour Cisco-Microsoft

🖥 IP Filter I	List						?
₽	An IP filter list is compo addresses and protoco	used of multiple filte Is can be combine	rs. In this way multiple sub d into one IP filter.	nets, IP			
Name:							
Cisco-Micr	rosoft						
Description	r.						Add
			*				Edit
			*				Remove
Filters:			_			V	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address	Source Ma
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>192.168.1.0</td><td>255.255.25</td>	192.168.1.0	255.255.25
•							Þ
						OK	Cancel

Pour Microsoft-Cisco

:

.

IP Filter l	.ist					?)
	An IP filter list is com addresses and proto	posed of multiple filte cols can be combine	rs. In this way multiple sub d into one IP filter.	nets, IP		
Name:						
Microsoft-0	Lisco					
, Description	κ					Add
			A			Edit
						Remove
Filters:			_		T	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>10.32.50.0</td>	10.32.50.0
-						
-1					OK	Cancel

Paramètre du tunnel - homologues de chiffrement :Pour Cisco-Microsoft

Ed	t Rule Properties		?	×
3	IP Filter List	1	Filter Action	
	Authentication Methods	Tunnel Setting	Connection Type	į.
	The tunnel end IP traffic destin List. It takes tw	fpoint is the tunneling c ation, as specified by t o rules to describe an	computer closest to the he associated IP Filter IPSec Tunnel.	
	C This rule does not specif	v an IPSec tunnel.		-
	The tunnel endpoint is s	pecified by this IP Addr	ess:	
	172.18.124	. 157		
	,			
			Cancel Acadia	
			Apply Apply	

Edit Ru	e Properties		? ×
Aul	IP Filter List hentication Methods	 Tunnel Setting	Filter Action
	→ The tunnel endp → IP traffic destina List. It takes two	point is the tunneling co ation, as specified by th prules to describe an If	omputer closest to the le associated IP Filter PSec Tunnel.
 This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 			
	172.18.124.	35	
		ОК С	ancel Apply

Configuration des périphériques Cisco

Configurez le routeur Cisco, les concentrateurs PIX et VPN, comme indiqué dans les exemples cidessous.

- Routeur Cisco 3640
- <u>PIX</u>
- <u>Concentrateur VPN 3000</u>
- <u>Concentrateur VPN 5000</u>

Configuration du routeur Cisco 3640

Routeur Cisco 3640

```
Current configuration : 1840 bytes !
```

```
version 12.1
no service single-slot-reload-enable
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname moss
1
logging rate-limit console 10 except errors
1
ip subnet-zero
no ip finger
ip audit notify log
ip audit po max-events 100
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
!
call rsvp-sync
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
1
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
```

```
!
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

Configuration de PIX

PIX			
PIX Version 5.2(1)			
nameif ethernet0 outside securitv0			
nameif ethernet1 inside security100			
enable password 8Ry2YjIyt7RRXU24 encrypted			
passwd 2KFQnbNIdI.2KYOU encrypted			
hostname pixfirewall			
fixup protocol ftp 21			
fixup protocol http 80			
fixup protocol h323 1720			
fixup protocol rsh 514			
fixup protocol smtp 25			
fixup protocol sqlnet 1521			
fixup protocol sip 5060			
names			
<pre>! Source/Destination networks defined access-list 115</pre>			
permit ip 192.168.1.0 255.255.255.0 10.32.50.0			
255.255.255.0			
access-list 115 deny ip 192.168.1.0 255.255.255.0 any			
pager lines 24			
logging on			
no logging timestamp			
no logging standby			
no logging console			
no logging monitor			
no logging buffered			
no logging trap			
no logging history			
logging facility 20			
logging queue 512			
interface ethernet0 auto			
interface ethernet1 10baset			
mtu outside 1500			
mtu inside 1500			
1p address outside 172.18.124.35 255.255.255.240			
1p address inside 192.168.1.1 255.255.255.0			
ip audit into action alarm			
ip audit attack action alarm			
foilever timeout 0.00.00			
failever timeout 0:00:00			
failover poir is			
failover in address inside 0.0.0.0			
arn timeout 1//00			
L Except Source/Destination from Network Address			
Translation (NAT), nat (inside) 0 access-list 115			
route outside 0 0 0 0 0 0 0 172 18 124 36 1			
timeout xlate 3:00:00			
timeout conn 1.00.00 half-closed 0.10.00 udn 0.02.00 rpc			

0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable sysopt connection permit-ipsec no sysopt route dnat !--- IPSec transforms crypto ipsec transform-set myset esp-des esp-md5-hmac !--- IPSec lifetime crypto ipsec security-association lifetime seconds 3600 crypto map rtpmap 10 ipsec-isakmp !--- Source/Destination networks crypto map rtpmap 10 match address 115 !--- Encryption peer crypto map rtpmap 10 set peer 172.18.124.157 crypto map rtpmap 10 set transform-set myset crypto map rtpmap interface outside isakmp enable outside !--- Encryption peer isakmp key ******* address 172.18.124.157 netmask 255.255.255.240 isakmp identity address !--- Authentication method isakmp policy 10 authentication pre-share !--- IKE encryption method isakmp policy 10 encryption des !--- IKE hashing isakmp policy 10 hash sha !--- Diffie-Hellman group isakmp policy 10 group 1 !--- IKE lifetime isakmp policy 10 lifetime 28800 telnet timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08 : end

Configuration du concentrateur VPN 3000

Utilisez les options de menu et les paramètres indiqués ci-dessous pour configurer le concentrateur VPN si nécessaire.

 Pour ajouter une proposition IKE, sélectionnez Configuration > Système > Protocoles de tunnellisation > IPSec > Propositions IKE > Ajouter une proposition.

```
Proposal Name = DES-SHA

!--- Authentication method Authentication Mode = Preshared Keys !--- IKE hashing

Authentication Algorithm = SHA/HMAC-160 !--- IKE encryption method Encryption Algorithm =

DES-56 !--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime

Measurement = Time Date Lifetime = 10000 !--- IKE lifetime Time Lifetime = 28800
```

 Pour définir le tunnel LAN à LAN, sélectionnez Configuration > System > Tunneling Protocols > IPSec LAN à LAN.

```
Name = to_2000
Interface = Ethernet 2 (Public) 172.18.124.35/28
!--- Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none
(Use Pre-shared Keys) Pre-shared key = cisco123 !--- IPSec transforms Authentication =
ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA
Autodiscovery = off !--- Source network defined Local Network Network List = Use IP
```

Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below IP Address 10.32.50.0 Wildcard Mask 0.0.0.255

 Pour modifier l'association de sécurité, sélectionnez Configuration > Policy Management > Traffic Management > Security Associations > Modify.

```
SA Name = L2L-to_2000
Inheritance = From Rule
IPSec Parameters
!--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm =
DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime
= 10000 !--- IPSec lifetime Time Lifetime = 3600 Ike Parameters !--- Encryption peer IKE
Peer = 172.18.124.157 Negotiation Mode = Main !--- Authentication method Digital Certificate
= None (Use Preshared Keys) !--- Use the IKE proposal IKE Proposal DES-SHA
```

Configuration du concentrateur VPN 5000

```
Concentrateur VPN 5000
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35
[ General ]
IPSecGateway = 172.18.124.36
DeviceName = "cisco"
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console
[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 192.168.1.1
[ Tunnel Partner VPN 1 ]
!--- Encryption peer Partner = 172.18.124.157 !---
IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet
1:0" !--- Authentication method SharedKey = "cisco123"
KeyManage = Auto !--- IPSec transforms Transform =
esp(md5,des) Mode = Main !--- Destination network
defined Peer = "10.32.50.0/24" !--- Source network
defined LocalAccess = "192.168.1.0/24" [ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1 [ IP VPN 1 ] Mode =
Routed Numbered = Off [ IKE Policy ] !--- IKE hashing,
encryption, Diffie-Hellman group Protection = SHA_DES_G1
Configuration size is 1088 out of 65500 bytes.
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner vos configurations.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'<u>Output Interpreter Tool</u> (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Note : Avant d'émettre des commandes debug, consultez <u>Informations importantes sur les</u> commandes de débogage.

Routeur Cisco 3640

- debug crypto engine Affiche les messages de débogage sur les moteurs de chiffrement, qui effectuent le chiffrement et le déchiffrement.
- debug crypto isakmp Affiche les messages relatifs aux événements IKE.
- debug crypto ipsec Affiche les événements IPSec.
- show crypto isakmp sa Affiche toutes les associations de sécurité IKE (SA) actuelles sur un homologue.
- show crypto ipsec sa Affiche les paramètres utilisés par les associations de sécurité actuelles.
- clear crypto isakmp (à partir du mode de configuration) Efface toutes les connexions IKE actives.
- clear crypto sa (à partir du mode de configuration) Supprime toutes les associations de sécurité IPSec.

<u>PIX</u>

- debug crypto ipsec Affiche les négociations IPSec de la phase 2.
- debug crypto isakmp Affiche les négociations de la phase 1 de l'ISAKMP (Internet Security Association and Key Management Protocol).
- debug crypto engine Affiche le trafic chiffré.
- show crypto ipsec sa Affiche les associations de sécurité de phase 2.
- show crypto isakmp sa Affiche les associations de sécurité de phase 1.
- clear crypto isakmp (à partir du mode de configuration) Efface les associations de sécurité IKE (Internet Key Exchange).
- clear crypto ipsec sa (à partir du mode de configuration) Efface les associations de sécurité IPSec.

Concentrateur VPN 3000

- Démarrez le débogage du concentrateur VPN 3000 en sélectionnant Configuration > System
 Events > Classes > Modify (Severity to Log=1-13, Severity to Console=1-3) : IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- Le journal des événements peut être effacé ou récupéré en sélectionnant Monitoring > Event Log.
- - Le trafic de tunnel LAN à LAN peut être surveillé dans Monitoring > Sessions.
- Le tunnel peut être effacé dans Administration > Admin Sessions > LAN-to-LAN sessions > Actions Logout.

Concentrateur VPN 5000

- vpn trace dump all Affiche des informations sur toutes les connexions VPN correspondantes, y compris des informations sur l'heure, le numéro VPN, l'adresse IP réelle de l'homologue, les scripts qui ont été exécutés, et en cas d'erreur, la routine et le numéro de ligne du code logiciel où l'erreur s'est produite.
- show vpn statistics Affiche les informations suivantes pour les utilisateurs, les partenaires et le total pour les deux. (Pour les modèles modulaires, l'affichage comprend une section pour chaque logement de module.) Current Active : connexions actives en cours. In Negot Les relations actuellement en cours de négociation. Eau élevée : nombre le plus élevé de connexions actives simultanées depuis le dernier redémarrage. Total cumulé : nombre total de connexions ayant réussi depuis le dernier redémarrage. Tunnel Starts : nombre de démarrages du tunnel. Tunnel OK : nombre de tunnels pour lesquels aucune erreur n'a été détectée. Tunnel Error (Erreur de tunnel) : nombre de tunnels comportant des erreurs.
- show vpn statistics verbose Affiche les statistiques de négociation ISAKMP et beaucoup plus de statistiques de connexion actives.

Informations connexes

- Annonce de fin de commercialisation des concentrateurs Cisco VPN 5000
- <u>Configuration de la sécurité des réseaux IPSec</u>
- <u>Configuration du protocole IKE (Internet Key Exchange)</u>
- <u>Support technique Cisco Systems</u>