Exemple de configuration d'ASA avec WebVPN et authentification unique à l'aide d'ASDM et de NTLMv1

Contenu

Introduction Conditions préalables **Conditions requises** Composants utilisés **Conventions** Configurez Ajoutez un serveur d'AAA pour l'authentification de domaine windows Créez un certificat Auto-signé Webvpn d'enable sur l'interface extérieure Configurez une liste URL pour vos serveurs internes Configurez une stratégie de groupe interne Configurez un groupe de tunnel Configurez l'Automatique-ouverture de session pour un serveur **Configuration finale ASA** Vérifiez Testez une procédure de connexion de webypn Sessions de surveillance Débuggez une session de webvpn Dépannez Informations connexes

Introduction

Ce document explique comment configurer le dispositif de sécurité adaptatif (ASA) de Cisco pour transmettre automatiquement les identifiants de connexion de l'utilisateur WebVPN, ainsi que l'authentification secondaire, aux serveurs qui nécessitent une validation supplémentaire de la connexion dans Windows Active Directory exécutant NT LAN Manager version 1 (NTLMv1). Cette fonctionnalité est connue en tant qu'authentification unique. Le document propose des liens configurés pour qu'un groupe WebVPN spécifique puisse transmettre ces informations d'authentification de l'utilisateur, éliminant de ce fait plusieurs demandes d'authentification. Cette fonctionnalité peut également être utilisée pour la configuration globale ou pour la configuration de l'utilisateur.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

 Assurez-vous que des autorisations NTLMv1 et de Windows pour les utilisateurs de la cible VPN sont configurées. Consultez votre documentation Microsoft pour plus d'informations sur des droits d'accès de domaine windows.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Internet Information Services de Microsoft (IIS)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco</u>.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer l'ASA en tant que serveur de webvpn avec SSO.

Remarque: Utilisez l'outil <u>Command Lookup Tool</u> (clients <u>enregistrés</u> seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Ajoutez un serveur d'AAA pour l'authentification de domaine windows

Terminez-vous ces étapes pour configurer l'ASA pour utiliser un contrôleur de domaine pour l'authentification.

 La configuration choisie > le Properties > l'AAA installé > des serveurs d'AAA et cliquent sur Add. Fournissez un nom pour le groupe de serveurs, tel que Windows_NT, et choisissez le Domaine NT comme protocole.

🚰 Clarn ASDM 1	5.1 for ASA - 172.16.172.52		
Fig Rules Be	arch Options Tools Wizards	: Help	
6	🍫 😥	0000	CISCO SYSTEMS
Home C	Configuration Monitoring	Back Forward Search Refresh Save Help	- ماله معالم
_	Configuration + Properties + Av	AA Setuo × AAA Servers	
Ξ,	全立革 瞬间间间	医骨部の右	
internacios	Startup Wilzard	AAA Servers	
ω,	WAA Servers	Sener Groupe	
Security Policy	Mauth, Prompt	Server Group Protocol Accounting Node Reactivation Mode	Add
64	- MAN DAP AN DURS MSR	LOCAL LOCAL	Edit
NAT	₩- 🖬 ARF		Detele
84	- Auto Upcate R- D Cartificate		
VIN	🖶 💼 Device Access	<>	
<u>a</u>	単部Device Administration 現象のMCR Register		
CSD Manugar	- BDNS Clent	- Servers in Selected Group	
Q.	Falover	Server Name or IP Address Interface Timeout	Add
PS .	- RHistory Metrics		Edit
1	- WHITPHITPS		Deicle
Nouting	₩-號IF Audit D-罰 Logging		Minus up
- 🖓			2 weathers
Global Gbjects	-Mass		terre and the second se
2	- TCP Options	C. ALL CA	t Sarana Grann
Properties	-Timeoute		
	- ORL Filtering	Apply Reset applicable	AAA server group. The Accounting Mode stillute is only of RACIUS and TACACE+ protocols.
	4 ×		
		joisce (NA.(16) 🕞 🍰 📋 Server Gro	oup: Windows_NT
		Destace	NE Domein
		P*Dator	
		descunfing	g Koda, C Smulaneuus @ Single
		Reartwate	on Node: 💿 Depletion 💿 Timed
			10
			Dead Time. 10 minutes
		Mar Falar	t Atismuts: 3
		n de l'allou	
			and an and the state of
			OK Cantel Help

 Ajoutez des Windows Server.Sélectionnez le groupe de création récente et cliquez sur Add. Sélectionnez l'interface où le serveur se trouve et écrivez l'adresse IP et le nom de contrôleur de domaine. Soyez sûr que le nom de contrôleur de domaine est écrit dans toutes les majuscules. Cliquez sur OK quand vous avez terminé.

🚰 Cisco ASDM 5	5.1 for ASA	172.16.172.5								
FIE Rulas Se	arck Options	s Tools Wizard	is Help							
G Home C	Sonfiguration	2 Monitoring	Co Dack	O Forward	Q Search R	💽 🛄 stresti Save	? Help	Cisco Sr	attas.	
Har factor Security Policy NAT	Contiguration	In Properties - A Difference - A P Vitzard etup A Certens Un Prompt WP Adhibute Kep poofing Jociate cate	AM Setup AM S Setup	AVA Servers	Protocol LOCAL NTEComa	Accounting M	ode Reaction Dep	etion Mode Edit Delete		
CSD Hanager	臣 (1) Control 탄 (2) Control 탄 (2) Control 나 (2) Control (2) Control (2) Control (2) Control (2) Con	e Access o Administration 5 Eentoos Client er mant y Motnics Hitting Ni Ni Ni y Queue RPC Server Dotions	Sen	ers in Selecte ver Name or i	d Group P Address	Interface	Times	Sut Add Fold Fold Delate ModeLp Index Test		
Properties		ibering				Apply	Rese Se	ld AAA Server wer Group:	Windows_NT	
					£1560	NA (15)	間	erface Name or IP Address: neout: Domain Parameters Server Port: Jornein Controller:	inside 10.1.1.200 10 138 ESC-&J-7800 Cancel	seconds

Cette fenêtre affiche la configuration terminée d'AAA

:



Créez un certificat Auto-signé

Terminez-vous ces étapes pour configurer l'ASA pour utiliser un certificat auto-signé.

Remarque: Dans cet exemple un certificat auto-signé est utilisé pour la simplicité. Pour d'autres options d'inscription de certificat, telles que l'inscription avec une autorité de certification externe, référez-vous à <u>configurer des Certificats</u>.

- 1. La configuration choisie > le Properties > le certificat > le point de confiance > la configuration et cliquent sur Add.
- 2. Dans la fenêtre qui apparaît écrivez un nom de point de confiance tel que le Gens du pays-TP et le contrôle génèrent un certificat auto-signé sur l'inscription. D'autres options peuvent être laissées avec leurs valeurs par défaut. Cliquez sur OK quand vous avez terminé.



Cette fenêtre affiche la configuration terminée de point de confiance

1



Webvpn d'enable sur l'interface extérieure

Terminez-vous ces étapes pour permettre à des utilisateurs en dehors de votre réseau pour se connecter utilisant le webvpn.

- 1. Configuration choisie > VPN > webvpn > webvpn Access.
- 2. Sélectionnez l'interface désirée, cliquez sur l'enable, et vérifiez la liste déroulante de groupe de tunnel d'enable sur la page de connexion de webvpn.Remarque: Si la même interface est utilisée pour le webvpn et l'accès ASDM, vous devez changer le port par défaut pour l'accès ASDM du port 80 à un nouveau port tel que 8080. Ceci est fait sous la configuration > le Properties > l'accès au périphérique > le HTTPS/ASDM.Remarque: Vous pouvez automatiquement réorienter un utilisateur au port 443 au cas où un utilisateur naviguerait vers le <ip_address> de http:// au lieu du <ip_address> de https://. Sélectionnez la configuration > le Properties > le HTTP/HTTPS, choisissez l'interface désirée, cliquez sur Edit et choisi réorientez le HTTP à HTTPS.

🖆 Cisco ASDM !	5.1 for ASA - 172.16.171.51	
File Rules Se	arch Options Tools Wizards	Help
in the second se	Configuration Montering	O O Q Q Q Cisco Systems Back Forward Search Refresh Save Help
	Configuration > VPN > WebVPN	> WebVPN Access
Ξ,	●金革 ■ 前 炎暭	· • • • • • • • • • • • • • • • • • • •
Interfaces	(마 Material Proxy 📃	WebVPN Access
<u>6</u> ,	General	
Security Policy	- B Client Update	Configure access parameters for WebVPN. (Note: The WebVPN features in this software release are currently provided as a free trial, and future main: software releases will require the nurchase and
34.	Group Policy	installation of a WebVPN feature license.)
NAT	- Tunnel Group	
	- SIVPN System Opt	Interface WebVPN Enabled Enable
<u>88</u>	E Address Manager	autside Yes Disable
VPN	D-13IPSec	
<u> </u>		
CSD Manager	ACLs	
<u>(</u>	JAPOF	
IPS	- BCSD Setup	Port Number: 443
4 ∑¢	- Cache	Defaultide Timeet d. 1900
Routing	- The Encoding	Defaultidie Timeout: Tabu seconds
(A)	- Sport Forwarding	Max. Sessions Limit: 2
Clobal Objects	Proxies	WebVPN Nemory Bize: 50 % of Intal Intysical memory
Ordear Objects	- 33 SSL VPN Client	
34	SSO Servers	Enable Tunnel Group Drop-down List on WebYPN Login Page
Properties	Servers and URL	
	WebyPN Access	Apply Reset
Configuration cha	anges saved successfully.	cisco NA (15) 🛛 🖓 🛐 🔒 3/30/06 2:37:41 PM UTC

Configurez une liste URL pour vos serveurs internes

Terminez-vous ces étapes pour créer une liste qui contient les serveurs pour lesquels vous voulez accorder votre accès d'utilisateurs WebVPN.

- 1. Le Configuration > VPN > WebVPN > Servers and URLs choisi et cliquent sur Add.
- 2. Écrivez un nom pour la liste URL. Ce nom n'est pas visible aux utilisateurs finaux. Cliquez sur Add.
- Écrivez le nom d'affichage URL car il doit être affiché aux utilisateurs. Écrivez les informations URL du serveur. Ceci devrait être comment vous accédez à normalement le serveur.

Cisco ASDM 5. File Rules Sea	.1 for ASA - 172.16.172.52 rm Options Tools Wizards	: Help	
Home Co	anfiguration Monitoring	O O C C C C C C C C C C C C C C C C C C	Cisco Systems Latility, Latility,
Interfaces Security Policy NAT	Contiguiation - VEN - WebVPD		Add Eot
CSD Manager	CSD Betup Cache Content Rewrite Encoding Port Forwarding Proxies MProxy Bypass SSL VPN Client SSO Servers Content Servers and URLs Webpage Customi	Add Server and URL List List Name: webserver URL Display Name	URL Add
Properties	Add St ORL:	erver or USL Vaplay Name: Internal Server https v 10.1.1.200 ΟΚ Cancel Help	Move Op Move Down ancel Help

4. Cliquez sur OK, CORRECT, et puis appliquez.



Configurez une stratégie de groupe interne

Terminez-vous ces étapes pour configurer une stratégie de groupe pour vos utilisateurs WebVPN.

- 1. Sélectionnez le **Configuration > VPN > General > Group Policy**, cliquez sur Add, et sélectionnez la **stratégie de groupe interne**.
- Sur l'onglet Général, spécifiez un nom de stratégie, tel qu'Internal-Group_POL_WEBVPN. Décochez alors héritent à côté des protocoles de Tunnellisation et du webvpn de contrôle.

📬 Add Internal Group Policy							
Name: mal-GRP_POL_	WEBVPN						
General IPSec Client Confi	guration Cli	ent Firewall Hardware Client WebVPN					
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.							
Tunneling Protocols:	📃 Inherit	IPSec VebVPN					
Filter:	🗹 Inherit	Manage					
Connection Settings							
Access Hours:	🗹 Inherit	New					
Simultaneous Logins:	🗹 Inherit						
Maximum Connect Time:	🗹 Inherit	Unlimited minutes					
Idle Timeout:	🗹 Inherit	Unlimited minutes					
Servers							
DNS Servers:	🗹 Inherit	Primary: Secondary:					
WINS Servers:	🗹 Inherit	Primary: Secondary:					
DHCP Scope:	🗹 Inherit						
	ок	Cancel Help					

 Sur l'onglet de webvpn sélectionnez l'autre sous-titre-onglet. Décochez héritent à côté des serveurs et des listes URL et sélectionnent la liste URL que vous avez configurée de la liste déroulante. Cliquez sur OK quand vous avez terminé.

🖆 Add Internal Group Policy 🛛 🛛 🔀
Name: mal-GRP_POL_WEBVPN
General IPSec Client Configuration Client Firewall Hardware Client WebVPN
Configure WebVPN attributes using the following tabs . Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client
Servers and URL Lists: 🔄 Inherit 🛛 webserver 🗸 🔽 New
Web-Type ACL ID: Vielent Manage
SSO Server: Inherit New
HTTP Compression: V Inherit Cable Disable
Keepalive Ignore
Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore.
Transaction Size: Inherit
- Deny Message
✓ Inherit
OK Cancel Help

Configurez un groupe de tunnel

Terminez-vous ces étapes pour configurer un groupe de tunnel pour vos utilisateurs WebVPN.

 Sélectionnez la configuration > le VPN > le groupe de général > de tunnel, cliquez sur Add et sélectionnez le webvpn Access...



 Écrivez un nom pour le groupe de tunnel, tel que WEB_VPN-GRP. Sur l'onglet de base sélectionnez la stratégie de groupe que vous avez créée et la vérifiez que le type de groupe est

webvpn.

📧 Edit Tunnel Group 🛛 🔀
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure general eccess officientes from the following out take
Basic AAA Client Address Assignment Advanced
AAA Client Address Assignment Advanced
Group Policy: Internal-GRP_POL 💌
Internal-GRP_POL_WEBV DftGrpPolicy
strip the realm from usemame before passing it on to the AAA server
Strip the group from username before passing it on to the AAA server
OK Cancel Help

3. Allez à l'AAA l'onglet.Pour le groupe de serveurs d'authentification, choisissez le groupe que vous avez configuré afin d'activer l'authentification NTLMv1 avec votre contrôleur de domaine.Facultatif : Vérifiez les GENS DU PAYS d'utilisation si le groupe de serveurs n'active pas l'utilisation de la base de données locale des utilisateurs au cas où le groupe configuré d'AAA échouerait. Ceci peut vous aider à dépanner à une date ultérieure.

🖆 Edit Tunnel Group								
Name: WEB_VPN-GRP Type: webvpn								
General WebVPN								
Configure general access attributes from the following sub-tabs.								
Basic AAA Client Address Assignment Advanced								
To set authentication server group per interface, go to the Advanced tab.								
Authentication Server Group: Windows_NT								
Use LOCAL if Server Gra-None								
Authorization Server Group: LOCAL								
 Users must exist in the authorization database to connect 								
Accounting Server Group:								
Authorization Settings								
O Use the entire DN as the username								
Specify individual DN fields as the username								
Primary DN Field: CN (Common Name)								
Secondary DN Field: OU (Organization Unit)								
Password Management								
Override account-disabled indication from AAA server								
Enable notification upon password expiration to allow user to change password								
Enable notification prior to expiration Notify days prior to expiration								
OK Cancel Help								

- 4. Allez à l'onglet de webvpn et puis allez au sous-titre-onglet de **pseudonymes et URLs de groupe**.
- 5. Écrivez un pseudonyme sous des pseudonymes de groupe et cliquez sur Add. Ce pseudonyme apparaît dans la liste déroulante présentée aux utilisateurs WebVPN à la procédure de connexion.

🖆 Edit Tunnel Group		
Name: WEB_VPN-GRP	Type: webvpn	
General WebVPN		
Configure WebVPN access att	tributes from the following sub-tabs.	
Basic NetBIOS Servers Grou	up Aliases and URLs Web Page	
Group Aliases		
Alias:	Alias St Add >> Group-Selection ena	atus ible
Z Enable	<< Remove	
Group URLs		
LIDL (http://https/	URL St	atus
one (mp of mpoy.	Add >>	
Enable	<< Remove	
	OK Cancel Help	

6. Cliquez sur OK, puis sur Apply.

Configurez l'Automatique-ouverture de session pour un serveur

Commutez à la ligne de commande pour activer SSO pour vos serveurs internes.

Remarque: Cette étape ne peut pas être terminée dans l'ASDM et doit faire utilisant la ligne de commande. Référez-vous à <u>accéder au</u> pour en savoir plus d'<u>interface de ligne de commande</u>.

Utilisez la commande d'automatique-**ouverture de session** de spécifier la ressource de réseau, telle qu'un serveur, que vous voulez donner votre accès utilisateur à. Une adresse IP de serveur unique est configurée ici, mais une plage de réseau telle que **10.1.1.0** /24 peut également être spécifiée. Référez-vous au pour en savoir plus de commande d'automatique-<u>ouverture de session</u>.

memory

Dans cet exemple de sortie, la commande d'automatique-**ouverture de session** est configurée pour le webvpn globalement. Cette commande peut également être utilisée dans le mode de configuration de mode de configuration de groupe de webvpn ou de nom d'utilisateur de webvpn. L'utilisation de cette commande dans le mode de configuration de groupe de webvpn le limite à un groupe particulier. De même, l'utilisation de cette commande dans le mode dans le mode de configuration de nom d'utilisateur de webvpn le limite à un groupe particulier. De même, l'utilisation de cette commande dans le mode de configuration de nom d'utilisateur de webvpn le limite à un utilisateur individuel. Référez-vous au pour en savoir plus de commande d'automatique-<u>ouverture de session</u>.

Configuration finale ASA

Ce document utilise la configuration suivante :

Version 7.1(1) ASA

ASA#show running-config : Saved : ASA Version 7.1(1) ! terminal width 200 hostname ASA domain-name cisco.com enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface GigabitEthernet0/0 nameif outside securitylevel 0 ip address 172.16.171.51 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside securitylevel 100 ip address 10.1.1.1 255.255.255.0 ! interface GigabitEthernet0/2 shutdown no nameif no security-level no ip address ! interface GigabitEthernet0/3 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name cisco.com pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm512.bin no asdm history enable arp timeout 14400 route outside 0.0.0.0 0.0.0.0 172.16.171.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute !---AAA server configuration aaa-server Windows_NT protocol nt aaa-server Windows_NT host 10.1.1.200 nt-auth-domaincontroller ESC-SJ-7800 !--- Internal group policy configuration group-policy Internal-GRP_POL_WEBVPN internal group-policy Internal-GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn webvpn url-list value webserver username cisco password Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa authentication http console LOCAL aaa authentication ssh console LOCAL aaa authentication enable console LOCAL http server enable 8181 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart !---Trustpoint/certificate configuration crypto ca trustpoint Local-TP enrollment self crl configure crypto ca certificate chain Local-TP certificate 31 308201b0 30820119 a0030201 02020131 300d0609 2a864886 f70d0101 04050030 le311c30 1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334 3930345a 170d3136 30333237 31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404

```
9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17
68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3
776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06
092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544
59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d
3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b
af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de
775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a
f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c
quit !--- Tunnel group configuration tunnel-group
WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP
general-attributes authentication-server-group
Windows_NT default-group-policy Internal-GRP_POL_WEBVPN
tunnel-group WEB_VPN-GRP webvpn-attributes group-alias
Group-Selection enable telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
!--- WebVPN Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end
```

<u>Vérifiez</u>

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'<u>Outil Interpréteur de sortie</u> (clients <u>enregistrés</u> uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Testez une procédure de connexion de webvpn

Procédure de connexion en tant qu'utilisateur pour tester votre configuration.

 Tentative d'ouvrir une session à l'ASA avec les informations utilisateur de votre Domaine NT. Sélectionnez le groupe alias configuré dans l'étape 5 <u>configurent</u> dessous un <u>groupe de</u> <u>tunnel</u>.

WebVPN Service - Microsoft Internet Explorer	
Ele Edit View Figurantes Icols Help	- 🦧
🚱 Back 🔹 🐑 💌 😰 🏠 🔎 Search 🧙 Favorites 🤣 🍙 - 🌺 🚍 🦓	
Addross 💩 https://172.16.171.51/+webvpn+/index.html 💙 🋃 🙃	Unks »
CISCO SYSTEMS 	
Login	
Please enter your username and password.	
USERNAME: test	
PASSWORD:	
GROUP: Group-Selection	
Login Clear	
	~
S Doue	

2. Recherchez les liens configurés aux serveurs internes. Cliquez sur en fonction le lien pour vérifier.



Sessions de surveillance

Le Monitoring > VPN > VPN Statistics > Sessions choisi et recherchent une session de webvpn qui appartient au groupe configuré dans ce document.

Gisco ASDM	5.1 for ASA - 172.16.171.51							
File Rules Se	Configuration	Help (Back For	Covered Set	ych Re	tresh Save	? Неф		Cisco Systems
Hiterisces VPN Properties Logging	Monitoring > VPN > VPN Statistic VPN Connection Graph WebVPNUSVC Cluster Loads Crypto Statistics Compression Statistic Compression Statistic Compression Statistic Compression Statistic Compression Statistics Protocol Statistics Sessions WebVPN SSO Statistics	s - Session Sessions Remote Access 0 Filter By: Userr IP Ad test 171 59.89 To sort VPN Logout By:	s LAN-to-LAN 0 WebVPN name tress 116 V	WebVPN 1 Group Po Tunnel G Itemal-ORF VEB_VPN-G	SSL VPIN Client 0 All Sessions plicy P roup E POL WebVPI RP 3DE3	E-mail Proxy 0 Protocol Encryption N	Total 1 1 1 1 1 1 1 1 1 1 1 1 3 1 3 1 1 1 1	Total Cumulative 3 Filter ogin Ti Details aratior Logout Ping popup menu.
Data Refreshed 8	Successfully.			CISCO	INA (15)		🚱 🔄 🖸 3/30	06 3:05:21 PM UTC

Débuggez une session de webvpn

Cette sortie est un échantillon mettent au point d'une session réussie de webvpn.

Remarque: Référez-vous aux <u>informations importantes sur les commandes de débogage</u> avant d'utiliser les commandes de **débogage**.

```
ASA#debug webvpn 255 INFO: debug webvpn enabled at level 255 ASA# ASA#
webvpn_portal.c:ewaFormServe_webvpn_login[1570] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286] WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782] !--- Begin AAA WebVPN: calling AAA with
ewsContext (78986968) and nh (78960800)! WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422] WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn auth.c:http_webvpn_post_authentication[1095] WebVPN: user: (test) authenticated. !--- End
AAA webvpn_auth.c:http_webvpn_auth_accept[2093] webvpn_session.c:http_webvpn_create_session[159]
webvpn_session.c:http_webvpn_find_session[136] WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136] webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202] traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421] webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
```

webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924] WebVPN: session has been authenticated. *!--- Output supressed* webvpn_auth.c:webvpn_auth[286] webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924] WebVPN: session has been authenticated. webvpn_session.c:webvpn_update_idle_time[924]

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Si la liste déroulante de groupe n'est pas présente sur la page de connexion de webvpn, soyez sûr que vous vous êtes terminé l'étape 2 sous le <u>webvpn d'enable sur l'interface</u> <u>extérieure</u> et étape 5 <u>configurent</u> dessous un <u>groupe de tunnel</u>. Si ces étapes ne sont pas terminées et le déroulant manque, l'authentification tombe sous le groupe par défaut et échoue vraisemblablement.
- Bien que vous ne puissiez pas attribuer des droits d'accès à l'utilisateur dans l'ASDM ou sur l'ASA, vous pouvez limiter des utilisateurs avec des droits d'accès de Microsoft Windows sur votre contrôleur de domaine. Ajoutez les autorisations nécessaires de groupe de NT pour la page Web que l'utilisateur authentifie à. Une fois les journaux de l'utilisateur dans le webvpn avec les autorisations du groupe, accès aux pages spécifiées est accordés ou refusés en conséquence. L'ASA agit seulement en tant qu'hôte d'authentification de proxy au nom du contrôleur de domaine et toutes les transmissions ici sont NTLMv1.
- Vous ne pouvez pas configurer SSO pour Sharepoint au-dessus de webvpn parce que le serveur de Sharepoint ne prend en charge pas l'authentification basée par formes. En conséquence, les signets avec le poteau ou la procédure embrochable de poteau s'applique pas applicable ici.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques Cisco Systems