Forefront UAG mit DirectAccess

Implementierungsumgebung:

- Windows Server 2008 R2 englisch mit zwei Netzwerkkarten als Forefront UAG Server paralell zu der TMG Enterprise Umgebung als Firewall. Der Forefront UAG Server steht in der DMZ vor einer nicht Microsoft Firewall [®]
- Windows 7 Ultimate oder Enterprise Client fuer DirectAccess Zugriff
- Windows Server 2008 R2 Enterprise CA
- Windows Server 2008 R2 Enterprise als NLS Server

Weitere Informationen:

http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html http://www.it-training-grote.de/download/Forefront-UAG.pdf http://blogs.technet.com/b/tomshinder/archive/2010/08/03/how-to-configure-uag-topublish-your-private-certificate-revocation-list.aspx http://technikblog.rachfahl.de/wp-content/uploads/2010/07/Direct-Access-Howto.pdf http://technet.microsoft.com/en-us/library/ee861167.aspx http://www.microsoft.com/downloads/details.aspx?FamilyID=9A87EFE8-E254-4473-8A26-678ADEA6D9E9&displaylang=en

Auf dem Forefront UAG Server

NIC benennen



Netzwerkkarte Extern

NetBT kann am externen Interface deaktiviert werden!

🖣 EXTERNAL Properties 🛛 🗙
Networking Sharing
Connect using:
🔮 Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Clier
Configure
This connection uses the following items:
 Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4)
Install Uninstall Properties
Description Allows other computers to access resources on your computer using a Microsoft network.
OK Cancel

Bindungsreihenfolge – INTERNAL muss oben stehen



DNS Server GlobalqueryBlocklist ISATAP

Die GlobalQueryBlocklist muss von JEDEM DNS Server im LAN fuer ISATAP entfernt werden.

👞 Administrator: Eingabeaufforderung	
C:\>dnscnd sru-?:	_
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd srv-v? /config /globalqueryblocklist wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd_srv-wasadaa?? /config /globalqueryblocklist_wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd_srv+@l/config_/globalqueryblocklist_wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd sru-' /config /globalqueryblocklist wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd srv * * * * /config /globalqueryblocklist wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd srv=k.7 \?v:09 /config /globalqueryblocklist wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd sru—()}=();	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd srv-}config /globalqueryblocklist wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd sru= $\mathbb{L}_{p^{(1)}}$	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd sru= $\psi_{[V]}$ $\psi_{[V]}$?? /config /globalqueryblocklist wpad	
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt. Der Befehl wurde erfolgreich ausgeführt.	
C:\>dnscmd sru-koo as 94 /config /globalqueryblocklist wpad	
Pagistniawungssigeneeksft glabalguspubleeklist uunde gunückgesetgt	

Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.

A Record ISATAP = 10.80.20.29



Windows Firewallausnahmen fuer ICMPv6

GPO erstellen fuer DC und NLS Server

Anmerkung: Auf den Server kann die Firewall auch ausgeschaltet sein, auf den DirectAccess Clients muss diese eingeschaltet sein, wegen der vom DirectAccess Wizard erstellten Verbindungsrichtlinien!

Globale Windows Gruppe fuer DirectAccess Clients

Name = CG-DirectAccess

Neues Objekt - Gruppe		X
🥵 Erstellen in: 💘	III/Gruppen/Computergruppen	
Gruppenname:		
CG-DirectAccess		
Gruppenname (Prä-Windows 2000):		
CG-DirectAccess		
Gruppenbereich	Gruppentyp	
C Lokal (in Domäne)	 Sicherheit 	
Global	C Verteilung	
C Universal		
	OK Abbre	echen

Windows 7 Client (Ultimate oder Enterprise) Maschinen in die Gruppe aufnehmen

Modifizierung des CRL Verteilungspfad (CDP)

Es wird eine Windows Server 2008 R2 Enterprise CA verwendet Name = SRV-XXX-PKI01.XXX.LOCAL

Fuer das Publishing der CRL ueber das separate TMG Array wird ein oeffentlicher Hostname benoetigt:

Name = Legacy.xxxx.de \rightarrow 217.x.xxx.214

Damit von der CA ausgestellte Zertifikate den CRL Distribution Point auf HTTP mit dem externen Namen gesetzt bekommen, muss die CA gepatched werden. Das geht mit CERTUTIL Befehlen und/oder diesem netten Script, was mir freundlicherweise Carsten Zuege zur Verfuegung gestellt hat – Danke Carsten!. Der http-Pfad muss ersetzt werden durch den oeffentlichen DNS-Namen. Der CRL Pfad wird spaeter von Forefront TMG veroeffentlicht. Angepasst werden muss der CN fuer die AD Konfigurationspartition und der http CRL Pfad.

 □ CA-PASI-Config - Editor
 □

 Date Bearbeken Format Ansicht ?

 I::Declare Configuration NamingContext

 certutil -setreg CA\DSConfigDN CN=Configuration,DC=80,DC=Less.

 ::Define CRL Publication Intervals

 certutil -setreg CA\CRLPeriodUnits 1

 certutil -setreg CA\CRLPeriod "weeks"

 certutil -setreg CA\CRLPeriod "weeks"

 certutil -setreg CA\CRLPeriod "weeks"

 certutil -setreg CA\CRLPeriod "weeks"

 certutil -setreg CA\CRLPeriod "days"

 ::Apply the required CDP Extension URLS

 PAUSE

 Certutil -setreg CA\CRLPublicationURLS "1:%windir%\system32\CertSrv\CertEnroll\%%

 \$%8%9.crl\n79:ldap:///CN=%%7%%8.cN=%%2.cN=CDP,CN=Public Key

 Services,cN=Services,%%6%%L0\n6: http://l@new.hfw.badworment.de/certenroll/%%3%%

 \$%8%9.crl\n79:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%L1

 PAUSE

 ::Apply the required AIA Extension URLS

 certutil -setreg CA\CACertPublicationURLS "1:%windir%\system32\CertSrv\CertEnroll\%%1

 \n2: http://l@new.hfw.badworment.de/certenroll\%%3%%

 w%2

 Services, crl

 PAUSE

 ::Apply the required AIA Extension URLS

 certutil -setreg CA\CaCertPublicationURLS "1:%windir%\system32\CertSrv\CertEnroll\%%1

 \n2: Matt

Anmerkung: Publish ueber Forefront UAG geht auch:

http://blogs.technet.com/b/tomshinder/archive/2010/08/03/how-to-configure-uag-to-publish-your-private-certificate-revocation-list.aspx

Nach Aenderung

enschaften vor	n RootCA	?
Speicherung	Zertifikatverwaltungen	Registrierungs-Agents
Überwachung	Wiederherstellungs-	Agents 📔 Sicherheit
Allgemein 📔 Ri	ichtlinienmodul 📔 Beendigu	ngsmodul Erweiterungen
Erweiterung ausv	vählen:	
- Sperrlisten-Verte	ilungspunkt	•
Geben Sie Stand erhalten können.	lorte an, von denen Benutzer	eine Zertifikatsperrliste
C:\Windows\sy: Idap:///CN= <c4< td=""><td>stem32\CertSrv\CertEnroll\<c \TruncatedName><cblname< td=""><td>CaName><crlnamesuffix><i eSuffix>.CN=<servershortnar< td=""></servershortnar<></i </crlnamesuffix></td></cblname<></c </td></c4<>	stem32\CertSrv\CertEnroll\ <c \TruncatedName><cblname< td=""><td>CaName><crlnamesuffix><i eSuffix>.CN=<servershortnar< td=""></servershortnar<></i </crlnamesuffix></td></cblname<></c 	CaName> <crlnamesuffix><i eSuffix>.CN=<servershortnar< td=""></servershortnar<></i </crlnamesuffix>
http://longenit	The import do/certenroll/	(CaName> <crlnamesuffix></crlnamesuffix>
•		▶
	Hi	nzufügen Entfernen
🗖 Sperrlisten ar	n diesem Ort veröffentlichen	
In alle Sperifi Veröffentlicht	sten einbeziehen. Legt fest, w ung im Active Directory veröffe	o dies bei manueller entlicht werden soll
🗖 In Sperrlisten	einbeziehen. Wird z. Suche v	von Deltasperrlisten verwende
🗌 In CDP-Erwe	iterung des ausgestellten Zert	ifikats einbeziehen
🗖 Deltasperrlisti	en an diesem Ort veröffentlich	en
🗖 In die IDP-Er	weiterung ausgestellter CBLs	einbeziehen

CRL Pfad vor Modifizierung – Zu sehen in den Zertifikateigenschaften



CRL Pfad in einem neu ausgestellten Zertifikat

Certificate	×	
General Details Certification Path	1	
	' (
Show: <all></all>	•	
Field	Value	
Application Policies	[1]Application Certificate Polic	
🛐 Subject Key Identifier	13 a8 de ea c0 3a 7e d8 05 e4	
a Authority Key Identifier	KeyID=c1 b9 df bd 8c 18 db 1	
CRL Distribution Points	[1]CRL Distribution Point: Distr	
Authority Information Access	[1]Authority Info Access: Acc	
🛅 Thumbprint algorithm	sha1	
Thumbprint 🔚	5d f7 22 d3 18 77 65 5f 94 40	
Friendly name		
[1]CRL Distribution Point		
Full Name:		
URL=ldap:///CN=RootCA	CN=SAUGE-	
PKI01, CN=CDP, CN=Public%20Key		
certificateRevocationList?base?obi	ectClass=cRLDistributionPoint	
URL=http://kanaukii:ki	.de/certenroll/RootCA.crl	
I		
Fo		
Learn more about <u>certificate details</u>		
	OK	

CRL ueber Forefront TMG veroeffentlichen

2 🗐	CA-CRL	🧭 Zulassen	🎼 НТТР	🥽 CA-CRL	📄 SRV-🏬 PKIO 🦓 Alle Benutzer
Parame	<u>eter</u>				
Webse	rververoeff	entlichung			
Kein H	TTPS	_			
Pfad /c	ertenroll/*				
Keine A	Authentifizio	erung			
Keine A	Authentifizio	erungsdelegati	on		
Keine H	ITTP Kom	primierung			
Alle Be	nutzer				
Zeitpla	n = Immer				

Oeffentlicher Name der Name, welche als CDP in den CA Eigenschaften steht

Ueberpruefen

C Internet Explorer cannot display the webpage - Windows Internet Explo	rer
🕞 🕞 🗢 🙋 http://	
File Edit View Favorites Tools Help	
🔆 Favorites 🛛 🚓 📶 Forefront Foren 🛛 MCSEBoard 🕺 XING 🙋 TV 🙋 MC	IT 🙋 Banking
SInternet Explorer cannot display the webpage	
File Download X Do you want to open or save this file? Image: RootCA.crl Type: Certificate Revocation List, 959 bytes From: Image: Certificate Revocation List, 959 bytes From: Image: Certificate Revocation List, 959 bytes Open Save Cancel Image: Certificate Revocation List, 959 bytes Cancel Image: Certificate Revocation List,	O% of RootCA.crl from O% of RootCA.crl from Getting File Information: RootCA.crl from Is RootCA.crl from Is Bestimated time left: Download to: Transfer rate: Close this dialog box when download completes Open Open Folder Cancel

Testen der CRL

certutil -URL http://crl.domain.de/crld/ca.crl

URL Retrieval Tool		×
Status Type	hU	<u> </u>
 Timeout (sec) 15 ☐ Sign LDAP Traffic 	Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.	Retrieve C Certs (from AIA) CRLs (from CDP) COCSP (from AIA) Retrieve
Url to Download http://d	crl. domain. de/crld/ca.crl	

Computerzertifikat fuer UAG Server

Interner DNS FQDN – SAN ist meines Erachtens nicht noetig. Steht aber so im UAG Step by Step Guide von MS!

CN = SRV-xxx-xxx.LOCAL SAN = SRV-xxx-xxx.xxx.LOCAL

Console1 - [Console1 - [Consol	ole Root\Certificates (Local Computer)\Personal\Certificates]	
Console Root	Issued To A Issued By Expira	Actions
Certificates (Lo	cal Com	Certificates
+ C Re	quest Certificates	
🗄 🔁 You	can request the following types of certificates. Select the certificates you want to request, and the	n click Enroll.
	Certificate Properties	
	General Subject Extensions Private Key Certification Authority Signature	
	The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject pame and alternative pame values that can be used	S W
	in a certificate.	s®
	Subject of certificate	
	The user or computer that is receiving the certificate	
	Type: CN=SRV-DBinkArGourDBin .LOCAL	
	Common name Add >	
	Value:	
	< Remove	
Lea	Alternative name:	
	Type:	
	DNS	Cancel
	Value:	
	Add >	
	< Remove	
•		
Personal store contains		
	Learn more about <u>subject name</u>	
	OK Cascal Apply	
	CalicelApply	

Webserverzertifikat fuer UAG Server

 $CN = DirectAccess.xxx.de \rightarrow A$ Record auf erste oeffentliche IP, welche auf dem externen Interface des Forefront UAG Server gebunden ist! SAN = DirectAccess.xxx.de

WICHTIG: Der CN, welcher hier verwendet wird, muss im Public DNS auf die erste oeffentliche IP gebunden sein, welche am externen Interface des Microsoft Forefront UAG Server verwendet wird.

🛱 Console1 - [Cor	sole Root\Certificates (Local Co	mputer)\Personal\Certific	ates]		
🚠 File Action	/iew Favorites Window Help				_ & ×
🗢 🔿 🔁 🗔	📋 🙆 😹 🚺 📅				
Console Root	Issued To 🔺	Issued By		Expira	Actions
🖃 🔂 Certificates (Local Com 🛛 🌠 SRV- encommendatio .	ocal RootCA		02.08	Cortificatos 🔺
Lert	licate Enroliment		_	-	
🖃 🚰 🗐 Cerl	ificate Enrollment				.bfw 🔺
	equest Certificates				•
۱ 🗄 🗄 ۱	ou can request the following types of	certificates. Select the certifica	ates you want to request,	and ther	click Enroll.
÷ 🧧	Certificate Properties				×
+ 	🔥 Subject General Extens	ons Private Key Certificatio	n Authority Signature		s®
± <u>=</u>	The subject of a certificate is th enter information about the typ in a certificate.	e user or computer to which the es of subject name and alterna	e certificate is issued. You tive name values that can	can be used	s®
	Subject of certificate				
	The user or computer that is rec	eiving the certificate			
	Type:				
	Common name	Add >			
	Value:				
		< Remove			
L	a Alternative name:		•	>	
	Туре:		DNS		
	DNS]	DirectAccess.t	.ue	Cancel
	Value:				
		Add >			
		< Remove			
			-		
		OK	Cancel	Apply	

2 Public IPv4 Adressen auf dem externen Interface von Forefront UAG

217.x.xxx.212 → DirectAccess.xxx.de 217.x.xxx.213

ACHTUNG: http://technet.microsoft.com/en-us/library/ee844123(WS.10).aspx

NLS Server konfigurieren

Anhand des NLS Servers prueft der DirectAccess Client, ob er im LAN oder im Internet steht. Der NLS Server muss ein Webserver (IIS; Apache etc.) sein, auf dem eine HTTPS-Bindung existiert und das Zertifikat von einer vertrauenswuerdigen Zertifizeirungsstele ausgestellt ist, welcher der DirectAccess Client und der Forefront UAG Server vertrauen.

xx.xx.xxx.LOCAL

Der NLS sollte hochverfuegbar gemacht werden, weil der DA Client anhand der Verfuegbarkeit des NLS prueft, ob er im LAN oder im Internet steht. **Achtung**: Der NLS wird von der NRPT ausgeschlossen und ist somit vom DirectAccess Client, wenn dieser nicht mit dem LAN verbunden ist, nicht erreichbar ist. Es muss also ein NLS verwendet werden, der nur im LAN erreichbar sein muss.

Тур	Hostname	Port	IP-Adresse	Bindung	Hinzufügen
http		80	*		
net.tcp				808:*	Bearbeiten
net.pip	e			*	Fotfernen
net.m				localhos	Entremen
msmq				localhos	Durchsuchen
https		443			
•				•	

Forefront UAG Installation und Konfiguration

Die Installation erfolgt auf einem voll gepatchten Windows Server 2008 R2 mit zwei Netzwerkkarten.

Forefront UAG Set	up Wizard
1. Welcome	
2. Sign 2. Agreement	Installing Forefront UAG
3. Select Location	Installing Forefront UAG may take some time. Please wait
4. Install	Progress: Installing Roles and Features10%
5. Finish	
	< Back Next > Cancel

Server rebooten

Forefront UAG Setu	up Wizard
1. Welcome	
^{2.} Agreement	the Forefront UAG Setup Wizard
3. Select Location	The server must be restarted .
4. Install	How do you want to proceed? Restart now Restart later
5. Finish	
	< Back Next > Cancel

Forefront UAG Update 1 installieren

🙀 Microsoft Forefront Unifie	d Access Gateway Setup
	Please read the Microsoft Forefront Unified Access Gateway License Agreement
	MICROSOFT SOFTWARE SUPPLEMENTAL
	UNIFIED ACCESS GATEWAY 2010 UP1 FOR MICROSOFT UNIFIED ACCESS GATEWAY
	Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Unified Access Gateway software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use this supplement with
KKAKK (☑ I accept the terms in the License Agreement
Print	t Back Install Cancel

Systemrichtlinie konfigurieren fuer Remote Computer Zugriff



Malware Inspection ausschalten



Logging/Alerting konfigurieren

WFP Filter Alerting Konflikt ausschalten



Interne Netzwerke am TMG des UAG eintragen, da der UAG nur Proxy in der DMZ ist und die Netze hinter dem UAG ueber ein Forefront TMG Enterprise Array erreichen muss.

ernal Properties		
Auto Discovery F General IP address ranges in	Forefront TMG Client We Addresses Domai Icluded in this network:	eb Proxy CARP NLB ns Web Browser
Start Address 10.80.0.0 10.80.16.0 10.80.20.0	End Address 10.80.7.255 10.80.17.255 10.80.20.255	Add Adapter Edit Remove Add Private Add Range
	ОК	Cancel Apply

Statische Rouetn konfigurieren

Forefront Threat Manager	ment Gateway:	2010			Network Enterpr
Networks Network Sets	Network Rules Netmask	Network Adapters	Routing Web Ch Metric	haining VISP Redundancy V	Tasks Help
Network Topology Routes	5				Routing Tasks
10.80.0.0	255.255.248.0	10.80.20.1	0		🛅 Create Network Topology
10.80.16.0	255.255.254.0	10.80.20.1	0		Route

UAG Getting Started Assistent

AUQULELIQUE	Internal	External	Unassigned
EXTERNAL	2110011101	∠	ondooignod
INTERNAL	· ·	-	
SSL Network Tunneling			V
dapter name: INTERNAL P DHCP enabled: No P address: 10.80.20.29			

Server Management WizardX
Coloct Configuration
Select Configuration
Specify whether this is a single Forefront UAG server, or configure it as an array member.
Single server
C Array member
Forefront UAG array members must belong to a domain.
< Back Next > Cancel
Use Microsoft Update for Forefront UAG
Microsoft Update offers security and important updates for Windows and other Microsoft software, including Forefront UAG. Updates are delivered using your existing Windows
Update settings.
📝 🕫 Use Microsoft Update when I check for updates (recommended)
This option does not change your existing Windows Update settings.
😥 🔿 I don't want to use Microsoft Update.
See the Missee # Lindete ERO
Read our Privacy Statement
OK Cancel
Activate Configuration
Activate Configuration
The system is being activated for the first time.
Enter a passiona and choose a anottery to store the backup coningulation mes.

The system is being ac Enter a password and	tivated for the first time. choose a directory to store the backup configuration files.	
Password:	•••••	
Confirm password:	••••••	
Backups directory:	C:\ProgramData\Microsoft\UAG\AutoBackups	Browse

×

Konfiguration sichern und aktivieren

Act	tivate Configuration
	Activate Configuration
	You must activate the configuration to apply your changes.
	If you select to back up the configuration, current settings (prior to activation) will be saved.
	Back up configuration before performing this activation
	Activation might take several minutes.
	Activate > Cancel

DirectAccess Einrichtung

SMicrosoft Forefront Unified Ac	cess Gateway Management	
File View Admin Messages Help		
Forefront Unified Access SRV-##UAG01 HTTP Connections HTTPS Connections DirectAccess	Forefront UAG DirectAccess Configuration	
	Clients Select the security groups	Infrastructure Servers Identify the Infrastructure Servers (DNS, DC, Management) required by DirectAccess clients.
	of client computers that will be enabled for UAG DirectAccess configure Configure	Application Servers Select application servers that require additional authentication and encryption.
	۲	•
	Overview of DirectAccess Prerequisites for deploying UAG DirectAccess	Disable Generate Policies

Angabe der globalen Gruppe, welche alle zukuenftigen Direct Access Clients enthaelt. Diese Gruppe wird vom UAG DA Assistenten verwendet, um ueber die Sicherheitsfilterung eine erstellte Gruppenrichtlinie anzuwenden, welche fuer die DA-Einstellungen verwendet wird.

a UAG DirectAccess Client Configuration	×
UAG DirectAccess Client Configuration	
Select the security groups of client computers that will be enabled for UAG Dir	ectAccess configuration.
ScG-DirectAccess	
	Remove
Learn more	Finish Cancel

Angabe der ersten IP-Adresse, welche am externen Interface von Forefront UAG gebunden ist, auf der auch das IP-HTTPS Zertifikat gebunden ist und der Publis Hostname verweist.

au UAG DirectAccess Server Config	juration	×
UAG DirectAcces	s Server Configuration	
Connectivity Managing DirectAccess Services Authentication Options	To set up the UAG DirectAccess server, assign IP addresse	es to the Internet-facing and internal networks. DirectAccess r
	Internet-facing First Internet-facing IPv4 address:	Internal Internal IPv4 address used when ISATAP is
	217	deployed on the UAG DirectAccess server: 10.80.20.29
	Second Internet-facing IPv4 address: 217 : 1999 -213	Internal IPv6 address:
	ISATAPIPv6 transition technologies will be en DNS name "ISATAP" with "10.80.20.29" on the these domains. In addition ensure that ISATAP DNS servers.	abled on the UAG DirectAccess server. Register the DNS in all domains to enable IPv6 connectivity on Pis not blocked in the <u>Global Query Block List</u> on all
Learn more		< Back Next > Finish Cancel

Forefront UAG fungiert als NAT64 und DNS64 Gateway / Router.

au UAG DirectAccess Server Config	uration	×
UAG DirectAccess	Server Configuration	
Connectivity Managing DirectAccess Services Authentication Options	NAT64 and DNS64 enable DirectAccess clients to access IPv4-only resources, and are required by UAG DirectAccess. You can use either the UAG DirectAccess NAT64 and DNS64, or deploy external NAT64 and DNS64. Select whether to use UAG DirectAccess NAT64 and DNS64: Fnable UAG DirectAccess NAT64 Enable UAG DirectAccess DNS64	
Learn more	< Back Next > Finish	Cancel

Auswahl der Root CA, welche alle Zertifikat fuer den NLS, UAG und DA Client ausgestellt hat, sowie des IP-HTTPS Zertifikats, falls der DA Client nicht per 6to4 oder Teredo connecten kann.

au UAG DirectAccess Server Config	uration	×
UAG DirectAccess	Server Configuration	
Connectivity Managing DirectAccess Services Authentication Options	UAG DirectAccess uses certificates to help secure the connection between remote clients and the internal network. Browse and select a root or intermediate certificate that verifies certificates sent by DirectAccess clients. Use root certificate DC=local, DC=CN=RootCA Browse Select the certificate that authenticates the UAG DirectAccess server to a client connecting using IP-HITPS. CN=DirectAccess.b Browse The IP-HITPS certificate should be copied to all members of a UAG DirectAccess array. EditIPSec compto graphy settings Accept connections only from: Clients that log on using a PKI smart card Computers that comply with your organization's NAP policy	
Learn more	< Back Next > Finish	Cancel

Angabe der URL des NLS Server

ar Infrastructure Server Configur 💐	ation	×
Infrastructure Se	rver Configuration	
Network Location Server DNS Suffixes Management Servers and DCs	An internal network location server helps a dient computer to determine whether it is connected to the Internet or to the internal network.	
	Enter the HTTPS URL of the network location server. https:// Validate Example: insideoutside.corp.contoso.com It is recommended that you use a high availability network location server. If the HTTPS URL is unavailable, client connectivity may be disrupted.	
	Validation successful. The URL https://dimensionalistical is reachable.	
Learn more	< Back Next > Finish Ca	incel

Angabe der DNS Suffixe, welche vom DNS64 durch UAG dem DA Client zur Verfuegung gestellt werden. Die DNS Suffixe werden in die NRPT eingetragen, so dass der DA Client weiss, fuer welche DNS Domaenen er welche DNS Server verwenden soll.

💐 Infrastructure Server Configura	tion			x
Infrastructure Ser	ver Conf	iguration		
Network Location Server				
DNS Suffixes	Enterthe na	me suffixes and IP addresses o	f internal DNS servers used to resolve DNS suffix	queries.
Management Servers and DCs	Na	me Suffix	IP address of DNS Server	
	*.	No local	[DNS64]	
		History and Co cal	[Excluded]	
	*.4	local	[DNS64]	
	▶ * Doi	uble-click here to add		
	4	Name Resolution Servers	s used by DirectAccess	×
	Selecta lo C Only L Fall bi unrea C Fall bi	Select and enter a DNS suff DNS Suffix C Specif Example: corp.contoso.co Choose the DNS server to r UAG DNS64 server Do not use an internal O Other DNS server IPv4 a	fix or a single server (FQDN): ic Server m resolve DNS suffix queries: DNS server for the specified server or suffix, address(es):	-
Learn more				ish Cancel
e Time Message Type	Overview of Dir Prerequisites fc Message		OK Cancel	Disable

Angabe der Infrastruktur Server, welche ueber den ersten IPSEC Tunnel mit dem DA-Client kommunizieren koennen. Hierbei handelt es sich um Domaenencontroller, Virenscanner, Softwareverteilungsserver usw.

💐 Infrastructure Server Configura	ition 🔀
Infrastructure Ser	ver Configuration
Network Location Server DNS Suffixes Management Servers and DCs	List all internal servers that are required to manage and authenticate DirectAccess clients.
Learn more	< Back Next > Finish Cancel

Beispiel:

a Infrastructure Server Configura	tion			X
Infrastructure Ser	ver Configuration			
Network Location Server	List all internal servers that are req	uired to manaq	e and authenticate DirectAccess clients.	
DNS Suffixes		- Pefrech	📑 Add Server 📼 🗙	Select All
Management Servers and DCs	Access Enabling Groups: Domains Domains Coal	st refreshed on	Servers List:	
Learn more			< Back Next >	Finish Cancel

Der Zugriff auf einzelne Server im LAN kann zusaetzlich noch verschluesselt und authentifiziert werden, wenn das gewuenscht ist. Wird keine Aenderung vorgenommen, werden die Verbindungen zwischen DirectAccess Client und Forefront UAG Server authentifiziert und verschluesselt (kerberos, Computer Zertifikate, NTLMv2, AES192, DH Gruppe 2 usw.).

Application Server Configuration	×
Application Server Configuration	
By default, traffic between DirectAccess clients and the UAG DirectAccess serve You can also enable authentication and encryption between clients and specifi	er is authenticated and encrypted (end-to-edge). ed applications servers (end-to-end).
Select an authentication and encryption model: Require end-to-edge authentication and encryption Require end-to-end authentication and encryption to specified application	servers
EditIPSec cryptography settings Select the security groups that contain the servers that require end-to-end aut	hentication and
	Add Remove
Learn more	Finish Cancel

Konfig sichern und aktivieren

Group Policy erstellen lassen

Forefront UAG DirectAccess Configural	ion Review	_ 🗆 🗙
Forefront UAG Direct/	Access Configuration Review	A.
🐙 Clients		^
Connectivity and security	policies will be applied to the following security group(s).	
🥾 CG-DirectAccess		
DirectAccess Server		
The following connection and se internal network.	ecurity policies will be enabled between remote client computers and the	
 '217. 212' will connect '10.80.20.29' will connect The internal network sub The root certificate to wh DC=local, DC=tor, CN=R The certificate that the Di CN=DirectAccess of the of Smart card authentication Infrastructure Servers (The HTTPS URL that prov https://DirectAccess should be directed to the 	ect the DirectAccess server to the Internet. : the DirectAccess server to the internal network. het is 2002:4907:8004:8000::/49 ich remote clients chain is: !aotCA rectAccess server uses for HTTPS is: Executed: In is not required. DNS, DC, Management) ides clients with location information is: cal/ will use the following DNS suffixes to determine which DNS queries internal DNS servers:	
Name Suffix	IB/6 Address of DNS Server	
	2002:d907:80d5:::	
essite state of the second		
	2002:d907:80d5:: #ddiated	
	2002:d907:80d5:: ::::::::::::::::::::::::::::::::::	
 Local name resolution op Client computers will fall DNS servers are unreach 	ition: back to local name resolution if the name does not exist in DNS or if the able when the client computer is on a private network.	-
Learn more	Apply Now Print Review Export Script	Cancel

Fuer die angegebenen Server werden auf den internen DNS Servern Ipv6 Adressen erstellt.

Management server	s on the following subnet(s) will be able	to connect to remote client computer:
Server	IP Address/Prefix	
SRV- M - Notal iocal	2002:d907:80d4:8001::a50:1402 2002:d907:80d4:8000:0:5efe:10.80.20.2	
SRV (SPD- SRV (Sphine).local	2002:d907:80d4:8001::a50:1403 2002:d907:80d4:8000:0:5efe:10.80.20.3	
SRV-WE-	2002:d907:80d4:8001::a50:1502 2002:d907:80d4:8000:0:5efe:10.80.21.2	
SRV-WE-	2002:d907:80d4:8001::a50:1503 2002:d907:80d4:8000:0:5efe:10.80.21.3	
	Romer Real ocal	
SRV- SHV -	2002:d907:80d4:8001::a50:1002 I 2002:d907:80d4:8000:0:5efe:10.80.16.2	
SRV-Bar-	2002:d907:80d4:8001::a50:1003 I 2002:d907:80d4:8000:0:5efe:10.80.16.3	
SRV-X400 BRX400004400.loca	2002:d907:80d4:8001::a50:1202 I 2002:d907:80d4:8000:0:5efe:10.80.18.2	
SRV-WAR-	2002:d907:80d4:8001::a50:1203 I 2002:d907:80d4:8000:0:5efe:10.80.18.3	
	and the second s	
SRV CAN AND	2002:d907:80d4:8001::a50:2 2002:d907:80d4:8000:0:5efe:10.80.0.2	
SRV	2002:d907:80d4:8001::a50:3 2002:d907:80d4:8000:0:5efe:10.80.0.3	
SRV- 440 - Setting with the will be ca	2002:d907:80d4:8001::a50:802 I 2002:d907:80d4:8000:0:5efe:10.80.8.2	
SRV-) Min k- Definition wildow	2002:d907:80d4:8001::a50:803 2002:d907:80d4:8000:0:5efe:10.80.8.3	
	Anti-Virus Updates	
srvetter	2002:d907:80d4:8001::a50:1406	
Materia local	2002:d907:80d4:8000:0:5efe:10.80.20.6	

WICHTIG: Ipv6 muss in den NIC Eigenschaften der Domaenencontroller aktiviert sein. Es reicht, das Kontrollkaestchen fuer Ipv6 wieder zu aktivieren, ein Reboot ist nicht erforderlich.

Angelegte DNS Eintraege in den DNS Zonen

	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1402
📗 🗐 (identisch mit übergeordnete	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1403
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1405
srv-l	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1407
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1409
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:140a
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:140f
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1410
srv-l	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1414
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1415
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1417
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:141d
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:141e
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:141f
🗐 (identisch mit übergeordnete	IBv6 Host (AAAA)	2002;d907;80d4;8000;0000;5efe;0a50;1002
	IPv6 Host (AAAA)	
		200210907180041800010000156Fe10a5011006
SRV.	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b
	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013
	IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1015
	IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:3907:8034:8000:0000:5efe:0a50:1005 2002:3907:8034:8000:0000:5efe:0a50:1005 2002:3907:8034:8000:0000:5efe:0a50:1013 2002:3907:8034:8000:0000:5efe:0a50:1015 2002:3907:8034:8000:0000:5efe:0a50:101c
SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1015 2002:d907:80d4:8000:0000:5efe:0a50:101d
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1016 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1016 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:101f
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1016 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:1022 2002:d907:80d4:8000:0000:5efe:0a50:1022
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1015 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:1022 2002:d907:80d4:8000:0000:5efe:0a50:1023 2002:d907:80d4:8000:0000:5efe:0a50:1023
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1015 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:1022 2002:d907:80d4:8000:0000:5efe:0a50:1023 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1015 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:1022 2002:d907:80d4:8000:0000:5efe:0a50:1023 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1016 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:1022 2002:d907:80d4:8000:0000:5efe:0a50:1023 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1026 2002:d907:80d4:8000:0000:5efe:0a50:1026 2002:d907:80d4:8000:0000:5efe:0a50:1026
SRV- SRV- SRV- SRV- SRV- SRV- SRV- SRV-	IPv6 Host (AAAA) IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006 2002:d907:80d4:8000:0000:5efe:0a50:100b 2002:d907:80d4:8000:0000:5efe:0a50:1013 2002:d907:80d4:8000:0000:5efe:0a50:1016 2002:d907:80d4:8000:0000:5efe:0a50:101d 2002:d907:80d4:8000:0000:5efe:0a50:101f 2002:d907:80d4:8000:0000:5efe:0a50:1022 2002:d907:80d4:8000:0000:5efe:0a50:1023 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1024 2002:d907:80d4:8000:0000:5efe:0a50:1026 2002:d907:80d4:8000:0000:5efe:0a50:102b 2002:d907:80d4:8000:0000:5efe:0a50:102b 2002:d907:80d4:8000:0000:5efe:0a50:1046 2002:d907:80d4:8000:0000:5efe:0a50:1046

Ipv6 Adresse eines DNS Server (DC). Man beachte die Kombi Ipv4 und Ipv6 Adresse

Eigenschaften von 🌨 local	? ×
Host (AAAA) Sicherheit	
Host (bei Nichtangabe wird übergeordnete Domäne verwendet):	
(identisch mit übergeordnetem Ordner)	
Vollqualifizierter Domänenname:	
IP-Adresse:	_
2002:d907:80d4:8000:0:5efe:10.80.20.2	_
Entsprechenden Zeigereintrag (PTR) aktualisieren	
OK Abbrechen Überne	hmen

Ggfs. Ipv6 Einstellungen auf den DNS Servern aktualisieren (nach DA Aktivierung)

sc control iphlpsvc paramchange

Erstellte GPO und Erlaeuterung

Gruppenrichtlinie UAG DirectAccess - DA Server

GPO-Status

Benutzereinstellungen deaktiviert

Richtlinie

Richtlinienversion Statusbehaftetes FTP deaktivieren Statusbehaftetes PPTP deaktivieren IPsec-Ausnahme IPsec über NAT Verschlüsselung des vorinstallierten Schlüssels SA-Leerlaufzeit Sichere Zertifikatsperrlistenprüfung Private Profileinstellungen<u>hide</u>

Richtlinie

Firewallstatus Eingehende Verbindungen Ausgehende Verbindungen Lokale Firewallregeln anwenden Lokale Verbindungssicherheitsregeln anwenden Benachrichtigungen anzeigen Unicast-Antworten zulassen Verworfene Pakete protokollieren Erfolgreiche Verbindungen protokollieren Protokolldateipfad Maximale Größe der Protokolldatei (KB) Öffentliche Profileinstellungen<u>hide</u> **Richtlinie**

Firewallstatus Eingehende Verbindungen Ausgehende Verbindungen Lokale Firewallregeln anwenden Lokale Verbindungssicherheitsregeln anwenden Benachrichtigungen anzeigen Unicast-Antworten zulassen Verworfene Pakete protokollieren Erfolgreiche Verbindungen protokollieren Protokolldateipfad Maximale Größe der Protokolldatei (KB) Verbindungssicherheitseinstellungen<u>hide</u> Regelnhide

Einstellung

2.10 Nicht konfiguriert Nicht konfiguriert ICMP Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Fehler bei Sperren des Zertifikats.

Einstellung

Ein

Nicht konfiguriert Nicht konfiguriert

Einstellung

Ein

Nicht konfiguriert Nicht konfiguriert

Name

UAG DirectAccess Gateway -
Clients Access Enabling Tunnel
- AllPolicies to enable access granting resources(DC, DNS, NAP,
etc.) over IPsec. Generated on Tuesday, 03 August 2010 14:15
UTC.

Wahr Eingehend und ausgehend erforderlich 2002:d907:80d4:8001::a50:1402, 2002:d907:80d4:8000:0:5efe:10.80.20.2, 2002:d907:80d4:8001::a50:1403, 2002:d907:80d4:8000:0:5efe:10.80.20.3, 2002:d907:80d4:8001::a50:1502, 2002:d907:80d4:8001::a50:1503, 2002:d907:80d4:8001::a50:1503, 2002:d907:80d4:8001::a50:1003, 2002:d907:80d4:8001::a50:1002, 2002:d907:80d4:8001::a50:1002, 2002:d907:80d4:8000:0:5efe:10.80.16.2
2002:d907:80d4:8001::a50:1003, 2002:d907:80d4:8000:0:5efe:10.80.16.3, 2002:d907:80d4:8001::a50:1202, 2002:d907:80d4:8000:0:5efe:10.80.18.2, 2002:d907:80d4:8001::a50:1203, 2002:d907:80d4:8001::a50:1203,
2002:d907:80d4:8000:0:5efe:10.80.18.3, 2002:d907:80d4:8001::a50:2, 2002:d907:80d4:8000:0:5efe:10.80.0.2, 2002:d907:80d4:8001::a50:3, 2002:d907:80d4:8000:0:5efe:10.80.0.3, 2002:d907:80d4:8001::a50:802, 2002:d907:80d4:8001::a50:803, 2002:d907:80d4:8001::a50:803, 2002:d907:80d4:8001::a50:1406, 2002:d907:80d4:8001::a50:1406, 2002:d907:80d4:8001::a50:1402, 2002:d907:80d5::d907:80d5
Beliebig Beliebig {C3D8F907-29F8-4356-A64C-570950685CC5}
{DD5FBEF2-4438-4CEC-81C4-169B50E66418} {7487C8D9-E9E5-4C1D-9012-3166FFEDCB49} Beliebig Privat, Öffentlich Beliebig Beliebig Beliebig

Aktiviert

Authentifizierungsmodus

Endpunkt 1

Endpunkt 2 Endpunkt 1 (Port) Endpunkt 2 (Port)

Erste Authentifizierung

Zweite Authentifizierung

Datenschutz

Protokoll Profil Tunnelendpunkt 1 Tunnelendpunkt 2 Netzwerkschnittstellentyp Erste Authentifizierung

Integritätszertifikat

Zweite Authentifizierung

Wahr Eingehend und ausgehend erforderlich 2002:d907:80d4:800 0::/49 Beliebig Beliebig Beliebig {EA98A748-D882-491C-958D-9ACE7395FEB0} {5A830407-7E7E-4943-9F81-90BB65F71061} {F98D74C6-8DD6-410B-A372-E66CDA8DDD61} Beliebig Privat, Öffentlich Beliebig

Beliebig Beliebig

Beschreibung

Beschreibung

Name

UAG DirectAccess Gateway - Clients Access Enabling Tunnel - All - Phase 1Auth Set {C3D8F907-29F8-4356-A64C-570950685CC5}VersionAuthentifizierungComputerzertifikatZertifizierungsstelleDC=local, DC=xxx, CN=RootCAZertifizierungsstellenzuordnungAusgeschlossene ZertifizierungsstelleIntegritätszertifikatFalschFalsch

Name

UAG DirectAccess Gateway - Clients Corp Tunnel - Phase 1 Auth Set{EA98A748-D882-491C-958D-9ACE7395FEB0}Version2.10AuthentifizierungComputerzertifikatZertifizierungsstelleDC=local, DC=xxx, 0ZertifizierungsstellenzuordnungFalschAusgeschlossene ZertifizierungsstelleFalsch

DC=local, DC=xxx, CN=RootCA Falsch Falsch Falsch

NameBeschreibungUAG DirectAccess Gateway - Clients Corp Tunnel - Phase 2 Auth Set
{5A830407-7E7E-4943-9F81-90BB65F71061}
Version2.10Version2.10AuthentifizierungBenutzer (Kerberos)Beschreib

ung

UAG DirectAccess Gateway - Clients Access Enabling Tunnel - All - Phase 2 Auth Set {DD5FBEF2-4438-4CEC-81C4-169B50E66418} Version 2.10 Authentifizierung Benutzer-NTLM Schlüsselaustausch (Hauptmodus)

Name	Beschreibung
Standardsatz	
Version	2.10
Schlüsselgültigkeitsdauer (in Minuten)	60
Schlüsselgültigkeitsdauer in Sitzungen	0
Version überspringen	2.0
Schlüsselaustausch	Diffie-Hellman-Gruppe 2
Verschlüsselung	AES-128
Integrität	MD5
Version überspringen	0.0
Schlüsselaustausch	Diffie-Hellman-Gruppe 2
Verschlüsselung	AES-128
Integrität	SHA-1
Version überspringen	0.0
Schlüsselaustausch	Diffie-Hellman-Gruppe 2
Verschlüsselung	3DES
Integrität	SHA-1
Datenschutz (Schnellmodus)	

Na	me	Beschreibung
UAG DirectAccess Gateway - Clients Ac	ccess Enabling Tunnel - Al	l - Phase 2
Crypto Set {7487C8D9-E9E5-4C1D-901	2-3166FFEDCB49}	
Version	2.10	
Perfect Forward Secrecy	Deaktiviert	
Version überspringen		0.0
Protokoll		ESP
Verschlüsselung		AES-192
ESP-Integrität		SHA-1
Schlüsselgültigkeitsdauer (in Minuten)		60
Schlüsselgültigkeitsdauer (in Kilobyte)		100000

Name Beschreibung UAG DirectAccess Gateway - Clients Corp Tunnel - Phase 2 Crypto Set {F98D74C6-8DD6-410B-A372-E66CDA8DDD61} Version 2.10 Perfect Forward Secrecy Deaktiviert Version überspringen 0.0 Protokoll ESP Verschlüsselung AES-192 ESP-Integrität SHA-1 Schlüsselgültigkeitsdauer (in Minuten) 60 Schlüsselgültigkeitsdauer (in Kilobyte) 100000 Benutzerkonfiguration (Deaktiviert)hide Keine Einstellungen definiert

Gruppenrichtlinie UAG DirectAccess - Client

NLS

reich D)etails	Einstellungen	Delegierung			
		Die Liste so Leerzeicher Beispiel: fe80::/9,fe8	llte durch Komn n aufweisen. 11::/9	nas getrennt sein ur	nd keine zusätzlichen	
	R	ichtlinie		Einstellung	Kommentar	
	T D	esthostadresse NS	für Firmen-	Aktiviert		
		Testadresse Geben Sie o den zu teste Beispiel: 2001:4898:	e für Firmen-DN die erwartete DI enden Firmenho 28:3:38a1:c31:	S: NS-Adresse für Istnamen an. 7b3d:bf0	::1	
	R	ichtlinie		Einstellung	Kommentar	
	Т	esthostname für Testhostnar Geben Sie e Testen der I Beispiel: ncsi.corp.mi	Firmen-DNS me des Firmen-f einen aufzulöse Unternehmensk icrosoft.com	Aktiviert DNS: nden Firmenhostna sonnektivität an.	UAGDirectAccess- corpConnectivityHost.	
	B	ichtlinie		Einstellung	Kommentar	
	U D	RL zur Bestimm omänenorts	ung des	Aktiviert		
		URL zur Be Firmendomä Geben Sie o	stimmung des inenorts: die HTTPS-URI	_ der Firmenwebsite	https:// diabagegegedia l.local/ an,	
		um den Dor Beispiel: https://nid.c	nänenort inner- corp.microsoft.c	oder außerhalb zu (:om/	ermitteln.	
	Netzw	erk/TCP/IP-	Einstellunger	//Pv6-Obergang	jstechnologien	<u>sho</u>
	Zusät	zl. Regeinst				show

NRPT fuer den DA Client

🗐 Group Policy Management E	ditor								
File Action View Help									
🗢 🔿 🖄 📅 🛛 🗊									
Administrative T Policies Windows Setting Windows Setting Windows Setting Windows Setting Name Resolu Scripts (Star Administrative T Policies Policie Pol	The Name Resolution Pol You can use this page to Learn more about DNSSE Description Name Resolution Policy object (GPD) that contains the policy information found in the Name Resolution Policy Table (NRPT).		licy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and Direct Access on DNS client computers. create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (DU). ic on the Web Create Rules To which part of the namespace does this rule apply? Suffix Certification authority: (Dptional) DNSSEC DNS settings for Direct Access Image: Comparison of the compa						client computers. ational unit (OU). Browse
							Undate	Create	
	Name Resolution P	'olicy Ta	ble					Advanced Gl	obal Policy Settings
	Namespace D	A	DNSSEC IV	DNSSEC (I	DNSSEC (I	Direct Acce	Direct Acce	Direct Acce	Direct Acce
	. State Di	C=lo				2002:d907:		No	
	www.bullet.vD	C=lo						No	
	local D	C=lo				2002:d907:		No	
	antanii Diocal Di	C=lo				2002:d907:		No	
								Delete Rule	Edit Rule
•								Apply	Cancel

Namespace

UAG DirectAccess: Client{3491980e-ef3c-4ed3-b176-a4420a810f12}

Bereich Details Einstellungen Delegierung

on oton angon	
amespace	
Real provide	
Richtlinie	Wert
Namespace	sin ilocal
Zertifizierungsstelle	DC=local, DC=b
Konfiguration	Direktzugriff
DNSSEC (Überprüfung)	Nicht konfiguriert
DNSSEC (IPsec)	Nicht konfiguriert
DNSSEC (IPsec-Verschlüsselung)	Nicht konfiguriert
Direktzugriff (IPsec)	Nein
Direktzugriff (IPsec-Verschlüsselung)	Keine Verschlüsselung (nur Integrität)
Direktzugriff (Proxyeinstellungen)	Keinen Webproxy verwenden
Direktzugriff (Webproxy)	Leer
Direktzugriff (DNS-Server)	2002:d907:80d5::d907:80d5
Version	1
.local	
Richtlinie	Wert
Namespace	Alternation and Alternation local
Zertifizierungsstelle	DC=local, DC= him CN=RootCA
Konfiguration	Direktzugriff
DNSSEC (Überprüfung)	Nicht konfiguriert
DNSSEC (IPsec)	Nicht konfiguriert
DNSSEC (IPsec-Verschlüsselung)	Nicht konfiguriert
Direktzugriff (IPsec)	Nein
Direktzugriff (IPsec-Verschlüsselung)	Keine Verschlüsselung (nur Integrität)
Direktzugriff (Proxyeinstellungen)	Keinen Webproxy verwenden
Direktzugriff (Webproxy)	Leer
Direktzugriff (DNS-Server)	Leer
Version	1
Richtlinie	Wert
Namespace	local
Zertifizierungsstelle	DC=local, DC= lease CN=RootCA
Konfiguration	Direktzugriff
DNSSEC (Überprüfung)	Nicht konfiguriert
DNSSEC (IPsec)	Nicht konfiguriert
DNSSEC (IPsec-Verschlüsselung)	Nicht konfiguriert
Direktzugriff (IPsec)	Nein
Direktzugriff (IPsec-Verschlüsselung)	Keine Verschlüsselung (nur Integrität)
Direktzuariff (Proxyeinstellungen)	Keinen Webproxy verwenden

WICHTIG: Den TEREDO Adapter per GPO auf "Enterprise Client" setzen, damit in einem Domain Managed Network zuerst Teredo verwendet und nicht auf IP-HTTPS geschwenkt wird:

http://blogs.technet.com/b/edgeaccessblog/archive/2010/05/21/directaccess-andteredo-adapter-behavior.aspx

Connection Security Rules fuer die DirectAccess Clients



UAG DirectA	ccess Client - Clients Access Enabling Tunnel - All Pro 🔀
General Co	omputers Protocols and Ports Authentication Advanced
()	This rule contains properties that are not supported through this interface.
General	
	Name: G DirectAccess Client - Clients Access Enabling Tunnel - Al)
	Description:
	Policies to enable access granting resources(DC, DNS, AP, etc.) over IPsec. Generated on Tuesday, 03 August 2010 14:15 UTC.
	C Enabled
	OK Cancel Apply

UAG DirectAccess Client - Clients Access Enabling Tunnel - All Pro 💌
General Computers Protocols and Ports Authentication Advanced
Endpoint 1
C These IP addresses:
Add
Edit
Remove
Endpoint 2
Any IP address These IP addresses:
2002:d907:80d4:8001::a50:140 Add 2002:d907:80d4:8000:0:5efe:1 Add
2002:d907:80d4:8000:0:5efe:1(2002:d907:80d4:8001::a50:150 2002:d907:80d4:8000:0:5efe:1(▼ Remove
Learn more about computer endpoints
OK Cancel Apply

USC DirectOccess Client - Clients Occess En	abling Tuppel - All Pro			Enabled	Endpoint 1	Endpoint 2	Authentication mo
ONG DIRECTACCOS CIENC CIENCS ACCOS EN		lient - Clients Access Enabling Tunnel -	- All	Yes	Any	2002:d907	Require inbound a
General Computers Protocols and Ports Aut	hentication Advanced	lient - Clients Corp Tunnel		Yes	Any	2002:d907	Require inbound (
Specify how and when authentication is perfor	med between computers.	Llient - Exempt NLA		Yes	2002:d907	2002:d907	Do not authentica
- Bequirements							
Authentication mode:							
Require inbound and outbound	_						
Method							
C Default C Computer and user (Kerberos V	51						
C Computer (Kerberos V5)	Tomize Aduanced Authentic	ation Mothods					V
C User (Kerberos V5)	tomize Auvanceu Authentit	ation Methous					
	First authentication		Seco	ond authenticat	ion		
Mavancea.	Specify computer authenticatio negotiations. Those higher in t	n methods to use during IPsec he list are tried first.	Spe duri	cify user authe ng IPsec negot	ntication methods iations. Those hi	or a health certif gher in the list are	ficate to use e tried first.
	First authentication methods:		Sec	ond authentica	tion methods:		
	Method Add	itional Information	M	ethod	Additiona	I Information	
Learn more about authentication	Computer certificate Roc	t CA, RSA Certificate S	Us	ser (NTLMv2)			
UK		<u>~</u>					^
🛨 🔚 Advanced Audit Policy Config							
🗉 🎳 Policy-based QoS		<u> </u>					
🕀 🧮 Administrative Templates: Policy defir							
Preferences							
Policies	J						
Preferences	Add Edit	Remove		Add	Edit	Remove	
	First authentication is optio	nal		Second auther	ntication is option	al	
			A se key	econd authentio is in the first au	ation cannot be thentication meth	specified when a ods list.	preshared
Le	earn more about authentication s	ettinas					
	/hat are the default values?						
						ОК	Cancel

IPSEC Endpunkte

HAG DirectAccess Client - Clients Access Enabling Tunnel - All Pro	X	Enabled	Endpoint 1
	Client - Clients Access Enabling Tunnel - All	Yes	Any
General Computers Protocols and Ports Authentication Advanced	Lient - Clients Corp Tunnel	Yes	Any
D-0-	Elient - Exempt NLA	Yes	2002:d907
Profile Specify profiles to which this rule applies.	Customize IPsec Tunneling Settings		×
	Connections from Endpoint 1 to Endpoint 2 will pass th tunnel endpoints. Tunnel endpoints are generally gate	rough the sp way servers.	eched
	Note: When IPsec tunneling is used, the authenticatio "Require inbound and outbound" or "Require inbound (for gateway devices).	n mode mus and clear o	t be set to utbound''
Interface types			
Specify the interface types to which this rule Customize	V Use IPsec tunneling		
	E Exempt IPsec protected connections		
Specify whether IPsec tunneling should be used.	Local tunnel endpoint (closest to Endpoint 1):		
	IPv4: JAny	E dit.	
	IPv6: Any		
	Remote tunnel endpoint (closest to Endpoint 2):		
Learn more about these settings	IPv4:	E dit.	
OK Cancel Apply	IPv6: 2002:d907:80d5::d907:80d5		
Advanced Audit Policy Configuration Jy Policy-based Qo5 Administrative Templates: Policy definitions (ADMX	Learn more about IPsec tunneling		
Preferences User Configuration Policies	ОК		Cancel

NLA Ausnahmen fuer NLS Server

UAG DirectAccess Client - Exempl	NLA Properties	X
General Computers Protocols and	Ports Authentication Advanced	_
Protocols and ports		
Protocol type:	TCP	
Protocol number:	6 🛨	
Endpoint 1 port:	All Ports	
	J Example: 80, 445, 5000-5010	
Endpoint 2 port:	Specific Ports	
	443	
	Example: 80, 445, 5000-5010	
Learn more about protocol and por	<u>ts</u>	
	DK Cancel Apply	

Computerzertifikat fuer Windows 7 Client

Fuer die DA Clients muss ein Computerzertifikat der vertrauenswuerdigen Zertifizierungsstelle ausgestellt werden, welche auch von Forefront UAG und dem NLS verwendet wird.

CN = Interner DNS FQDN der Clients

Ueberpruefung der Ipv6 Konnektivitaet auf dem UAG Server

Host Name	. : SRV-xxx-xxx
Primary Dns Suffix	: xxx.local
Node Type	: Hybrid
IP Routing Enabled	: Yes
WINS Proxy Enabled	: No
DNS Suffix Search List	: xxx.local

Ethernet adapter Local Area Connection:

Media State: Media disconnected Connection-specific DNS Suffix .: Description: SSL Network Tunneling Physical Address.....: 00-FF-08-01-19-47 DHCP Enabled....: Yes Autoconfiguration Enabled: Yes

Ethernet adapter INTERNAL:

	Connection-specific DNS Suffix .: xxx.local
	Description : Broadcom BCM5708S NetXtreme II GigE (NDIS VBD
(Client)
	Physical Address : 00-1A-64-32-7C-28
	DHCP Enabled : No
	Autoconfiguration Enabled : Yes
	Link-local IPv6 Address : fe80::114e:2cc8:f287:ed65%11(Preferred)
	IPv4 Address : 10.80.20.29(Preferred)
	Subnet Mask : 255.255.255.0
	Default Gateway :
	DHCPv6 IAID
	DHCPv6 Client DUID: 00-01-00-01-13-E8-71-9E-00-1A-64-32-7C-28
	DNS Servers
	10.80.20.3
	NetBIOS over Tcpip : Enabled

Ethernet adapter EXTERNAL:

Connection-specific DNS Suffix .: Description: Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Client) #2 Physical Address.: 00-1A-64-32-7C-26 DHCP Enabled.: No Autoconfiguration Enabled: Yes Link-local IPv6 Address: fe80::d5e0:d210:51c2:7422%12(Preferred) IPv4 Address.: 217.x.xxx.212(Preferred) Subnet Mask: 255.255.255.240 IPv4 Address.: 217.x.xxx.213(Preferred) Subnet Mask: 255.255.255.240 IPv4 Address.: 217.x.xxx.213(Preferred) Subnet Mask: 255.255.255.240 IPv4 Address.: 217.x.xxx.213(Preferred) Subnet Mask: 255.255.255.240 Default Gateway: 217.x.xxx.217 DHCPv6 IAID : 301996644 DHCPv6 Client DUID. : 00-01-00-01-13-E8-71-9E-00-1A-64-32-7C-28 DNS Servers : fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1 NetBIOS over Tcpip. : Disabled

Tunnel adapter 6TO4 Adapter:

Tunnel adapter Local Area Connection* 9:

Connection-specific DNS Suffix .: Description: Teredo Tunneling Pseudo-Interface Physical Address.....: 00-00-00-00-00-00-00-E0 DHCP Enabled....: No Autoconfiguration Enabled: Yes Link-local IPv6 Address: fe80::8000:f227:26f8:7f2b%13(Preferred) Default Gateway: NetBIOS over Tcpip.....: Disabled

Tunnel adapter isatap.xxx.local:

Tunnel adapter isatap.{C36EA179-74B6-4982-A670-1866E35A968F}:

Connection-specific DNS Suffix .: Description: Microsoft ISATAP Adapter #2 Physical Address. : 00-00-00-00-00-00-00-E0 DHCP Enabled. : No Autoconfiguration Enabled . . . : Yes Link-local IPv6 Address . . . : fe80::200:5efe:217.7.128.212%17(Preferred) Link-local IPv6 Address . . . : fe80::200:5efe:217.7.128.213%17(Preferred) Default Gateway : fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1 NetBIOS over Tcpip. : Disabled

Tunnel adapter IPHTTPSInterface:

Connection-specific DNS Suffix .:
Description : IPHTTPSInterface
Physical Address : 00-00-00-00-00-00-E0
DHCP Enabled : No
Autoconfiguration Enabled : Yes
IPv6 Address : 2002:d907:80d4:8100:44ca:3c67:31f2:48c4(Preferred)
Link-local IPv6 Address : fe80::44ca:3c67:31f2:48c4%18(Preferred)
Default Gateway :
NetBIOS over Tcpip : Disabled

Tunnel adapter isatap.{BCE2BA7D-B251-480A-97C6-24DECBFC7FFC}:

Media State : Media disconnected Connection-specific DNS Suffix .: Description : Microsoft ISATAP Adapter #3 Physical Address..... : 00-00-00-00-00-00-E0 DHCP Enabled..... : No Autoconfiguration Enabled : Yes

Troubleshooting

DirectAccess Troubleshooting Assistant http://www.microsoft.com/downloads/details.aspx?FamilyID=9A87EFE8-E254-4473-8A26-678ADEA6D9E9&displaylang=en

MICROSOFT DIRECTACCESS CONNECTIVITY ASSISTANT	
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft	
• undates	-
ution	These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

Brille aufsetzen



DA Assistant – GPO Einstellungen



Die moeglichen Einstellungen sind in dem DA Assistenten Word Dokument erlaeutert



Client Experience

Alles Gut, always on 🙂

