Die Informationen in diesem Artikel beziehen sich auf:

? Microsoft ISA Server 2004

Einleitung

Der ISA 2004 bietet als erste Firewall Lösung von Microsoft die Möglichkeit, eine Benutzer Authentifizierung für das Regelwerk über eine RADIUS (Remote Access Dial In Service) Verbindung einzurichten.

Die Microsoft Implementierung von RADIUS nennt sich IAS (Internet Authentication Service) und steht unter Windows 2000 und 2003 für alle Windows Versionen (Ausnahme Windows 2003 Web Editon), zur Verfügung.

Nachteile der IAS Authentifizierung mit dem ISA Server 2004

- ? RADIUS Traffic ist per Default unverschlüsselt. Die Verwendung von IPSEC wird empfohlen
- ? Bei jedem matchen der Regel muss RADIUS den Client reauthentifizieren, was bei ausgelasteten Servern mehr Netzwerk- und Verarbeitungslast erzeugt.
- ? ISA enthält nicht sehr viele Informationen im RADIUS Acces-Request Paket, so dass eine Unterscheidung zwischen ISA und anderen Diensten sehr schwer ist, wenn alle auf derselben Maschine laufen.

Hinweis:

Webbowser verstehen kein RADIUS als Authentifizierungstyp, so dass der ISA Server 2004 den Clint auffordert sich per Basic Authentication zu identifizieren. ISA packt diese Pakete in ein RADIUS Access Request Paket und sendet diese zum ausgewählten RADIUS Server.

Warum RADIUS/IAS

Ein ISA 2004 Server befindet sich in der Regel in einer DMZ (DeMilitarisierten Zone). Dabei handelt es sich um einen Hochsicherheitsbereich welcher nur die notwendigsten Verbindungen zwischen LAN und WAN (Internet etc.) herstellen soll.

Aus diesem Grund implementiert man einen ISA Server 2004 als Firewall Lösung nicht in das interne Netzwerk – sprich, der ISA Server 2004 wird **KEIN** Mitglied der Domäne. Eine Ausnahme von der Regel ist ein ISA 2004 Server als reine Proxy Lösung. Dort befindet sich der ISA Server 2004 hinter einer anderen ISA 2004 Firewall oder Third Party Firewall und kann so Mitglied der Domäne sein, um z. B. über die integrierte Windows Authentifizierung ein Regelwerk für den Webzugriff abzubilden.

Die Benutzerseite

Stellen Sie sicher, dass die Benutzer eine RAS Einwahlberechtigung haben. Es handelt sich hierbei zwar um keine RAS Einwahl, aber mit diesem Schalter teilen Sie mit, dass jetzt RAS Richtlinien und IAS Richtlinien verwendet werden können, welche ja für den ISA Server 2004 Zugriff über RADIUS erforderlich sind.

1 C	
Sicheheit Ungebung	Sitzungen
Renoteuberwachung Terminaktiens Allgemein Acteuse Konto Pooli Ru Veröllentlichte Zetriikate Nitglied von	tprofile DOM+ utnummern Organisation Einwichten Objekt
PAS-Beechtigung (Einwählen oder VPN) Qugilf gestatten Qugilf gestatten Qugilf gewegen Qugilf über PAS-Richtinen steuent	
Synulok ennung volitiseren Rickutoptonen Kein Bückut	
C Vgn Anufer textgelegt (nor fiR4S-Dienst)	
C Igner Rücknuf an	
Reficile (P.Adesse takesen Reficile Routen anvenden Definier zu ektivierende Routen für desse	Suborn Exam

Müssen Sie mehreren Benutzern den Zugriff auf Dienste über den ISA ermöglichen, so empfiehlt sich das Anlegen einer Benutzergruppe um dieser die entsprechenden Berechtigungen zu vergeben und die entsprechenden Benutzer zum Mitglied dieser Gruppe zu machen.

In unserem Beispiel verwenden wir die Gruppe WWW-Benutzer.

Installation der IAS Servers

Sie installieren den IAS Server wie jede Microsoft Komponente über Start – Systemsteuerung – Software – Windows Komponenten Hinzufügen / Entfernen. Gehen Sie dann in Netzwerkdienste und wählen dort *Internetauthentifizierungsdienst* aus.

indows-Komponenten Windows-Komponenten können hinzugefügt bzw. enternt werden.	C	Netzwerkdienste Ricken Sie auf die Kontrolkästchen der Komponenten, die hinzuge werden solen. Grau gefüllte Kästchen komponenten	lügt bow. entlemt , die nur zum Teil
Klicken Sie auf die Kontrolikärlichen der Komponenten, die hinzugefügt be werden pollen. Brau gefülte Kärtchen kennzeichnen Komponenten, die r installert werden. Klicken Sie auf "Detaile", um die Urterkomponenten ar	ow en fem I w zum Teil izuzeigen.	Installet welden. Kucken Sie auf "Detais", um die Unterkomponen Untergoniponenten von "Netzierkerkdienste", DHDP-Protokiol (Dynamic Host Configuration Protocol) Die BDS-Server (Domain Name System)	en arouzeigen. 0.0 MB 1,7 MB
Lonponenten:		🗹 👼 Einfache TCP/IP-Dienste	0,0 MB
Pindevidienet	0,0 MB	🗹 🛃 Internetauthentifizierungsdienst	0.0 MB
🗹 👷 Netzwerkdienste	2,6 MB	RFC-LberHTTP-Proxy	0,0 MB
🗖 🗔 🛃 Remoteinstallationscienste	2.0 MB	🗹 🌉 WINS (Windows Internet Name Service)	0,9 MB
🔲 🍠 Leminskerver	0.0 M8 🚽		CHERREN
Beschreibung: Einthält eine Vielzahl an spezialisierten, netzwerk bezogen Protokolien. Erforderlicher Speicherpfelz: 4.2 MB Verfügbarer Speicherpfelz: 6222,5 MB	en Diensten und	Beschreibung: Installieit einen DHCP-Server, der temporale IP Adl Clerkomputern im gleichen Netzwerk zuweid. Erfordarlicher Speicherplatz: 4,2 M8 Verfügberer Speicherplatz: 6222,5 M8	essen Detaist Abbreche

Nach erfolgter Installation des IAS müssen Sie diesen Server im Active Directory registrieren, damit der IAS berechtigt ist, Kontenanfragen über LDAP an das Active Directory zu richten.

Klicken Sie dazu in der IAS Konsole mit der rechten Maustaste auf Internetauthentifizierungsdienst und wählen im Kontextmenü Server im Active Directory registrieren aus.

🐤 Internetauthentifizier	ungsdienst		
Datei Aktion Ansicht	2		
Internetauthentifizierun Internetauthentifizierun ADJUS-Clients AS-Protokollierung RAS-Protokollierung	Dienst <u>s</u> tarten Dienst <u>b</u> eenden Server im Active Director	y registrieren	illkommen
E · 🚺 Verbindungsanforde	Ansicht		tauthentifizierungsdienst (IAS) kann für die erung, Autorisierung und Kontoführung von
Eigens	Eigens <u>c</u> haften		drahtlosen und Ethernet-Verbindungen mit dem erwendet werden. IAS kann ebenfalls für die
	Hilfe		g von Authentifizierungsanforderungen für fserver verwendet werden, der kompatibel mit
		RADIUS is Klicken Sie registriere von Benut Weitere Ir Bereitstellu in der Onli	t. im Menü "Aktion" auf "Server im Active Directory n", um den IAS zum Lesen der RAS-Eigenschaften zerkonten im Active Directory zu konfigurieren. iformationen über das Einrichten von IAS, ungsszenarios und Problembehandlung finden Sie nehilfe.

Erstellen des ISA 2004 Servers als IAS Client

Damit der ISA Server 2004 eine Benutzerauthentifizierung über RADIUS nutzen kann, müssen Sie den ISA Server als RADIUS Client einrichten. Hierzu sind zwei Schritte erforderlich. Der erste Schritt ist es im IAS einen neuen RADIUS Client zu erstellen. Klicken Sie dazu mit de rechten Maustaste in den Container *RADIUS-Client* und fügen einen neuen Client hinzu.

🞾 Internetauthentifizierungsdienst				
Datei Aktion Ansicht ?				
⇔ → 🖻 🖬 🗙 📽 💀 😫				
🦻 Internetauthentifizierungsdienst (Lokal)	Angezeigter Name	Adresse	Protokoll	Clienthersteller
	1 DLINK	192.9.200.114	RADIUS	RADIUS Standard
RAS-Protokollierung	15A2004	192.9.200.167	RADIUS	Microsoft
👾 🅰 RAS-Richtlinien 🗈 🦲 Verbindungsanforderungsverarbeitung	ISA-PRODUKTIV	192.9.200.240	RADIUS	RADIUS Standard

Sie müssen einen Namen für den neuen RADIUS Client angeben. Das muss nicht zwingend der NetBIOS / DNS Name des Clients sein, es handelt sich hierbei nur um den angezeigten Namen.

Als nächstes müssen Sie die IP Adresse oder den DNS Namen des RADIUS Client angeben und den Clienthersteller auswählen. Wir wählen als Clienthersteller *RADIUS Standard*.

igenschaften von IS	A-PRODUKTIV		? ×
Einstellungen			
Angezeigter <u>N</u> ame			
ISA PRODUKTIV			
Adresse (IP oder DN	S);		
192.9.200.240			
Veilaieren.			
Wenn Sie eine RAS Dients basiert, müss	Richtlinie verwenden, di en Sie den Hersteller de:	ie auf dem Herstellerati s RADIUS-Clients ange	bibut des eben
Dienthersteller	RADIUS Stendard		*
🗐 Antorderung mus	s das Allibut "Message	Authenticator" enthal	len
<u>G</u> emeinsener gehein	er Schlüssel:		_
Gemeinsamen gebei Schlizzei bestätigen	nen [nessa:		1
	DK	Abbrechen 01	garstman

Ein sehr wichtiger Punkt ist das so genannte *Shared Secret* – beim IAS *Gemeinsam geheimer Schlüssel* genannt.

Hier bei handelt es sich um eine Methode der Authentifizierung zwischen ISA Server und IAS Client. Ist der gemeinsam geheime Schlüssel identisch, erfolgt eine Kommunikation zwischen Server und Client.

Es wird die Verwendung eines sehr langen und kryptischen Schlüssels empfohlen. Die Qualität steht und fällt mit der Länge und Komplexität des Schlüssels. Ein brauchbarer Schlüssel wäre zum Beispiel: Xd5\$1"xSS(&aäsD03?Q.

Wichtig:

Bei der Vergabe des geheimen Schlüssels ist die Groß- und Kleinschreibung zu beachten.

Den hier gewählten Schlüssel müssen Sie später auch noch beim ISA Server verwenden, also merken Sie sich den Schlüssel gut *∠*

RAS Richtlinie

Erstellen Sie eine neue RAS-Richtlinie mit welcher Sie einer neu zu erstellen Active Directory Benutzergruppe *WWW-Benutzer* das Recht geben, den mit IP Adresse angegebenen ISA Server nutzen zu dürfen.

🦻 Internetauthentifizierungsdienst		
Datei Aktion Ansicht ?		
← → 🗈 📧 🗙 🖀 🗟 😤 ≁ 🔸		
Internetauthentifizierungsdienst (Lokal) RADIUS-Clients RAS-Richtlinien Verbindungsanforderungsverarbeitung	Name SISA2004 Eigenschaften von ISA2004 Einstellungen Geben Sie Bedingungen an, mit denen Verbindu übereinstimmen müssen. Bichtlinienbedingungen: Windows-Groups stimmen überein mit "BIGMAR NAS-IP-Address stimmen überein mit "192.9.200	Reih 1 rgsanforderungen CI\\w/w/w/-Benutzer'' AND 18''
	Hinzufügen Bearbeiten Entfernen Das zugewiesene Profil wird für diese Verbindung Verbindungsanforderungen mit den in der Richtlin Bedingungen übereinstimmen. Image: Comparison of the State	g übernommen, wenn nie angegebenen werk, solange keine utzerprofil angegeben sind. egebenen Bedingungen

Auf dem ISA Server

Auf dem ISA Server 2004 müssen Sie verschiedene Konfigurationsänderungen vor nehmen, damit der ISA eine Benutzerauthentifizierung über IAS durchführt.

Als erstes müssen Sie überprüfen ob die ISA Server 2004 Firewall Systemrichtlinie den RADIUS Zugriff auf das interne Netzwerk zulässt.

Starten Sie dazu die ISA Server Verwaltungskonsole und klicken Sie mit der rechten Maustaste auf *Firewallrichtlinie* und wählen im Kontextmenü *Systemrichtlinie bearbeiten* aus. Die Firewallrichtlinie ist per Default aktiviert ...



... mit Zugriff auf das Netzwerkobjekt Intern.

ystemrichtlinien-Editor				?
Konfigurationsgruppen	Allgemein Nach			
Netzwerkdienste DHCP DNS NTP Authentifizierungsdienste Active Directory RADIUS RSA SecurID CRL-Download Remoteverwaltung Microsoft Manageme	Diese Regel betrifft	Datenverkehr, der	an diese Ziele ges Hir Be	endet nzufügen agrbeiten
Terminalserver ICMP (Ping) Firewallclient Firewallclientinstallat Diagnosedienste ICMP Windows-Netzwerk Microsoft-Fehlerberik HTTP-Konnektivitäts	Ausnahmen:		Hir Be	n gufügen ea <u>r</u> beiten Egtfernen
			ОК	Abbrechen

Als nächstes müssen wir dem Netzwerkobjekt *Intern* mitteilen, dass ab sofort eine Authentifizierung der Benutzer erfolgen muss und die Authentifizierungsmethode RADIUS ist.

Starten Sie dazu die ISA Verwaltungskonsole und navigieren Sie über die *Konfiguration* zum Container *Netwerke* und wählen dort das Netzwerkobjekt *Intern* aus und gehen in dessen Eigenschaften.



Klicken Sie auf den Reiter *Webproxy* und wählen dort bei der zugelassenen Authentifizierungsmethode *Authentifizierung* aus.

Im nun erscheinenden Fenster wählen Sie die Authentifizierungsmethode Integriert (Standardmethode) ab und klicken stattdessen auf *RADIUS*.

Eigenschaften von Intern	Authentifizierung
Allgemein Adressen Domänen Webbrowser Automatische Erkennung Firewallclient Webproxy	Geben Sie die Authentifizierungsmethoden und -einstellungen an, die für die Authentifizierung von Clients, die eine Verbindung mit dem ISA Server-Computer herstellen, verwendet werden sollen. Hilfe über <u>Authentifizierung</u>
LTTP-Port: 8080 SSL SSL_aktivieren SSL-Port: 8443 Zertifikat: Auswählen	Image: Standard Image: Standard Image: Standard Image: Standard
Zugelassene Authentifizierungsmethoden konfigurieren: Authentifizierung	Authentifizierungsserver Standarddomäne für Authentifizierung auswählen: Domäne auswählen RADIUS-Server für Authentifizierung auswählen: EADIUS-Server Formularbasierte OWA-Authentifizierung konfigurieren: Konfigurieren
OK Abbrechen Obernehmen	OK Abbrechen

Als nächstes aktivieren Sie Authentifizierung ist für alle Benutzer erforderlich. Damit wird sichergestellt, dass nicht autorisierte Benutzer zur Authentifizierung aufgefordert werden.

Im Feld Authentifizierungsserver wählen Sie bitte *RADIUS-Server* aus. Es erscheint folgendes Fenster (in diesem Beispiel ist bereits ein RADIUS Server konfiguriert). Klicken Sie auf *Hinzufügen*.

lame	Port	Beschreibung	Hinzufügen
92.9.200.18	1812	Interner DC	
			Bearbeiten
			- 10
			Entrernen
			+
			+

Geben Sie unter Servername die IP Adresse oder den Namen des IAS Servers an. Die Serverbeschreibung ist optional, jedoch zur besseren Orientierung und zur Dokumentation sinnvoll.

RADIUS-Server bear	beiten	? ×
Geben Sie den Namen legen Sie fest, wie ISA	oder die IP-Adresse des RADIUS-Servers ein, un A Server mit diesem Server kommunizieren soll.	ıd
<u>S</u> ervername:	192.9.200.18	
Serverbes <u>c</u> hreibung:	Interner DC	
Gemeinsamer geheimer Schlüssel:	Ändern	
<u>P</u> ort:	1812	
Zeitlimit (Sekunden):	5	
Nachrichtenauthen	tifizierung immer verwenden	
	OK Abbreche	en

Im Feld *Gemeinsamer geheimer Schlüssel* geben Sie den im IAS erstellen Schlüssel an. Sie erinnern sich: Xd5\$1"xSS(&aäsD03?Q. Bestätigen Sie den Schlüssel noch einmal.

Tipp: Verwenden Sie NICHT den Schlüssel in diesem Beispiel.

Der Standard *Port* für RADIUS ist 1812,1645 für die Authentifizierung und 1813,1646 für die Kontoführung. Ändern Sie die Ports nicht. Wenn ja, müssen die Änderungen auch am IAS erfolgen.

Das Zeitlimit (Sekunden) sollten Sie nur verändern, wenn der ISA Probleme hat in dieser Zeit den IAS zu kontakten. Das sollte aber nur sehr selten bis gar nicht der Fall sein.

Den Punkt Nachrichtenauthentifizierung immer verwenden können Sie unverändert lassen.

Firewallregel auf dem ISA Server

Der nächste Schritt ist die Erstellung eine Firewallregel mit der Verwendung von RADIUS als Benutzerauthentifizierung. In diesem Beispiel verwenden wir eine Firewallregel für den HTPP/HTTPS Zugriff für einen Active Directory Benutzer namens MSISAFAQ.



Die ersten Schritte des Wizards zur Erstellung einer Firewallregel erspare ich mir, weil diese sich nicht von der Erstellung einer normalen Regel unterscheiden.

Wir steigen bei dem Punkt *Benutzersätze* des Assistenten für neue Zugriffregeln ein. Entfernen Sie *Alle Benutzer* und klicken Sie auf *Hinzufügen* um einen neuen Benutzersatz zu erstellen.

Assistent für neue Zugriffsregel	×
Benutzersätze Sie können die Regel auf Anforderungen von allen Benutzern anwende können den Zugriff aber auch auf bestimmte Benutzersätze einschränk	n. Sie en.
Diese Regel betrifft Anforderungen von folgenden Benutzersätzen:	1
hlle Benutzer 🐣	<u>H</u> inzufügen
	Bearbeiten
	Entfernen
,	
	
< <u>∠</u> urück <u>W</u> eiter :	Abbrechen

Klicken Sie auf Neu

Veu Bearbeiten Lösr	then
Alle authentifizierten	Benutzer
Alle Benutzer	
鴅 System- und Netzwer	kdienst

Im Assistenten für Benutzersätze vergeben Sie einen Namen für den neuen Benutzersatz.

Assistent für neue Benutzers	ätze	×
Microsoft Internet Security & Acceleration Server 2004	Willkommen Mit diesem Assistenten können Sie einen neuen Benutzersatz erstellen. Ein Benutzersatz ist eine Gruppe von Benutzern (Windows-sowohl als auch Nicht-Windows-Benutzer, z. B. RADIUS), die zusammen als ein einzelner Satz definient werden. Wenn Sie Webveröffentlichungs-, Protokoll- und Zugriffsrichtlinienregehe nestellen, können Sie die Regel auf mehrere Sätze anwenden. Begutzersatzname: AD User ueber IAS	
-	Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.	
	< <u>Z</u> urtick. <u>W</u> eiter > Abbreche	n

Im Fenster Benutzer klicken Sie auf Hinzufügen und wählen RADIUS aus.

Assist	ent für neue Benu	tzersätze			×	
Benutzer Wählen Sie Benutzer aus, die im Benutzersatz enthalten sein sollen.				n sollen.		
N	amespace	Gruppe	Domäne		Hinzufügen) Windows-Benutzer	r und -Gruppen
					RADIUS SecurID	
			< <u>Z</u> urück	<u>W</u> eiter :	> Abbrechen	

Der Namespace ist RADIUS.

Als Benutzername stehen zur Wahl:

- ? Alle Benutzer im Namespace entspricht der Gruppe JEDER der Active Directory Domäne
- ? Angegebener Benutzername entspricht dem Active Directory Benutzernamen.

Benutzer hinzufüg	en		? ×
Namespace:	RADIUS		
Benutzername:			
Alle Benutzer i	m Namespace		
C A <u>ng</u> egebener I	Benutzername:		
			1
		OK	Abbrechen

Wir wählen Alle Benutzer im Namespace

Das Regelwerk ist fast fertig. Wählen Sie jetzt noch den neu erstellten Benutzersatz aus und bestätigen Sie die neu erstellte Firewallregel.

Sie können diese Regel jetzt verwenden um dem Benutzer das Surfen über den ISA Server 2004 zu erlauben.

Stand: 16.08.2004/MG - Kontakt: Marc Grote - http://www.it-training-grote.de