

Forefront Protection 2010 for Exchange und Cloudmark Engine Updates ueber Forefront TMG

Das Update der Cloudmark Engine von FPE ueber Forefront TMG schlaegt fehl. Der FPE Server ist Webproxy Client only.

Modul	Wird v...	Updates sind a...	Modulversion	Definitionsversi...	Letzte Aktualisier...	Letzte Überprüfung
Authentium Command Antivirus En...	Ja	Ja	5.3.6	201108180738	18.08.2011 10:32	18.08.2011 10:32
Cloudmark Antispam Engine	Ja	Ja	0.0.0	01.01.2000 01:00		Fehler bei 18.08.2011 10:55
Kaspersky Antivirus Technology	Ja	Ja	8.1.8.79	18.8.2011 6:43:0	18.08.2011 09:32	18.08.2011 10:31
Microsoft Antimalware Engine	Ja	Ja	1.1.7604.0	1.111.129.0	18.08.2011 08:31	18.08.2011 10:30
Norman Virus Control	Ja	Ja	6.7.10	6.7 #0	17.08.2011 23:31	18.08.2011 10:30
VirusBuster Antivirus Scan Engine	Ja	Ja	5.3.0 2011-04...	14.0.174 2011-08...	17.08.2011 17:28	18.08.2011 10:30
Worm List	Ja	Ja	11.0.2.193	65.252.140.49	17.08.2011 12:43	18.08.2011 10:30

Auf dem TMG Server taucht folgende Fehlermeldung im Logging auf. Wenn man versucht die angezeigte URL im Browser zu laden, hat man einen Blinker Effekt. Mal funktioniert der Download, mal funktioniert der Download nicht.

Fehlgeschlagener Verbindungsversuch 18.08.2011

Protokolltyp: Webproxy (Forward)
Status: 10054 Eine vorhandene Verbindung wurde vom Remotehost geschlossen.
Regel: FPE Updates
Quelle: Internal (192.168.1.100:64202)
Ziel: External (192.168.1.100:8080)
Anforderung: GET http://forefrontdl.microsoft.com/server/scanengineupdate/amd64/Cloudmark/Package/1107110001/cloudmark_fullpkg.cab
Filterinformationen: Req ID: 0c0236da; Compression: dient=No, server=Yes, compress rate=0% decompress rate=0%
Protokoll: http
Benutzer: anonymous
[Zusätzliche Informationen](#)

Der erste Versuch war dann, eine anonyme Zugriffsregel fuer die Cloudmark Zugriff zu erstellen. Dazu zwei Domaenennamensaetze erstellt.

Eigenschaften von Cloudmark

Allgemein

Name: Cloudmark

Regeln, die Domänennamensätze verwenden, werden eventuell nicht wie erwartet angewendet, falls DNS nicht richtig konfiguriert ist.

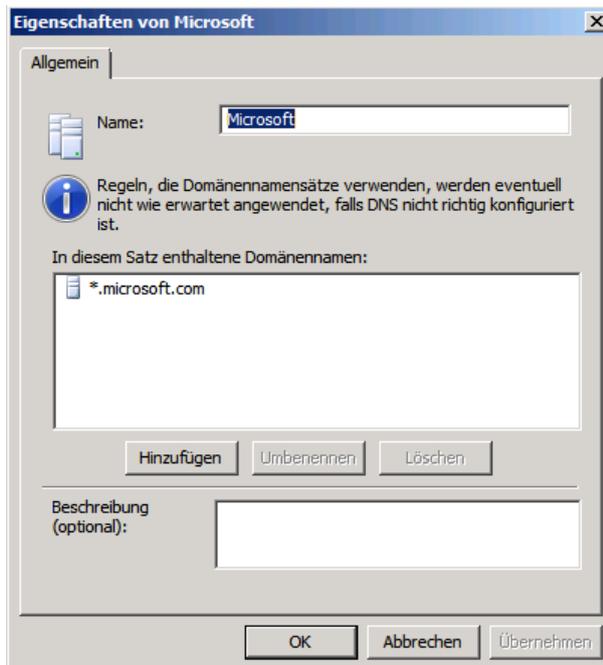
In diesem Satz enthaltene Domänennamen:

- *.cloudmark.com

Hinzufügen Umbenennen Löschen

Beschreibung (optional):

OK Abbrechen Übernehmen



Eine entsprechende Firewallregel erstellt fuer den FPE Zugriff auf Cloudmark.

Richtlinie für alle Firewalls						
Suchen... <input type="text"/> Beispiele						
Reihenfolge	Name	Aktion	Protokolle	Von / Listener	Nach	Bedingung
1	[redacted] FPE Updates	Zulassen	HTTP HTTPS	[redacted] 2	Cloudmark Microsoft	All Users

Danach kam noch die Meldung mit der HTTPS Inspection

Verweigerte Verbindung [redacted] 18.08.2011 10:15:02

Protokolltyp: Webproxy (Forward)

Status: 12226 Der Zertifizierungsstelle, von der das von einem Zielserver übergebene SSL-Serverzertifikat ausgestellt wurde, wird vom lokalen Computer nicht vertraut.

Regel: [redacted] FPE Updates

Quelle: Internal (192.168. [redacted]:57530)

Ziel: External (192.168. [redacted]:8080)

Anforderung: lvc.cloudmark.com:443

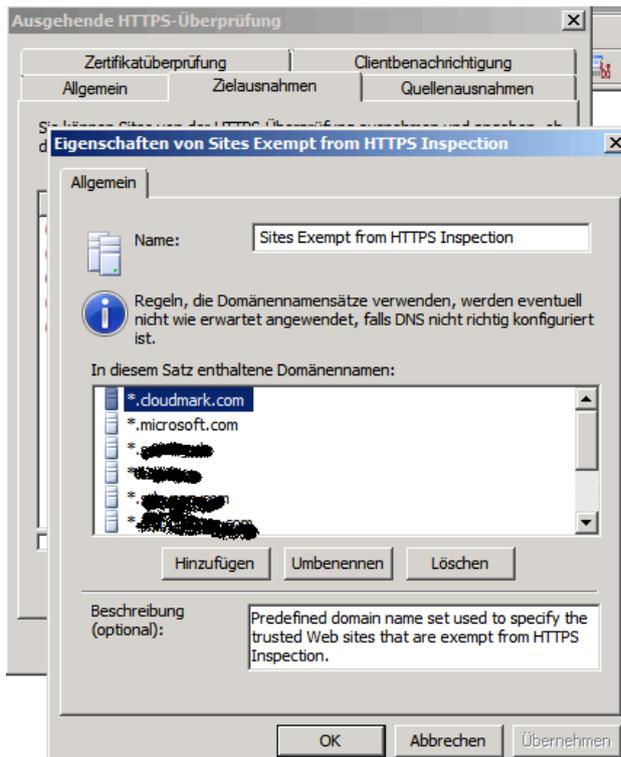
Filterinformationen: Req ID: 0c01b6f9; Compression: client=No, server=No, compress rate=0% decompress rate=0%

Protokoll: https-inspect

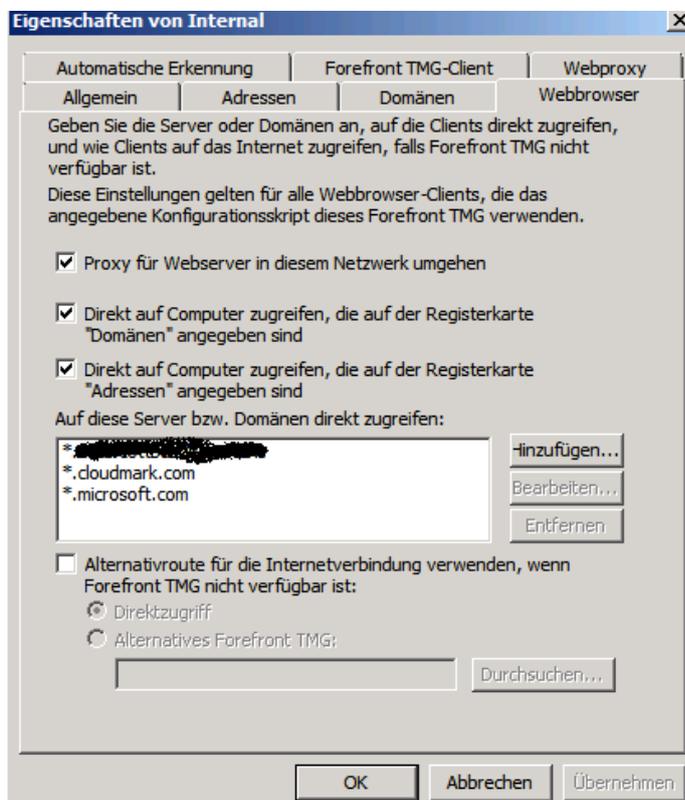
Benutzer: anonymous

[Zusätzliche Informationen](#)

Also die Cloudmark Website von der HTTPS Ueberpruefung ausgeschlossen



Danach funktionierte der Zugriff immer noch nicht, also als letzte Idee den TMG Server fuer den direkten Zugriff auf *.cloudmark.com und *.microsoft.com konfiguriert.



Danach konnten die FPE Updates auch erfolgreich geladen werden

Server Security-Ansichten - Dashboard
Statistiken für die aktivierten Schutzdienste anzeigen und den gesamten Integritätsstatus des Servers überwachen

Systemüberwachungen für Server [Servername]

Scanaufträge	Dienste	Module	Lizenzierung
✓	✓	✓	✓
Details anzeigen...	Details anzeigen...	Details ausblenden	Details anzeigen...

Integritätspunkt	Letzte Aktualisierung	Nachricht
✓ Spamdefinitionsupdate	19.08.2011 11:56:42	Der Inhaltsfilter ist aktiviert, und die Definitionen wurden innerhalb der letzten Stunde aktualisiert.
✓ Alle Modulaktualisierungen sin...	19.08.2011 11:56:42	Alle AntiMalware-Module, die in der Forefront-Verwaltungskonsole zum Scannen ausgewählt sind, wurden für ...
✓ Aktualisierungszeitraum der au...	19.08.2011 11:56:42	In den letzten fünf Tagen wurden alle AntiMalware-Module erfolgreich aktualisiert, die für Updates aktiviert sind.
✓ Ausgewählte Module wurden a...	19.08.2011 11:56:42	Beim letzten Versuch wurden alle AntiMalware-Module, die für Aktualisierungen aktiviert sind, erfolgreich aktus...

[Modulzusammenfassung](#)