

Enteo NetInstall und Forefront TMG

Bei einem Kunden habe ich Forefront TMG implementiert. Ebenfalls in diesem Netzwerk wird Enteo Netinstall zur System- und Softwarebereitstellung verwendet. Nach der TMG Installation haben wir festgestellt, dass per Enteo PXE Boot und anschliessendem PE Start, der Client keine Verbindung zu den Enteo Servern herstellen kann.

Ursache war nach einiger Suche die aktivierte NIS (Network Inspection System) Funktion von Forefront TMG. Durch das Erstellen von Zielausnahmen war dann der Client-Verbindungsaufbau zum Enteo NetInstall Server moeglich.

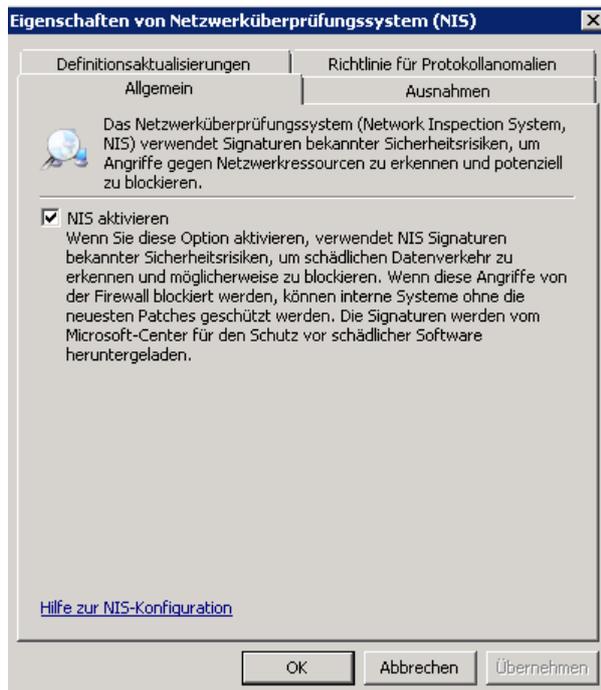
NIS Einstellungen am TMG

The screenshot shows the Microsoft Forefront Threat Management Gateway (TMG) configuration interface. The main window displays the Network Inspection System (NIS) settings. The NIS status is 'Aktiviert' (Activated) with a version of 4.27 (13.04.2010). The configuration is for a 'Konfigurationsspeicherserver: SR...' and 'Eindringungsschutzsystem'.

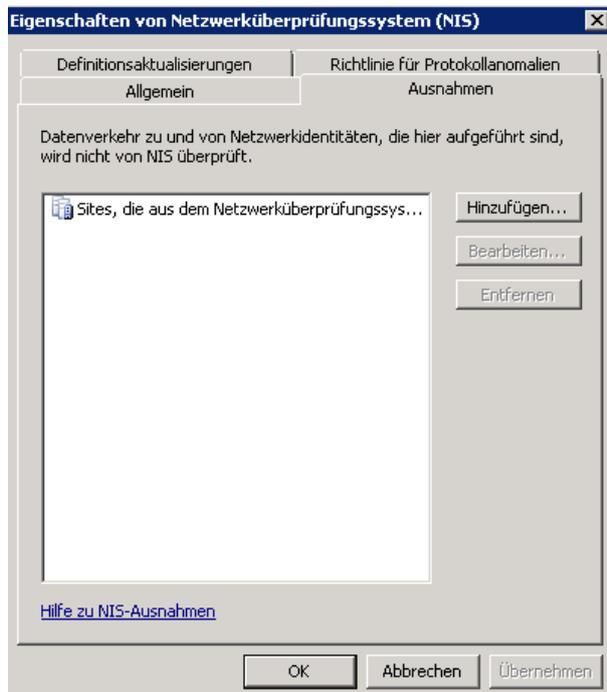
The main area shows a list of rules under the heading 'Markierung aufheben (keine Kenntnisnahme erforderlich)'. The rules are sorted by 'Aufsteigend' (Ascending) order. The columns are: Name, Kenntnisn..., Status, Reaktion, Richtlinien..., Datum der Ve..., Verwandte Bull..., and CVE-Numme.

Name	Kenntisn...	Status	Reaktion	Richtlinien...	Datum der Ve...	Verwandte Bull...	CVE-Numme
Expl:Win\ActiveX.DXImgTransform.R...	Markieru...	Aktiviert	Blockieren	Standard	13.06.2006	MS06-021	CVE-2006-23
Expl:Win\ActiveX.DXImgTransform.R...	Markieru...	Aktiviert	Blockieren	Standard	13.06.2006	MS06-021	CVE-2006-23
Expl:Win\ActiveX.Fpole.RCE12006-4704	Markieru...	Aktiviert	Blockieren	Standard	12.12.2006	MS06-073	CVE-2006-47
Expl:Win\ActiveX.Hhctr.RCE12006-3...	Markieru...	Aktiviert	Blockieren	Standard	08.08.2006	MS06-046	CVE-2006-33
Expl:Win\ActiveX.WebViewFolderIcon...	Markieru...	Aktiviert	Blockieren	Standard	10.10.2006	MS06-057	CVE-2006-37
Expl:Win\ActiveX.Hhctrl.Hhctrl.DoS1...	Markieru...	Aktiviert	Blockieren	Standard	12.12.2006	MS07-008	CVE-2007-02
Expl:Win\ADODB.Connection.DoS120...	Markieru...	Aktiviert	Blockieren	Standard	12.12.2006	MS06-009	CVE-2006-55
Expl:Win\Agent.AgentCharacterLoa...	Markieru...	Aktiviert	Blockieren	Standard	10.04.2007	MS07-020	CVE-2007-12
Expl:Win\Browser.Shellcode.RCE1000...	Markieru...	Aktiviert	Blockieren	Standard	04.06.2009	NA	NA
Expl:Win\CMS.SQLServer.RCE12002-...	Markieru...	Aktiviert	Blockieren	Standard	07.08.2002	MS02-041	CAN-2002-07
Expl:Win\COM.ActiveX.RCE12006-1303	Markieru...	Aktiviert	Blockieren	Standard	13.07.2006	MS06-021	CVE-2006-13
Expl:Win\COM.ActiveX.RCE12006-3638	Markieru...	Aktiviert	Blockieren	Standard	06.08.2006	MS06-042	CVE-2006-36
Expl:Win\COM.ActiveX.RCE12006-4697	Markieru...	Aktiviert	Blockieren	Standard	13.02.2007	MS07-016	CVE-2006-46
Expl:Win\COM.ActiveX.RCE12007-0219	Markieru...	Aktiviert	Blockieren	Standard	13.02.2007	MS07-016	CVE-2007-02
Expl:Win\COM.CAPICOM.RCE12007-...	Markieru...	Aktiviert	Blockieren	Standard	08.05.2007	MS07-028	CVE-2007-09
Expl:Win\COM.IME.RCE12007-0942	Markieru...	Aktiviert	Blockieren	Standard	08.05.2007	MS07-027	CVE-2007-09
Expl:Win\COM.SCM.RCE12007-2222	Markieru...	Aktiviert	Blockieren	Standard	12.07.2007	MS07-033	CVE-2007-22
Expl:Win\COM.URLMON.RCE12007-0...	Markieru...	Aktiviert	Blockieren	Standard	12.07.2007	MS07-033	CVE-2007-02
Expl:Win\DirectX.DAXCTLE.RCE12006...	Markieru...	Aktiviert	Blockieren	Standard	14.11.2006	MS06-067	CVE-2006-47
Expl:Win\DotNET.ASPState.RCE1200...	Markieru...	Aktiviert	Blockieren	Standard	06.06.2002	MS02-026	CAN-2002-05
Expl:Win\FlashPlayer.LoadMovie.RCE...	Markieru...	Aktiviert	Blockieren	Standard	13.06.2006	MS06-020	CVE-2006-00
Expl:Win\HTTP.Bitalk.RCE12003-0118	Markieru...	Aktiviert	Blockieren	Standard	30.04.2003	MS03-016	CAN-2003-01
Expl:Win\HTTP.URL.SQLInj10000-0000	Markieru...	Aktiviert	Nur erken...	Standard	30.03.2010	NA	NA
Expl:Win\HTTP.URL.XSSI10000-0000	Markieru...	Aktiviert	Nur erken...	Standard	30.03.2010	NA	NA

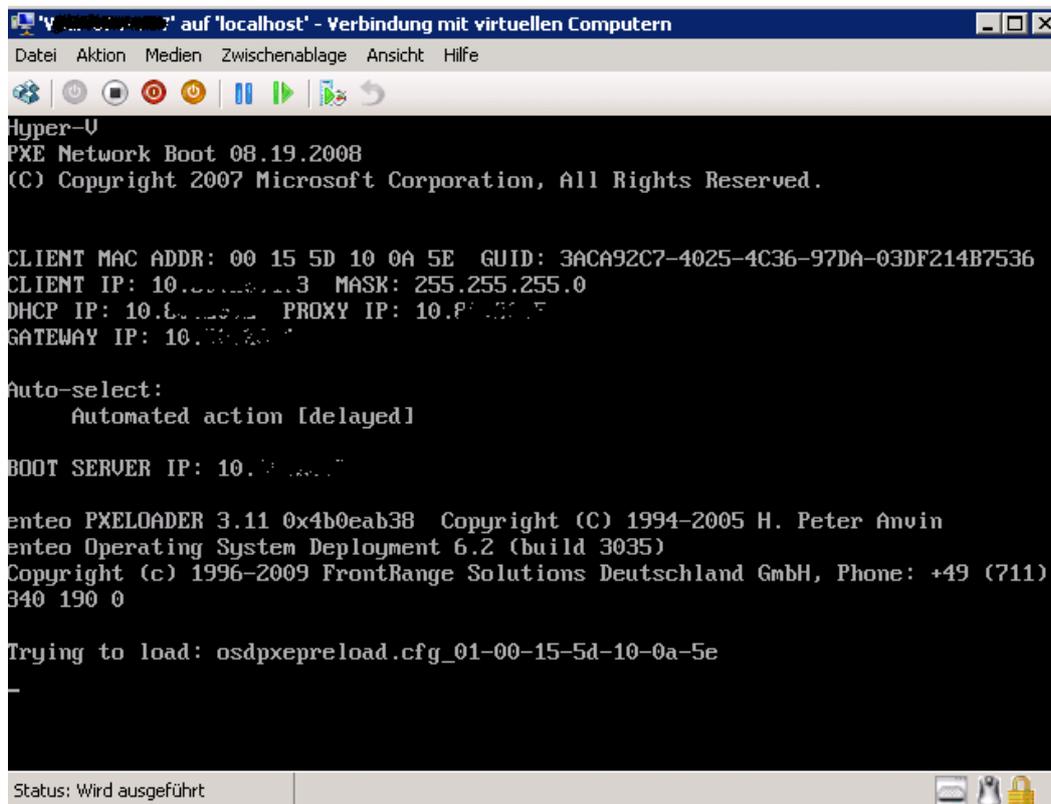
NIS ist aktiviert



Standard Ausnahmen



Meldung des PXE Boot des Enteo Clients



The screenshot shows a terminal window titled "Hyper-U" with a menu bar (Datei, Aktion, Medien, Zwischenablage, Ansicht, Hilfe) and a toolbar. The terminal output displays the following information:

```
Hyper-U
PXE Network Boot 08.19.2008
(C) Copyright 2007 Microsoft Corporation, All Rights Reserved.

CLIENT MAC ADDR: 00 15 5D 10 0A 5E  GUID: 3ACA92C7-4025-4C36-97DA-03DF214B7536
CLIENT IP: 10.0.0.103  MASK: 255.255.255.0
DHCP IP: 10.0.0.103  PROXY IP: 10.0.0.1
GATEWAY IP: 10.0.0.1

Auto-select:
  Automated action [delayed]

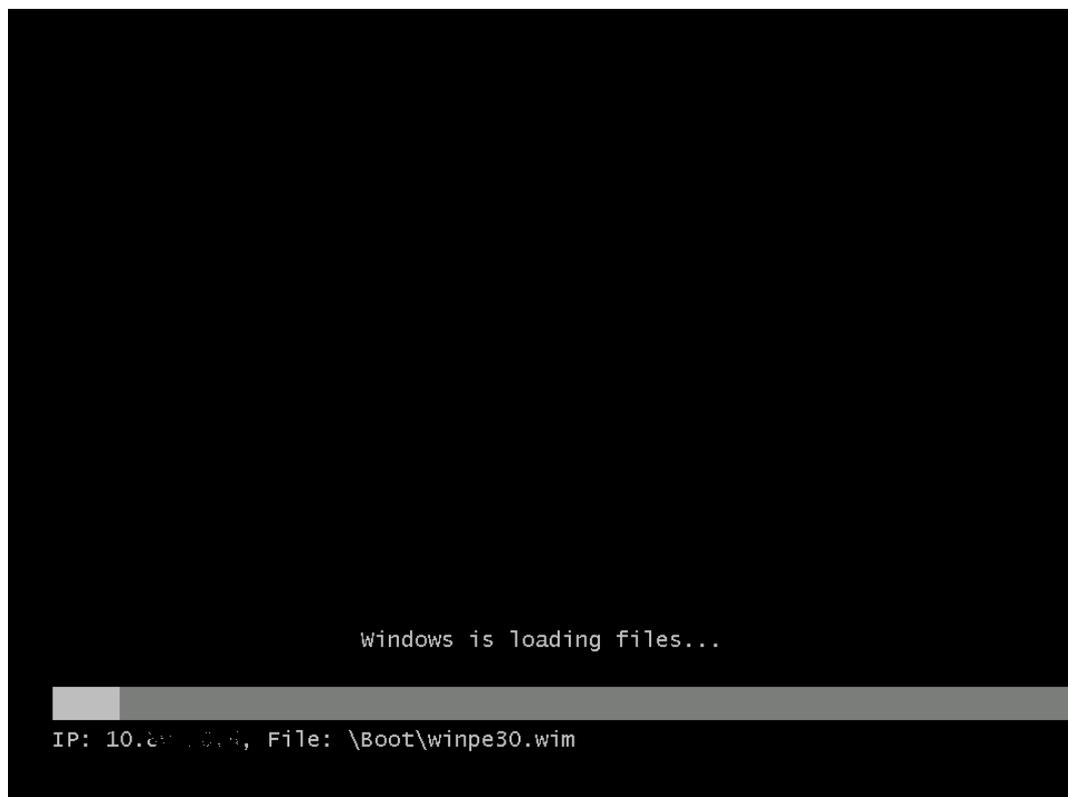
BOOT SERVER IP: 10.0.0.1

Enteo PXELOADER 3.11 0x4b0eab38  Copyright (C) 1994-2005 H. Peter Anvin
Enteo Operating System Deployment 6.2 (build 3035)
Copyright (c) 1996-2009 FrontRange Solutions Deutschland GmbH, Phone: +49 (711)
340 190 0

Trying to load: osdpxepreload.cfg_01-00-15-5d-10-0a-5e
-
```

At the bottom of the window, the status bar indicates "Status: Wird ausgeführt" and includes icons for help, a user profile, and a lock.

Windows PE 30 Boot



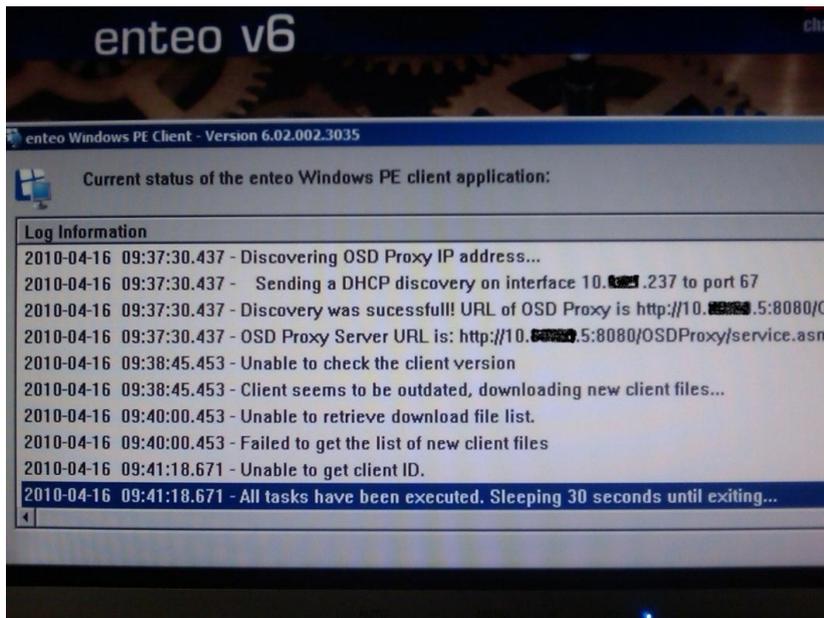
The screenshot shows a black terminal window with the following text:

```
Windows is loading files...
```

A progress bar is visible below the text, showing approximately 25% completion. At the bottom of the terminal, the following information is displayed:

```
IP: 10.0.0.103, File: \Boot\winpe30.wim
```

Kein erfolgreicher Verbindungsaufbau des Enteo Clients



Protokollierung in Forefront TMG bei NICHT erfolgreichem Verbindungsaufbau des Enteo Clients. Es werden keine Verbindungen verweigert, man sieht lediglich das die NIS Ueberpruefung stattfindet. Auf Enteo Client Seite macht sich die NIS-Ueberpruefung durch einen sehr langen Verbindungsversuch mit dem Enteo Server bemerkbar.

Wichtige Anmerkung: Die Probleme gelten nur fuer die OS-Installation in der PE Phase.

Microsoft
Forefront
Threat Management Gateway 2010

Konfigurationsspeicherserver: SRV-10.10.10.5.local

Protokollierung | Berichterstattung

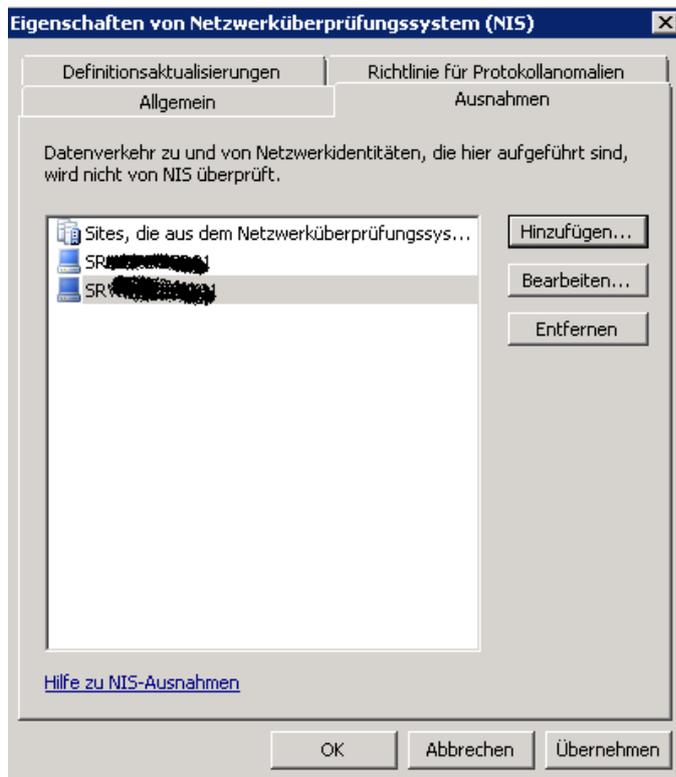
Filtern nach	Bedingung	Wert
Protokollkategorie...	Gleich	Firewall oder Webproxyfilter
Protokollzeit	Aktuell	
Client-IP	Gleich	10.10.10.237

Protokollzeit	Client-IP	Ziel-IP	Zielport	Protokoll	Aktion	Ergebnis der NI...	NIS-Signatur	NIS-A
16.04.2010 09:40:04	10.10.10.237	10.10.10.5	500	IKE-Client	Initiiert...			
16.04.2010 09:40:18	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Initiiert...			
16.04.2010 09:40:18	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Getren... Überprüft			
16.04.2010 09:40:33	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Initiiert...			
16.04.2010 09:40:33	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Getren... Überprüft			
16.04.2010 09:40:48	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Initiiert...			
16.04.2010 09:40:48	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Getren... Überprüft			
16.04.2010 09:41:03	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Initiiert...			
16.04.2010 09:41:03	10.10.10.237	10.10.10.5	8080	HTTP-Proxy	Getren... Überprüft			
16.04.2010 09:41:05	10.10.10.237	10.10.10.5	500	IKE-Client	Getren...			

Getrennte Verbindung SRV-10.10.10.5.local 0 09:41:05

Protokolltyp: Firewalldienst
 Status: Eine Verbindung wurde beim ordnungsgemäßen Herunterfahren mit einem FIN-initialisierten Dreivegehandshake getrennt.
 Regel: Clients: Zugriff auf NI-Server
 Quelle: 10.10.10.237 (10.10.10.237:500)
 Ziel: Intern (src=10.10.10.237, dest=10.10.10.5:500)
 Protokoll: IKE-Client
[Zusätzliche Informationen](#)

Die Enteo NetInstall Server als Zielausnahmen konfigurieren



Danach funktioniert es auch mit Enteo NetInstall und PXE Boot / PE