

created by: Rainer Bemsel - Version 1.0 - Dated: Aua/02/2003

The purpose of this document is to have a basic step-by-step instructions to install Network Associates Gauntlet Firewall on NT 4.

Minimum System Requirements:	Used System Specs for this implementation
Windows NT 4 with Service Pack 4 or 5	Windows NT 4 AS with SP 6a
233 MHz	1 GHz
128 MB RAM	128 MB RAM
512 MB of free disk space	1 GB of free disk space
2 NICs	2x Intel EtherExpress Pro/100 PCI LAN Adapter
DNS Server if you plan to run DNS	1x DNS server on untrusted network
SMTP mail server on trusted network	
(if you plan to send mail through the Firewall)	
POP3 mail server on trusted network	1x POP3 mail server on untrusted network
(if you plan to use POP3 to retrieve mail from trusted network)	
	No IIS has been installed
	Static IP Address
	No IPX/SPX enabled
	Server installed as stand-alone Server

Some more details about my test network, based on this installation and configuration

External Services:

DNS Server:	210.210.210.100
POP3 Server:	210.210.210.100
Web Server:	210.210.210.100
FTP Server:	210.210.210.100

Inside (trusted) Network Interface:		Outside (untrusted) Network Interface:		
IP Address:	135.100.100.253	IP Address:	210.210.210.253	
Host Name:	Gauntlet	Host Name:	Gauntlet	
Interface Name:	Gauntlet_Trust	Interface Name:	Gauntlet_UnTrust	
Netmask:	255.255.255.0	Netmask:	255.255.255.0	
Broadcast Address:	135.100.100.255	Broadcast Address:	210.210.210.255	
Default Gateway:	135.100.100.254	Default Gateway:	210.210.210.254	

Before installing Gauntlet Firewall, please ensure proper communication, like DNS Lookups, Routes and Subnet Addressing has been verified. Eventually, you have to change routes and router configuration as well. If you have several trusted networks inside your security perimeter, you may need to add static routes on the firewall for them.

My test network layout can be found here: www.bemsel.com/techtip/RBE VPN 1 3.pdf



DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support. Although I believe the information provided in this document to be accurate at the time of writing. I reserve the right to modify, update, retract or otherwise change the information contained within for any read withour notice. This technote has been created after studying the material and / or practical evolution by myself. All liability for use of the information presented here remains with the user

- **1.** Disconnect your firewall from the network by physically disconnecting the cables from both network adapters.
- 2. Log on to the firewall (not the domain) as administrator
- 3. Execute setup.exe
- 4. The Welcome Windows appears



Click on NEXT

5. End User License Agreement

You will be presented with the Gauntlet End User License Agreement.

Netwo	ark Associates 1 Gauntlet v5.5	Two (2)-Year End for Windows N1	d User License / [4.0	Agreement	-
Сору	right (c) 1999 N All Rights F	letworks Associa Reserved.	ates Technolog	, Inc.	
NOTICE T	O ALL USERS	CAREFULLY R	EAD THE FOLI	OWING LEGAL	
AGREEME	NT ("AGREEN RE ("SOFTWAI	IENT"), FOR TH RE") PRODUCE	E LICENSE OF BY NETWOR	SPECIFIED	INC.
("NETWO	RK ASSOCIAT	ES"), BY CLICKI WARE, YOU (EI	NG THE ACCE THER AN IND/	PT BUTTON OR VIDUAL OR A	
SINGLE E	NTITY) CONSE AGREEMENT.	IF YOU DO NO	IND BY AND BI T AGREE TO A	ECOME A PARTY LL OF THE	
TERMS O THAT YOU	F THIS AGREE J DO NOT ACI	MENT, CLICK T	HE BUTTON T	HAT INDICATES	00 _



In order to continue the installation, you have to accept all the terms, by clicking on YES

6. The Setup Program examines you Windows NT configuration,

and is looking for conflicts and settings not set optimally for use with Gauntlet. The installation will display a message and stop if a Mandatory item does not pass. The problem must be fixed before Gauntlet can be installed.



7. Choose Destination Location

I recommend to use default Destination Folder, in order not to conflict with eventual bugs.



8. Assign Network Adapters

In this window, you will assign both network cards to their proper location, meaning setting NICs to trusted and untrusted networks.



Assign Network Adapter	5			×
	Interface Name	Туре	Adapter Name	IP:Mask
(B)	Trusted Interface [1] Untrusted Interface [2]	T U	[2] Intel 82557-based PRO Adapter Driver [1] Intel 82557-based PRO Adapter Driver	135.100.100.253.255.255.255 210.210.210.253.255.255.255
GALINITIET	Set Interface Name and Type	_ (Trusted Untrusted 	
Queenorix		(Failover	Next > Cancel

9. Confirm Initial Configuration



You will be asked to confirm the initial configuration. In my case, I have following settings:

Trusted Network Card: [2] Intel 82557-based PRO Adapter Driver – 135.100.100.253:255.255.255.0

Untrusted Network Card: [1] Intel 82557-based PRO Adapter Driver – 210.210.210.253:255.255.255.0

Failover network card (none)



Gauntlet group name =GauntletGroup Proxy account name =GauntletProxy Setup will disable "Spooler" and "LicenseServer" services

The setup starts by copying files. In addition to installing the software, several Windows NT settings are modified to make them more secure.

10. Setup Completed



11. Reboot the System

Gauntlet requires a reboot. Please remove all disks from your disk drive, so Gauntlet setup can restart the computer in order to complete the installation

Gauntlet	v5.5 (Licensed) for NT	×
٩	Please remove all disks from your disk drives. installation.	Gauntlet [®] setup will restart the computer in order to complete the
		(OK)

12. Verify the proper start of Gauntlet Firewall

Do do so, open Programs - Gauntlet - Log Monitor. You should see proper startings.

LOG.TXT

You also should see on Services, following Gauntlet Services started:

GauntletAuthService	Started	Manual
GauntletFailover	Started	Manual
GauntletFTPProxy	Started	Manual
GauntletH323Proxy		Manual
GauntletHTTPProxy	Started	Manual
GauntletIKE		Manual
GauntletLogService	Started	Manual
GauntletMasterService	Started	Manual
GauntletMSSQLProxy		Manual
GanutletNetShowProxy		Manual
GauntletPlugProxy	Started	Manual
GauntletPOP3Proxy		Manual
GauntletRAPProxy		Manual
GauntletReportService		Manual



GanutletSMBProxy		Manual
GauntletSMTPProxy		Manual
GauntletSNMPProxy		Manual
GauntletSQLProxy		Manual
GauntletStramwrksProxy	7	Manual
GauntletSybaseProxy		Manual
GauntletTELNETProxy	Started	Manual
GauntletVDOLiveProxy		Manual

13. Installing Gauntlet Service Packs

At time of this writing, there exist 2 Service Packs for Gauntlet Firewall 5.5

14. Install Service Pack 1

- a) Extract the files from the zip files into a directory, i.e., c:/temp/SP1
- b) Open up a command prompt window and run INSTALL.BAT in the directory to which the files were extracted. This will rename all of the replaced files and copy the updated fiels to the appropriate directories
- c) Reboot the computer

15. Install Service Pack 2

- a) Extract the files from the zip files into a directory, i.e., c:/temp/SP2
- b) Open up a command prompt window and run INSTALL.BAT in the directory to which the files were extracted. This will move all files, being replaced to a backup directory and copy the updated files to the appropriate directories.
- c) Reboot the computer

After the final reboot – you should be able to use Network Associates Gauntlet Firewall.

