For Public Use

G/On

Basic Best Practice Reference Guide

Version 6

Make Connectivity Easy

Table of Contents

Scope

This document has been developed to provide best practice reference information to users and administrators of the G/On Product line. The document details best practice for configuration and placement of the G/On Server, and also a basic set of requirements for the PC where the G/On USB Key or G/On Desktop will be implemented.

It is assumed the reader of the document has the relevant technical skills and background to understand security implications of different network topologies. It is also assumed the reader understands how to secure the components of a network topology.

G/On Server Platform Requirements

In today's hostile environment of worms, viruses, denial-of-service attacks, Internet-wide scanning, and much, much more, it is imperative Internet facing servers are secured as much as possible.

The first and most important step in securing an Internet facing server is to keep the server updated with the latest security related fixes. Almost all exploits, giving access to a server, are based on known vulnerabilities in the operating systems and/or running applications. Eliminating most of these vulnerabilities is done by keeping the server updated with the latest service pack and security fixes, sometimes also called hot-fixes.

The second step in securing an Internet facing server is to harden the operating system by removing any services not needed by the application running on the server. Removing the services limits an attacker's options. Should an attacker gain access to parts of the network, reducing running services will limit the attacker in gaining additional access.

The third step in securing an Internet facing server is to reduce the amount of users that have access to the server. Only system administrators, with a valid business need, should have an account on the server. Renaming default administrators accounts, changing default passwords, and disabling or removing unnecessary accounts is a basic step making it more difficult for an attacker to gain access to the server.

Once these steps have been taken, the server is ready for installation of the G/On Server.

For more information on securing Internet facing servers, please see the reference section at the end of this document.

G/On USB and G/On Desktop Platform Requirements

Because of the hostile environment the Internet has become, it is necessary to take a few basic steps to protect a PC before connecting it to the Internet.

As described in the server section, it is equally important to keep a PC updated with the latest services pack and security related fixes.

Since you don't always have a way of knowing if the Internet connection you are using is protected by a firewall, and if it is, how well the firewall has been configured, it is always recommended to install firewall software on the PC. Some operating systems include firewall features, in other cases it must be purchased separately.

Antivirus software has also become a necessity. Not only does it protect from virus and worms, but most antivirus software also protects against Trojans and other forms of malware. There are a multitude of ways to get infected, not just from e-mails, but also by visiting certain Internet sites, or even using applications that appear "friendly", but aren't.

Spyware isn't normally malicious in nature, but it does slow down the PC by using the CPU, and it also reduces available bandwidth, by unnecessary use of the Internet connection. Installing anti-spyware software is becoming a necessity, and should be considered seriously.

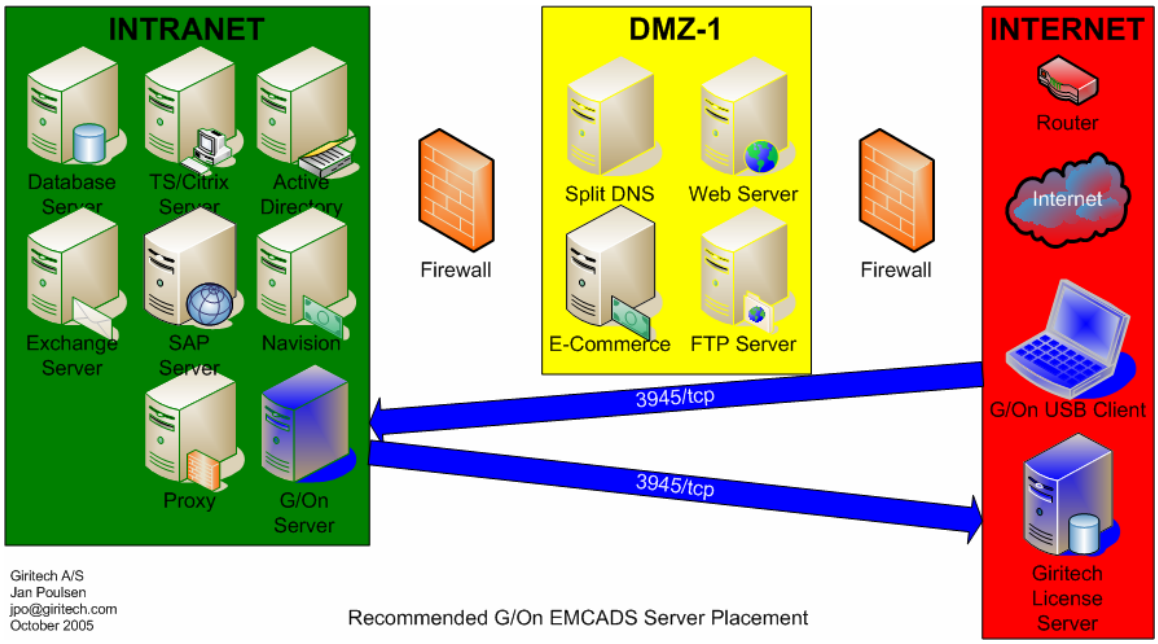
For more information on protecting a PC, please see the reference section at the end of this document.

Intrusion Detection

Implementing a firewall doesn't necessarily imply security. Without proactive monitoring, there's no way of knowing if the firewall is actually protecting the network. One way is constant log analysis. Depending on the amount of traffic, this may be an impossible task. A better way is to implement an Intrusion Detection System (IDS). The IDS can detect patterns of attack, and can send alarms, or even shut down parts of the network to protect the infrastructure.

G/On Server Placement

In the intranet



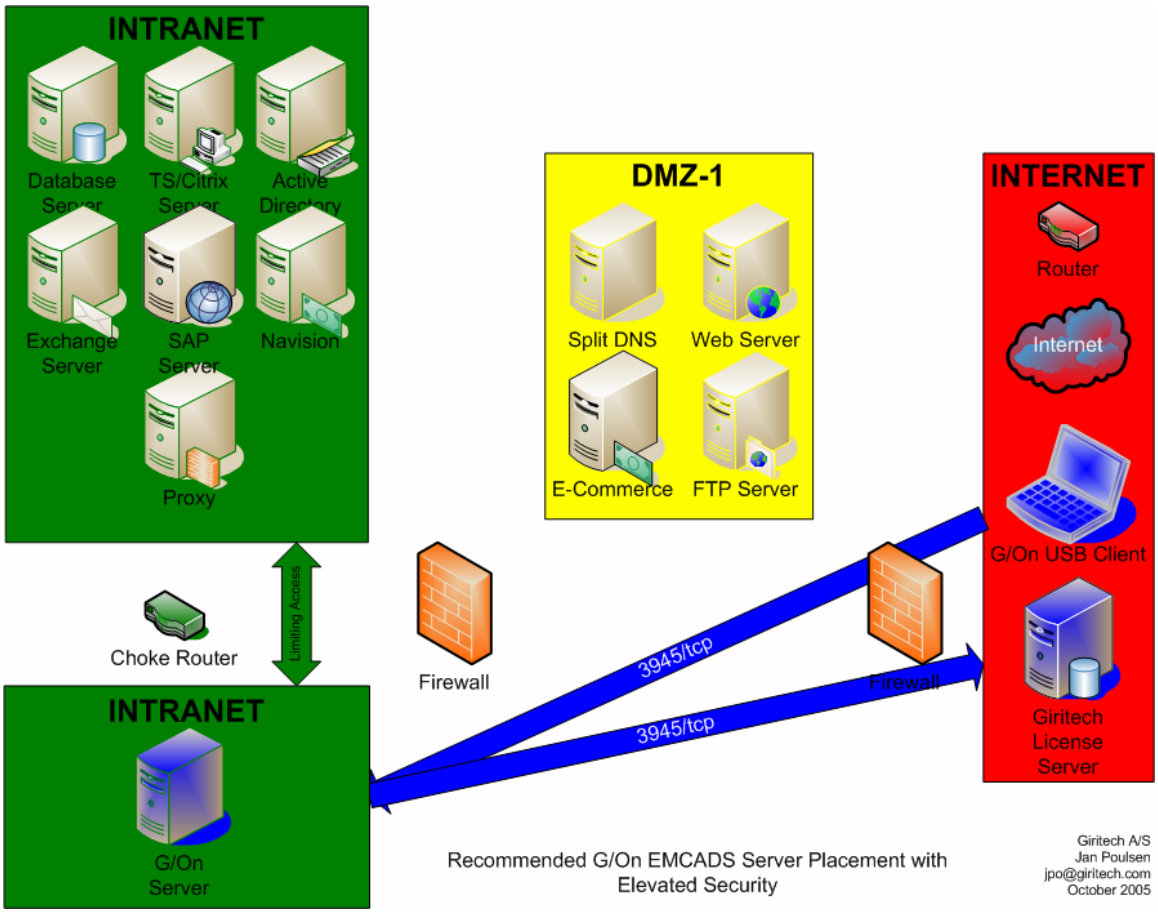
The G/On Server may be placed in the intranet with direct connectivity through the enterprise firewall to the Internet. This placement requires a single port on the firewall be configured to allow through traffic TCP. The Giritech IANA Registered default port is 3945. The server port is configurable and may be set to any port. If the G/On Server is configured to use another port, i.e. 443, the firewall must still be configured to allow outbound traffic on port 3945/tcp, to allow the G/On Server to contact the Giritech License Server, during the installation process. It is possible to utilize Port Address Translation (PAT) to allow different port configurations across firewalls.

This placement allows the G/On Server to connect to legacy systems without needing to open additional firewall ports. It is very important that the G/On Server be the only device allowed to connect through the firewall in this manner, in order to protect all other systems placed in the intranet, from being accessed directly from the Internet.

This placement also allows the G/On Server to authenticate users at the Active Directory (AD) without further configuration. This allows the AD administrator to make and remove users, disable accounts, apply group policies at the AD and sync to the G/On Server.
No password information is transferred to the G/On Server during sync.
Groups and user replicas are the only information passed to the G/On Server.

The default settings of the G/On Server represent a best practice approach. These settings can be customised to address in-house security policies.

Intranet with Elevated Security



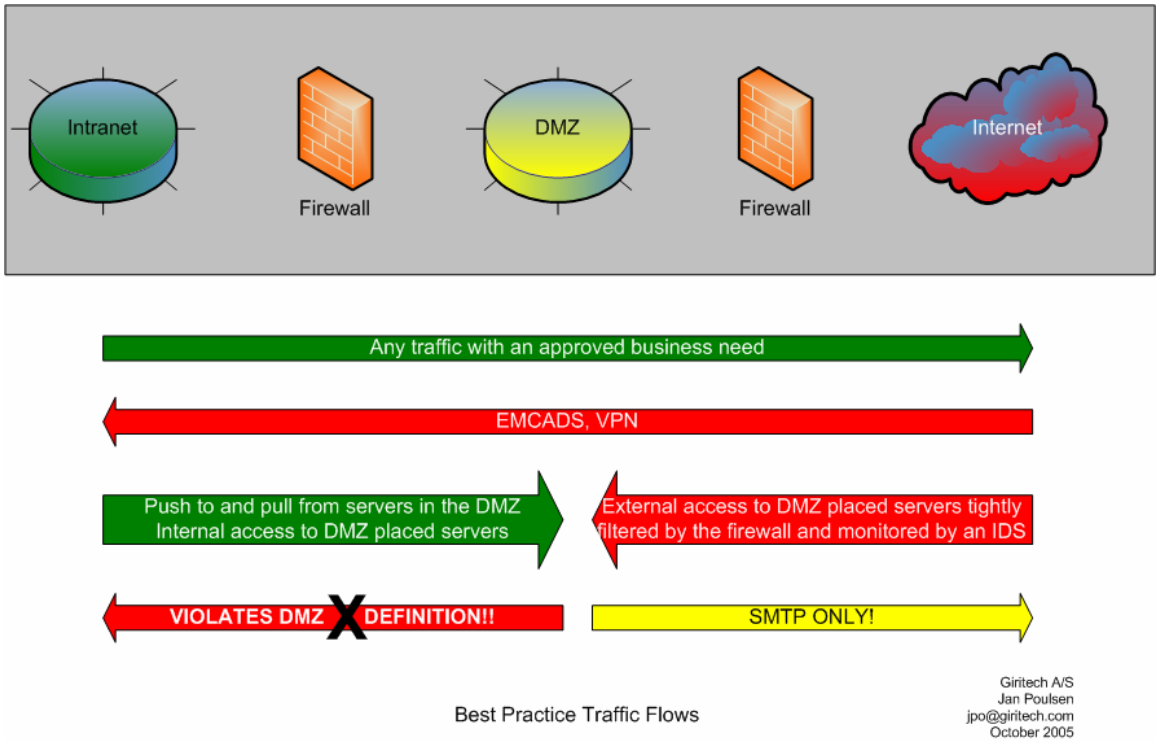
Depending on the type of environment the G/ON Server will be placed in, there may be elevated security consideration to be met. One such consideration is the fact that the G/On Server can be contacted directly from the Internet, which may be against the implemented security policy.

To limit and have better control over possible damage caused by an attack on the G/On Server, it is possible to place the G/On server on its own network segment, separated from the server farm by a choke router. The choke router is then configured with filters, allowing G/On Server access only to the servers it needs to communicate with, like the Active Directory, TS/Citrix Server, etc.

The G/On Server could also be attached on a separate network interface of the intranet firewall. Please note, this is **NOT** a DMZ, but simply a solution for more control, and better logging facilities, as this is often the case with firewalls compared to routers.

In the Demilitarized Zone (DMZ)

What is the definition of a DMZ?

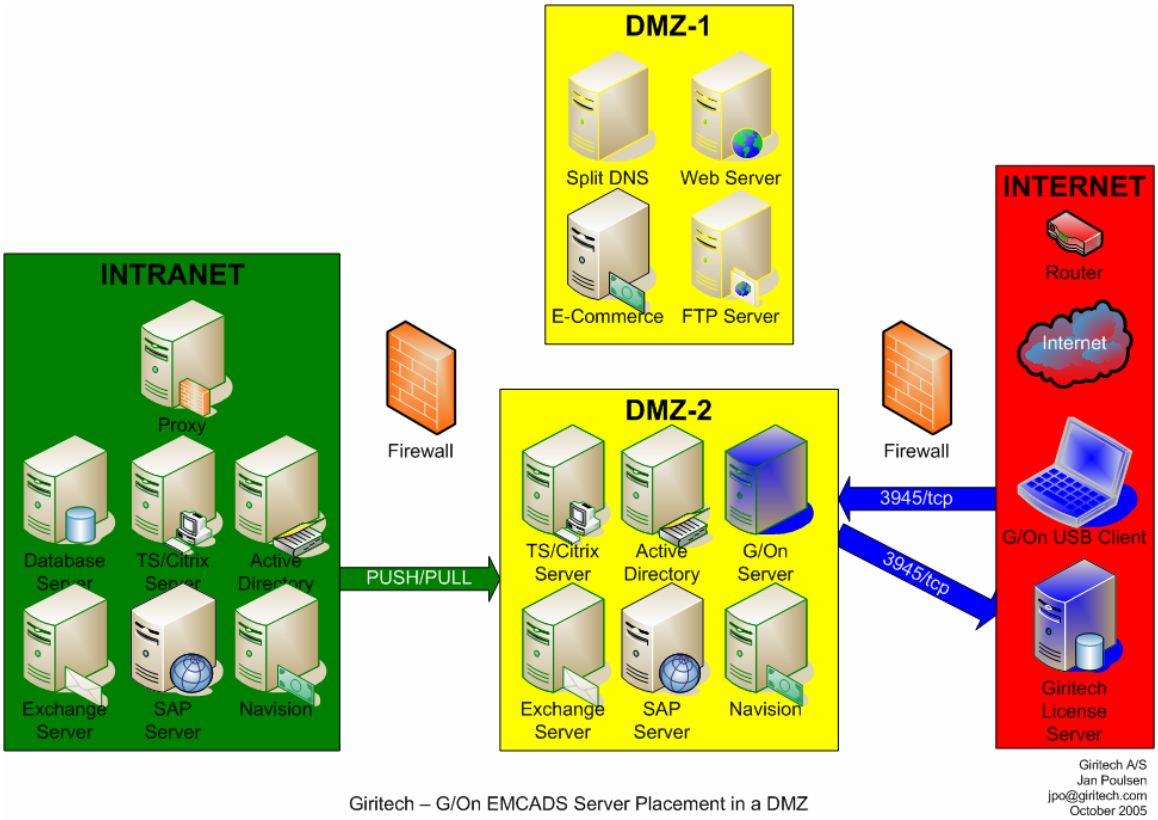


Demilitarized Zone (DMZ) – a buffer area between two enemies.

The definition of a DMZ is that no traffic originates from the DMZ. The DMZ can only answer a connection initiated outside the DMZ, and never initiate a connection of its own. The only exception to this rule is that in some cases, to simplify an e-mail solution, smtp (25/tcp) is allowed outbound from the DMZ.

By not permitting systems in the DMZ to establish outbound session, either to the Internet or intranet, DMZ systems are effectively prevented from initiating transfer of data from one zone to the other. As an example, if a DMZ placed system is compromised from the Internet, connections cannot be initiated to the intranet, effectively preventing the compromise from spreading to the intranet.

NB! Giritech does not recommend placing the G/On Server in a DMZ. To do it properly requires that all intranet systems, to be accessed, be duplicated to the DMZ, thereby increasing complexity and doubling administrative tasks. Placing duplicates of intranet systems in a DMZ also reduces the number of obstacles a hacker must pass to get to confidential data.



Giritech – G/On EMCADS Server Placement in a DMZ

The G/On Server may be placed in the DMZ with direct connection through the DMZ to the Internet. This placement requires a single port on the DMZ firewall to be configured to allow through traffic TCP. The Giritech IANA Registered default port is 3945. The server port is configurable and may be set to any port. If the G/On Server is configured to another port, i.e. 443, the firewall must also be configured to allow outbound traffic on port 3945, to allow the G/On Server to contact the Giritech License Server, during the installation process.

Using this placement requires that the systems and resources be replicated in the DMZ and that any synchronization from the intranet be pushed to the DMZ from the intranet. In other words the internal firewall must only contain outbound rules to allow synchronization to the DMZ systems.

This placement allows the G/On Server to connect to replicas of legacy systems without needing to open additional DMZ firewall ports. It is very important that the G/On Server be the only device that is allowed to connect through the DMZ firewall.

In order to synchronize the Active Directory (AD) from the G/On Server, the G/On Server **MUST** be a member of the domain.

The default settings of the G/On Server represent a best practice approach. These settings can be customised to address security policies.

References:

IANA Assigned Port Numbers

http://www.iana.org/assignments/port-numbers

Windows Server 2003 Security Guide

http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

Microsoft Baseline Security Analyzer (MBSA)

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

The Antivirus Defence-in-Depth Guide

http://www.microsoft.com/technet/security/topics/serversecurity/avdind_0.mspx

Intrusion Detection FAQ

http://www.sans.org/resources/idfaq/