Better Invisible than Agile: Application of RFC 1597

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 718 463 1079
gezelter@rlgsc.com

Thursday, December 7, 1995
1:00 pm – 1:50 pm
Room 309

Fall 1995 US DECUS Symposium
Moscone Convention Center
San Francisco, California

Better Invisible than Agile: Applications of RFC 1597
Slide 1

Robert Gezelter
Software Consultant 35 – 20 167th Street, Suite 215, Flushing, New York 11358 – 1731 USA
+1 718 463 1079

"Overall, he judged it to be better to be invisible than agile ..."

– Red Storm Rising

Robert Gezelter
Software Consultant

Routers filter packets based upon source and destination addresses and protocol type. Their efficacy is limited.

Robert Gezelter
Software Consultant

NOTES

Firewalls (bastion hosts) should be the exclusive "ports of entry" into your internal network.

Many assets are now addressable via IP, from printers to PBXes. It is highly undesireable that most of these resources be accessable from outside the security perimeter.

Robert Gezelter
Software Consultant

These concerns also apply to nested security environments.

Robert Gezelter
Software Consultant

NOTES

3

Enter RFC 1597 –
Address Allocation for
Private Internets

Robert Gezelter
Software Consultant

RFC 1597 is a scheme proposed to
reserve a portion of the
IPv4 address space for
guaranteed internal use in
publicly addressible networks.

Robert Gezelter
Software Consultant

NOTES

4

What is reserved by RFC 1597?

Guaranteed non-public allocation of:

- **1 Class A Address Block
  (10.0.0.0 – 10.255.255.255)**

- **16 Class B Address Blocks
  (172.16.0.0 – 172.131.255.255)**

- **255 Class C Address Blocks
  (192.168.0.0 – 192.168.255.255)**

Robert Gezelter
Software Consultant

RFC 1597 Intent

**Permit the connection of large
numbers of local devices to
LANs via IP without requiring
every LAN to hold a Class A
address space. It is worth
noting that even a private
residence could easily overflow
a Class C address space.**

Robert Gezelter
Software Consultant

NOTES

5

Implications of RFC 1597

- *Repeatedly sub-divideable*

- *internal nodes (workstations, servers, PCs) cannot connect to outside servers EXCEPT through an approved application proxy on an outside addressable host.*

- *inbound connections must go through approved proxies on the (externally visible) gateways*

- *internal nodes need not be renumbered due to changes in externally visible address ranges caused by CIDR adjustments and/or access provider changes.*

Robert Gezelter
Software Consultant

Router Configuration

- *Access Providers should filter the RFC 1597 Address Blocks*

- *Nested internal routers may filter addresses*

- *Your router outside your firewall should filter RFC 1597 addresses*

Robert Gezelter
Software Consultant

NOTES

Router Implications

- *Internal hosts (possibly nested) are invisible to systems outside the firewall*

- *Even if your router fails, the from address is ambiguous*

- *The previous note is not as safe as might be perceived, an attack on your link might be feasible.*

Robert Gezelter
Software Consultant

RFC 1597 and Domain Name Services

- *Internal DNS serving*

- *External DNS serving*

- *Implications*

Robert Gezelter
Software Consultant

NOTES

Internal DNS

- **Final authority on nodes inside the firewall**

- **Uses firewall to resolve external DNS**

Robert Gezelter
Software Consultant

External DNS

- **all internal mail targets are represented by MX records**

- **Internal nodes which are not to be addressed may be totally absent from the External DNS**

Robert Gezelter
Software Consultant

NOTES

DNS Implications

- *SMTP mail is forced to the route through the gateway*

- *FTP, TELNET, HTTP cannot even resolve the address of interior systems.*

Robert Gezelter
Software Consultant

Relationship Connectivity

- *RFC 1597 address can be used together with careful management to protect IP links with business and strategic partners*

- *Mutual distrust*

- *"No Man's" land*

Robert Gezelter
Software Consultant

NOTES

9

Summary

RFC 1597 provides and excellent framework for implementing an environment which enhances the safety support provided by your firewall(s)

Robert Gezelter
Software Consultant

Questions?

**Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America**

**+1 718 463 1079
gezelter@rlgsc.com**

Robert Gezelter   +1 718 463 1079
Software Consultant 35 – 20 167th Street, Suite 215, Flushing, New York 11358 – 1731 USA

NOTES