

Compatible Systems Tech Notes: IntraGuard Log Interpretation

Document ID: 17653

Introduction
Prerequisites
Requirements
Components Used
Conventions
Background Information
IntraGuard Log Interpretation
Related Information

Introduction

The log files for version 4.x does not provide as much detailed information as the version 5.x logs.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on IntraGuard all versions 5.x.

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

Background Information

Knowledge Base Article C000166

IntraGuard Log Interpretation

This information is only meant as a guide. To fully understand what this information means to a network, it is recommended that you refer to additional firewalling resources such as:

- Building Internet Firewalls by D. Brent Chapman and Elizabeth D. Zwicky. O'Reilly & Associates, 1995
- Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steven M. Bellovin. Addison-Wesley Publishing Company, Reading Massachusetts, 1994

Intraguard Log Files

Created – logs when a UDP or TCP session is created

Permit (est) – permit an established session back in

Redirected – packet redirected due to ICMP redirection

Free %d-%03x – frees up a finished session

P1, P2, ? indicates the path number. Look at the "show fire paths" command for a mapping of path names to path numbers. Paths indicate along which path this activity is being attempted.

-> Packets attempting to travel from the inside interface to the outside interface of a path.

<- Packets attempting to travel from the outside interface to the inside interface of a path.

Removing inactive sessions

UDP tmout – connection timeout due to inactivity

SYN Fail means that only half of the connection sequence was seen and the session was shut down. There is a well known attack that only sends a single SYN message to a server over and over with a different port number each time. This ties up all of the servers resources and is a denial of service attack. If all/many of the sessions logged with this server are from the same remote IP address, then suspect an attack: otherwise, consider increasing the SYN timer to eliminate some of the messages.

Half Shut – means that only half of the shutdown sequence was seen before the half shut timer killed the session.

FIN Fail – FIN Flag to tear down the TCP session was not acknowledged

TCP tmout – connection timeout due to inactivity

Sessions stopped by the filter

Reject EST – rejected an packet with an established flag because the session hadn't been created yet.

Reject nohash – NAT session returning without being requested first

Filtered – caught in the filter

Flt (n x) – "x" number of the same packets filtered

RA bad ver(x) – Set the PNA flag. Used for Real Audio.

```
Flags for the Port structure of the Intraguard
FULL_ACCESS          0x00000001          /* Port has full access to the bridge, no filters,
NO_ACCESS            0x00000002          /* Port has no access through the bridge */
BLOCK_IN_PACKETS    0x00000010          /* Block unknown inbound packets */
BLOCK_OUT_PACKETS   0x00000020          /* Block unknown outbound packets */
INITIALIZED          0x00000040          /* Path/Port has been initialized */
IN_FILTER_AND        0x00000100          /* Static AND filter inbound packets */
OUT_FILTER_AND       0x00000200          /* Static AND filter outbound packets */
IN_FILTER_OR         0x00000400          /* Static OR filter inbound packets */
OUT_FILTER_OR        0x00000800          /* Static OR filter outbound packets */
SEND_TCP_RST        0x00001000          /* Send TCP reset to rejected packets */
SEND_ICMP            0x00002000          /* Send ICMP message to rejected packets */
STCP_ICMP            0x00004000          /* Send ICMP message to rejected TCP packets */
RST_SYN_ONLY         0x00008000          /* Reset only TCP SYN rejects */
CHECK_FRAG           0x00010000          /* Check min IP fragment length */
```

```
FILT_SRCRT      0x00020000      /* Filter source routed packets */
PERMIT_EST      0x00040000      /* Allow established TCP sessions */
KILL_REDIRS     0x00080000      /* Kill session receiving ICMP redirects */
```

These Flags match the Free x-abc where x can either be a 0 (didn't send a reset packet) or 1 (sent a reset packet to the other end). Abc is a combination of the numbers above. For instance a P1 Free 0-012 would be freeing a session that was trying to be established on the way in and blocked because that particular port has no access for the P1 path.

Related Information

- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 03, 2004

Document ID: 17653
