NVC

IronPort パケットキャプチャ手順書

※各手順でコマンド入力前にEnterキーを押下してしまった場合は、
一つ前の手順からやりなおしてください。

1. IronPortのCLIにログインしてください。

2. コマンド「 diagnostic 」を実行し、以下のような出力がされることを確認してください。

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - NETWORK Utilities.
- REPORTING - REPORTING Utilities.
- TRACKING - TRACKING Utilities.
[ ] >

3. コマンド「 NETWORK 」を実行し、以下のような出力がされることを確認してください。

Choose the operation you want to perform:
- FLUSH - FLUSH all NETWORK related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[ ] >

4. コマンド「 TCPDUMP 」を実行し、以下のような出力がされることを確認してください。

- START - START packet capture
- STOP - STOP packet capture
- STATUS - STATUS capture
- FILTER - Set packet capture FILTER
- INTERFACE - Set packet capture INTERFACE
- CLEAR - Remove previous packet captures
[ ] >

5. コマンド「 FILTER 」を実行し、以下のような出力がされることを確認してください。

Enter filter: [tcp and port 80]

6. "(tcp or udp) and (port ***)"の形式でフィルタ条件を入力し、"New filter:"の値が変更されることを確認してください。全てのパケットをキャプチャする場合は"all"と入力してください。

以下は「 TCP ポート389番または443番 」のパケットをキャプチャする条件を入力した際の例です。

New filter: tcp port 389 or tcp port 443
- START - START packet capture
- STOP - STOP packet capture
- STATUS - STATUS capture
- FILTER - Set packet capture FILTER
- INTERFACE - Set packet capture INTERFACE
- CLEAR - Remove previous packet captures
[ ] >

7. コマンド「 INTERFACE 」を実行し、以下のような出力がされることを確認してください。

Enter INTERFACE: [Management]

8. キャプチャを行うインターフェイス名を入力し、"Setting Capture Interface to"の値が
変更されることを確認してください。

※以下は「Data(半角スペース)1」を指定した際の例です。

Enter INTERFACE: [Management] Data 1
Setting Capture Interface to Data 1
- START - START packet capture
- STOP - STOP packet capture
- STATUS - STATUS capture
- FILTER - Set packet capture FILTER
- INTERFACE - Set packet capture INTERFACE
- CLEAR - Remove previous packet captures
[ ] >

9. コマンド「START」を実行し、以下のような出力がされることを確認してください。

Capture started

- START - START packet capture
- STOP - STOP packet capture
- STATUS - STATUS capture
- FILTER - Set packet capture FILTER
- INTERFACE - Set packet capture INTERFACE
- CLEAR - Remove previous packet captures
[ ] >

10. キャプチャ対象となる通信を発生させてください。

11. コマンド「STOP」を実行し、以下のような出力がされることを確認してください。

Stopping Capture

- START - START packet capture
- STOP - STOP packet capture
- STATUS - STATUS capture
- FILTER - Set packet capture FILTER
- INTERFACE - Set packet capture INTERFACE
- CLEAR - Remove previous packet captures
[ ] >

12. FTPでアクセスし、以下のディレクトリ内にあるファイルをダウンロードしてください。
※この間、CLIにアクセスしている画面は終了しないでください。

ディレクトリパス：/diagnostic

13. CLIに戻ってコマンド「CLEAR」を実行し、以下のような出力がされることを確認してください。
※ファイルが複数存在する場合には、同様の表示が続きます。

Do you want to remove (tcp_and_port_389_or_443.cap): [N]

14.「Y」と入力することでファイルが削除されます。

15. Enterキーを3回押下した後に、コマンド「EXIT」を実行してログアウトしてください。

以上