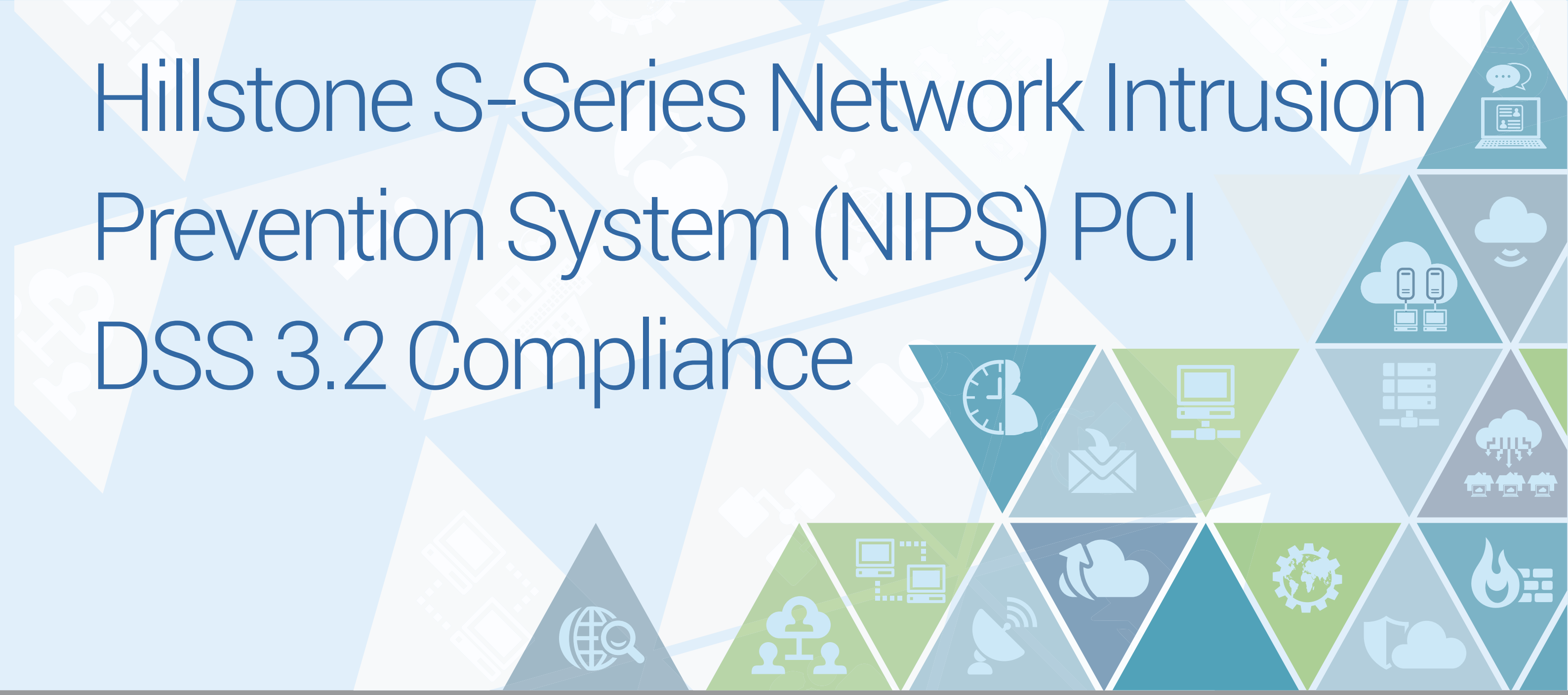
Hillstone NETWORKS

Hillstone S-Series Network Intrusion Prevention System (NIPS) PCI DSS 3.2 Compliance



Keywords: Payment Card Industry (PCI), Data Security Standard (DSS), DSS 3.2 Compliance, Hillstone S-Series Network Intrusion Prevention System (NIPS), cardholder data environment (CDE), Intrusion Prevention System (IPS), anti-virus (AV), anti-malware, encryption, Public Key Infrastructure (PKI), Virtual Private Network (VPN).

Abstract: This paper discusses PCI DSS 3.2 security requirements compliance of cardholder information when it is transmitted electronically across private and public network connections and how Hillstone's S-Series Network Intrusion Prevention System (NIPS) appliance can help your organization comply with these requirements.

1 Overview

As the threat landscape continues to evolve aggressively, an increasing number of network protection technologies have emerged. Among these technologies, an Intrusion Prevention System (IPS) remains one of the most widely deployed solutions, regardless of platform or form factor. Rapid growth in network information technologies, network size, and corporate business applications result in networks and data centers that are continuously under attack by increasingly creative and sophisticated methods.

Standards and requirements such as the Payment Card Industry Data Security Standard (PCI DSS) strive to improve the overall security of stored and transmitted payment card data and transactions in distributed networks and data centers of enterprises and governments.

2 PCI DSS Requirements

The PCI DSS standards were developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data.

PCI DSS 3.2 includes six control objectives, and twelve requirements.

Control Objective	Requirement
1. Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
2. Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.

3.Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
4. Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
5. Regularly Monitor and Test Networks	10.Track and monitor all access to network resources and cardholder data. 11.Regularly test security systems and processes.
6. Maintain an Information Security Policy	12.Maintain a policy that addresses information security for all personnel.

3 Hillstone NIPS Features

The PCI DSS standards provide an actionable framework for developing a robust payment card data security process—including prevention, detection and appropriate reaction to security incidents.

Hillstone offers and range of sophisticated, high-performance hardware- and software-based security products, including an IPS appliance (NIPS). An IPS system is a fundamental security element in any data center or computer network, and helps to offer compliance with the PCI DSS standard.

All traditional IPS features are supported, including (but not limited to):

- **Intrusion Detection and Protection**
    - o 7,000+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
    - o IPS actions: monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
    - o Packet logging
    - o Filter-based selection: severity, target, OS, application or protocol
    - o IP exemption from specific IPS signatures
    - o IDS sniffer mode
    - o IPv4 and IPv6 rate-based DoS protection with threshold settings for TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, and TCP/UDP/SCIP/ICMP session flooding (source/destination)

  - Active bypass with bypass interfaces
  - Predefined prevention configuration
- Anti-Virus (AV)
  - Over 10 million AV signatures
  - Flow-based anti-virus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP
  - Zip-file virus scanning
- **URL Filtering**
  - Flow-based web filtering inspection
  - Dynamic web filtering with a cloud-based real-time categorization database: over 140 million URLs with 64 categories (8 of which are security related)
  - Web filtering profile override: allows administrator to temporarily assign different profiles to user/group/IP
  - Web filter local categories and category rating override
  - Proxy avoidance prevention: proxy site category blocking, rate URLs by domain and IP address, block redirects from cache and translation sites, proxy avoidance application blocking, proxy behavior blocking (IPS)
- **Application Control**
  - Over 3,000 applications that can be filtered by name, category, subcategory, technology and risk
  - Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
  - Actions: block, monitor
  - Provide multi-dimensional monitoring and statistics for applications running in the cloud, including risk category and characteristics
- **High Availability (HA)**
  - Redundant heartbeat interfaces
  - Active/Active and Active/Passive
  - Standalone session synchronization
  - HA reserved management interface
- **Visible Administration**
  - Management access: HTTP/HTTPS, SSH, telnet, console
  - Central Management: Hillstone Security Manager (HSM), web service APIs
  - Multi-factored authentication: username/password, HTTPS certificates file
  - System Integration: SNMP, syslog, alliance partnerships
  - Rapid deployment: USB auto-install, local and remote script execution
  - Dynamic real-time dashboard status and drill-in monitoring widgets

  - Storage device management: storage space threshold customization and alarm, old data overlay, stop recording

- **Logging and Reporting**
  - Logging facilities: local memory and storage, multiple syslog servers and multiple Hillstone Security Audit (HSA) platforms
  - Encrypted logging and log integrity with HSA scheduled batch log uploading
  - Reliable logging using TCP option (RFC 3195)
  - Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets
  - Comprehensive event logs: system and administrative activity audits, routing and networking, VPN, user authentications, Wi-Fi related events
  - IP and service port name resolution option
  - Brief traffic log format option
  - Granular Reporting with User Targeted Viewpoints
    - HA Management/C-level View
    - Business System Owner View
    - Network Security Administrator View

4 Hillstone NIPS DSS 3.2 Compliance Summary

The PCI Security Standards Council offers robust and comprehensive standards to enhance payment card data security, specifically the PCI DSS 3.2 standard.

The following table summarizes the Hillstone NIPS features that can help you implement compliance with the PCI DSS 3.2 standard, specifically:

- Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs, including sub-requirements 5.1.1, 5.2 and 5.4.
- Requirement 6: Develop and maintain secure systems and applications, including sub-requirements 6.1, 6.5.2 and 6.6.
- Requirement 10: Track and monitor all access to network resources and cardholder data, including sub-requirements 10.6 and 10.8.
- Requirement 11: Regularly test security systems and processes, including sub-requirements 11.3.4 and 11.4.

Control Objective	Requirement	Hillstone NIPS Solution
1. Build and Maintain a Secure Network and Systems	1.Install and maintain a firewall configuration to protect cardholder data.	The Hillstone NIPS is a complementary security element to a firewall. It provides deep packet inspection, monitoring, blocking, session resetting, URL filtering, and sophisticated anti-virus checking of all inbound traffic accessing networks that contain cardholder data. Security policies configured on the Hillstone NIPS help protect and implement a DMZ to prohibit direct public access between the CDE system and the Internet. See section **6.1 Security Policies.**
	2.Do not use vendor supplied defaults for system passwords and other security parameters.	Hillstone NIPS requires user authentication and uses strong encryption for remote administration and all non-console sessions. This includes direct access and through the Hillstone centralized management system HSM. See section **6.2 User Authentication.**
2. Protect Cardholder Data	3. Protect Stored Cardholder data.	No cardholder data is stored on the Hillstone NIPS. The NIPS provides anti-virus, anti-malware, packet inspection, application protocol inspection, user authentication, URL/web filtering, encryption, and session and event logging to protect access to cardholder data stored on a system behind the NIPS. See section **6.1 Security Policies.** See section **6.3 Reporting and Logging.**
	4. Encrypt Transmission of cardholder data across open, public networks.	PKI infrastructure and VPNs are supported. See section **6.4 Encryption.**

3.Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs.	The Hillstone NIPS provides 7,000+ IPS signatures; protocol anomaly detection; rate-based detection; custom signatures; manual, automatic push or pull signature updates; and an integrated threat encyclopedia. Anti-virus capabilities include over 10 million AV signatures; flow-based anti-virus checking on protocols including HTTP, SMTP, POP3, IMAP, FTP/SFTP; support for zip-file virus scanning. See section **6.5 Threat Protection.**
	6. Develop and Maintain secure systems and applications.	The Hillstone NIPS supports prevention, detection and blocking of attacks, as well as sophisticated risk-based application filtering and reporting to aid in application-based security enforcement of your network. See section **5 Hillstone NIPS Reporting Examples for PCI DSS Compliance** See section **6.5 Threat Protection.**
4. Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know.	Granular application control and filtering aids in implementing detailed access control to cardholder data. Role-based user access to the Hillstone NIPS device is supported. See section **6.1 Security Policies.** See section **6.2 User Authentication.**
	8. Identify and authenticate access to system components.	Hillstone NIPS authenticates users by username, password, and HTTPS certificates. See section **6.2 User Authentication.**
	9. Restrict physical access to cardholder data.	N/A

5. Regularly Monitor and Test Networks	10. Track and Monitor all access to network resources and cardholder data.	The Hillstone NIPS includes HD storage to maintain logs, audit information and reports, including security events, server and application attack and threat information, as well as traffic and system resource information. Bundled with HSM, customized reporting capabilities can be provided. See section 5 Hillstone NIPS Reporting Examples for PCI DSS Compliance See section 6.3 Reporting and Logging.
	11. Regularly test security systems and processes.	The Hillstone NIPS deep packet inspection monitors, blocks, and mitigates identified threats. Events and incidents are logged and reported. Granular reports are available for auditing and follow-up. See section 6.3 Reporting and Logging.
6. Maintain an Information Security Policy	12.Maintain a policy that addresses information security for all personnel.	N/A

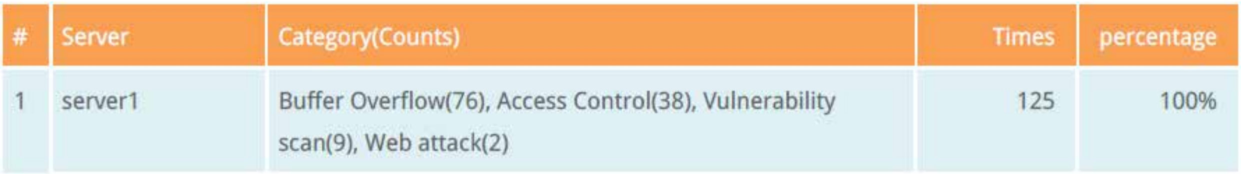
5 Hillstone NIPS Reporting Examples for PCI DSS Compliance

NIPS reports are generated for a given period of time, and provide summary and detailed information for the requested period that can help you with auditing and verifying PCI DSS compliance. Reports include:

- Security Risk Summary: Overall risk situation of servers, users and the business.
- Security Risk Detail: Observed server and user attacks.
- Risk Type Summary: Type and impact of the threats detected.
- Network Flow Analysis: User, application, interface, and zone traffic information.
- System Resource Situation: Lists CPU, memory, disk usage.

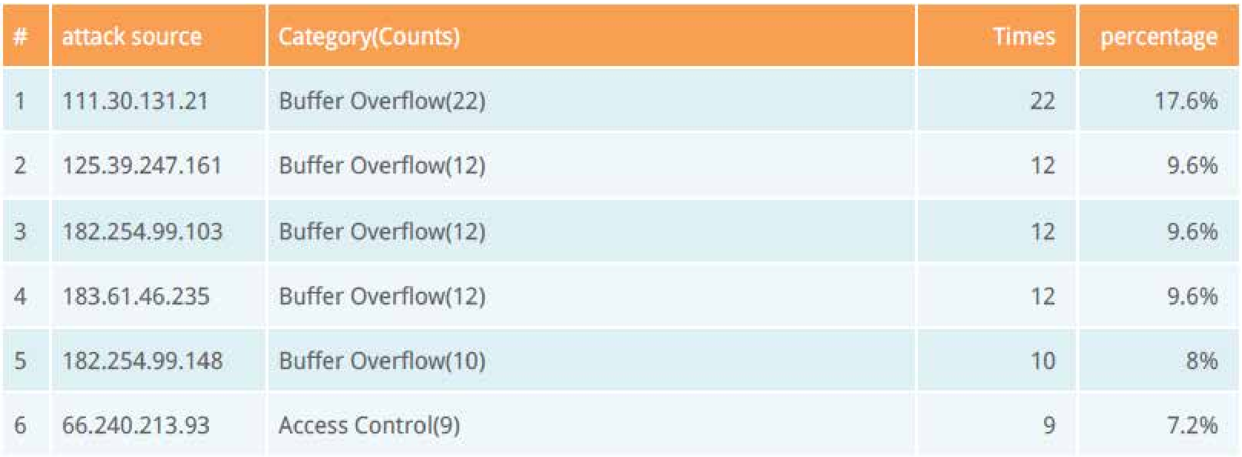
Server Security Risk Example

The report provides a ranked list of attacked servers.



#	Server	Category(Counts)	Times	percentage
1	server1	Buffer Overflow(76), Access Control(38), Vulnerability scan(9), Web attack(2)	125	100%

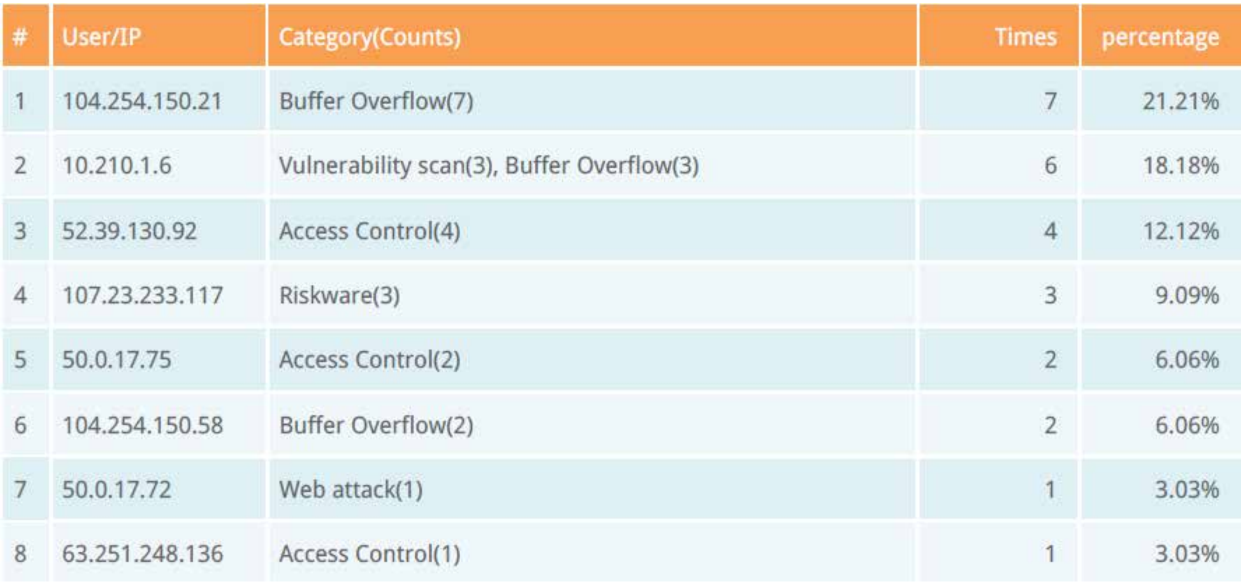
Additional information on server attacks is reported as shown below in an excerpt from the detailed section of the report.



#	attack source	Category(Counts)	Times	percentage
1	111.30.131.21	Buffer Overflow(22)	22	17.6%
2	125.39.247.161	Buffer Overflow(12)	12	9.6%
3	182.254.99.103	Buffer Overflow(12)	12	9.6%
4	183.61.46.235	Buffer Overflow(12)	12	9.6%
5	182.254.99.148	Buffer Overflow(10)	10	8%
6	66.240.213.93	Access Control(9)	9	7.2%

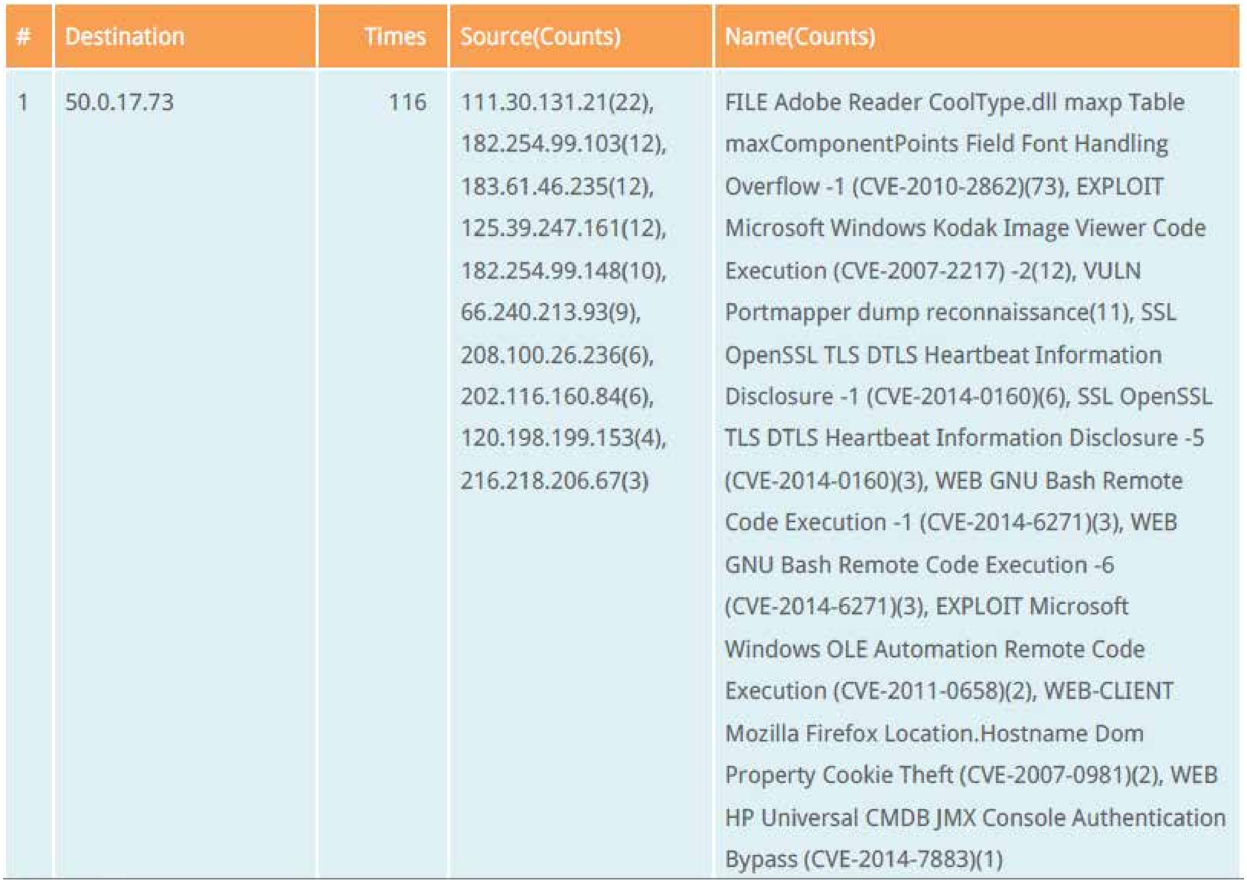
User Security Risk Example

The report provides a ranked list of attacked users (IP addresses).



#	User/IP	Category(Counts)	Times	percentage
1	104.254.150.21	Buffer Overflow(7)	7	21.21%
2	10.210.1.6	Vulnerability scan(3), Buffer Overflow(3)	6	18.18%
3	52.39.130.92	Access Control(4)	4	12.12%
4	107.23.233.117	Riskware(3)	3	9.09%
5	50.0.17.75	Access Control(2)	2	6.06%
6	104.254.150.58	Buffer Overflow(2)	2	6.06%
7	50.0.17.72	Web attack(1)	1	3.03%
8	63.251.248.136	Access Control(1)	1	3.03%

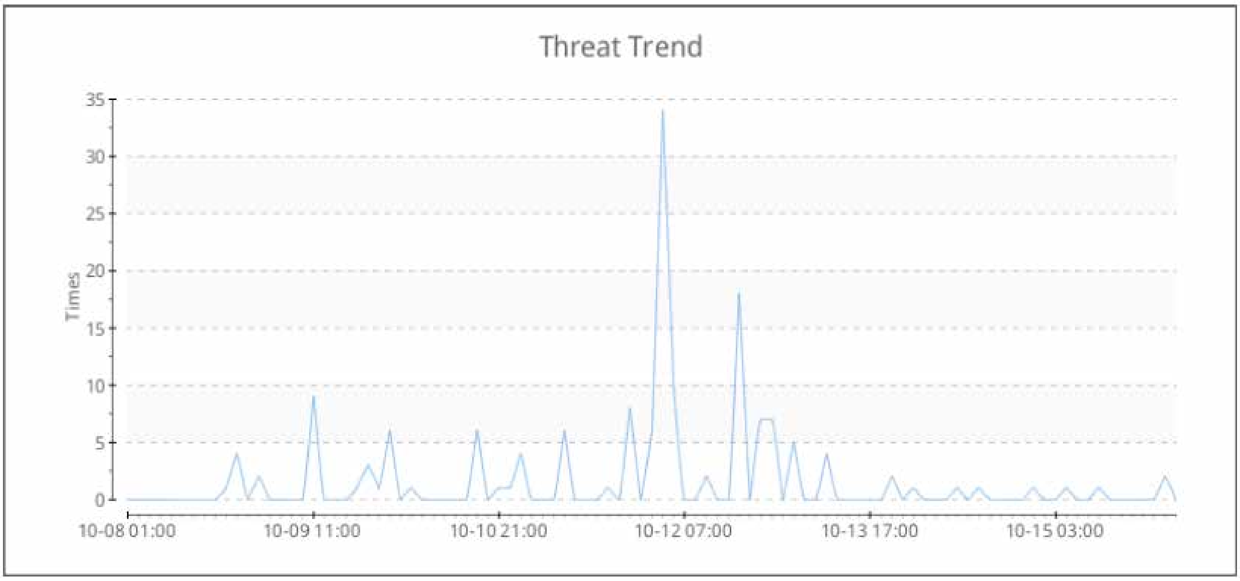
Additional information on user attacks is reported as shown below in an excerpt from the detailed section of the report.



#	Destination	Times	Source(Counts)	Name(Counts)
1	50.0.17.73	116	111.30.131.21(22), 182.254.99.103(12), 183.61.46.235(12), 125.39.247.161(12), 182.254.99.148(10), 66.240.213.93(9), 208.100.26.236(6), 202.116.160.84(6), 120.198.199.153(4), 216.218.206.67(3)	FILE Adobe Reader CoolType.dll maxp Table maxComponentPoints Field Font Handling Overflow -1 (CVE-2010-2862)(73), EXPLOIT Microsoft Windows Kodak Image Viewer Code Execution (CVE-2007-2217) -2(12), VULN Portmapper dump reconnaissance(11), SSL OpenSSL TLS DTLS Heartbeat Information Disclosure -1 (CVE-2014-0160)(6), SSL OpenSSL TLS DTLS Heartbeat Information Disclosure -5 (CVE-2014-0160)(3), WEB GNU Bash Remote Code Execution -1 (CVE-2014-6271)(3), WEB GNU Bash Remote Code Execution -6 (CVE-2014-6271)(3), EXPLOIT Microsoft Windows OLE Automation Remote Code Execution (CVE-2011-0658)(2), WEB-CLIENT Mozilla Firefox Location.Hostname Dom Property Cookie Theft (CVE-2007-0981)(2), WEB HP Universal CMDB JMX Console Authentication Bypass (CVE-2014-7883)(1)

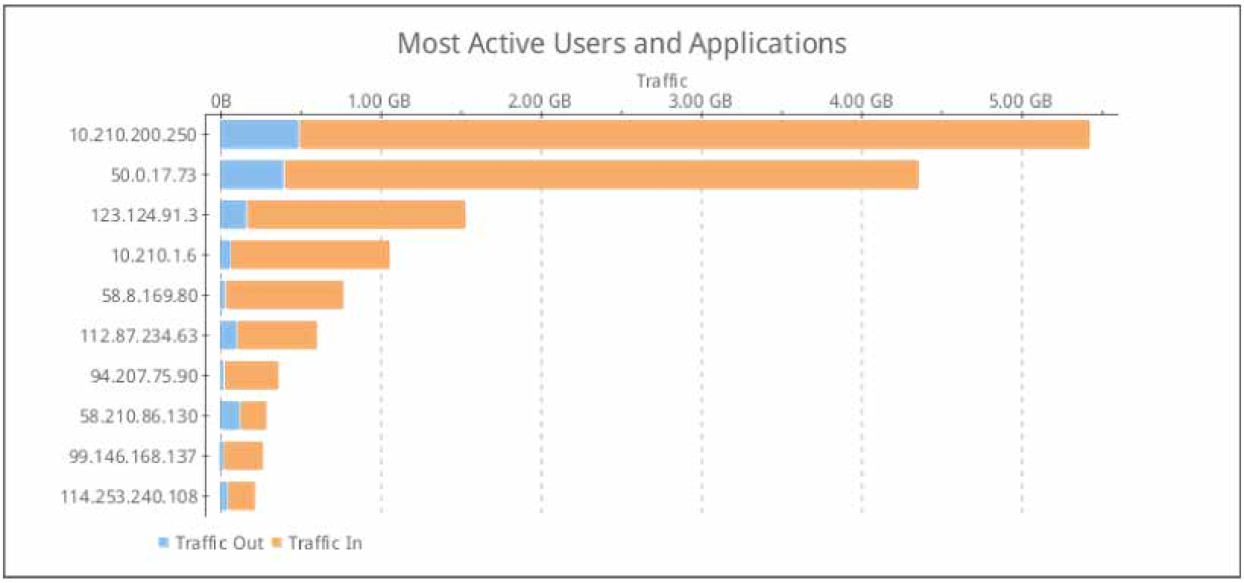
Overall Business Security Risk Example

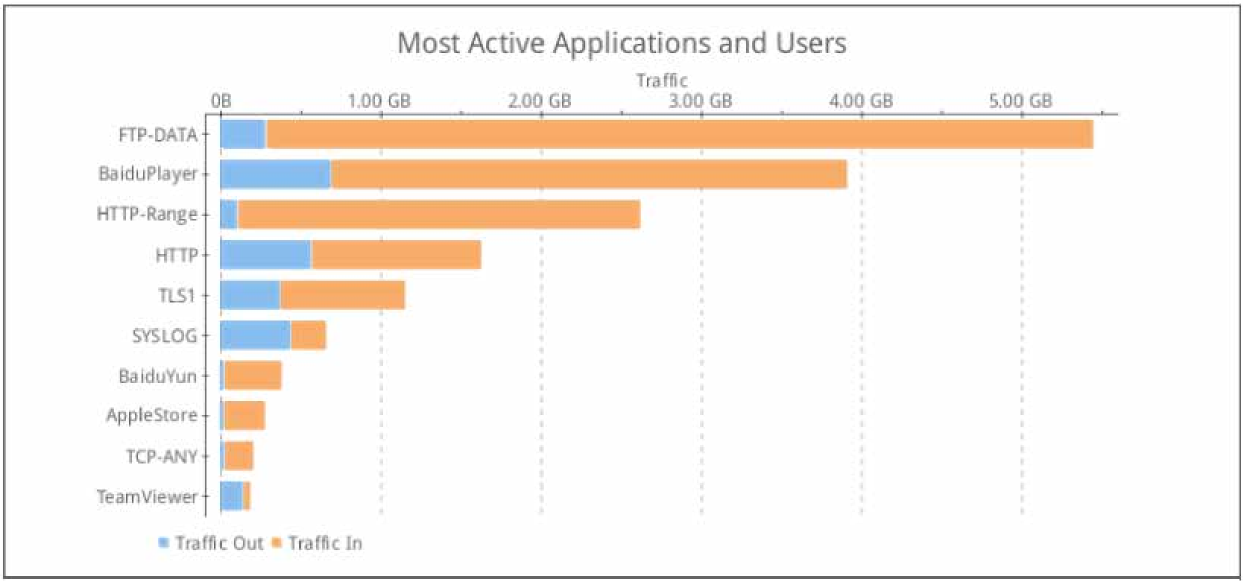
In this example report, a total of 158 attacks occurred during the reporting period of 8 Oct 2016 01:00 to 15 Oct 2016 03:00. During the most active period, 12 Oct 2016 03:00-05:00, 34 attacks occurred.



Network Flow Example

The report provides a traffic summary of users and applications.



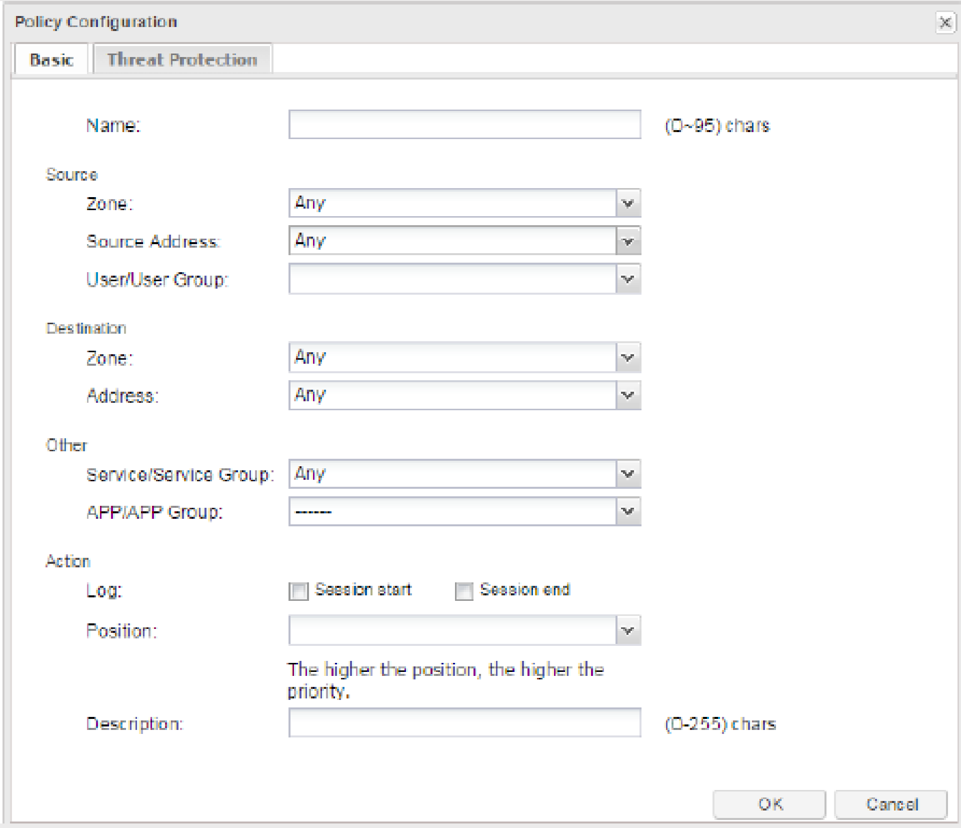


#	User/IP	Total Stream	Traffic Out	Traffic In	Application(Total/Out/In)
1	10.210.200.250	5.41GB	490.25MB	4.94GB	FTP-DATA(4.72GB/107.77MB/4.61GB), HTTP(395.16MB/345.14MB/50.01MB), TCP-ANY(205.68MB/2.96MB/202.72MB), TeamViewer(54.41MB/25.82MB/28.59MB), TLS1(23.57MB/6.12MB/17.46MB), WindowsUpdate(19.35MB/380.28KB/18.98MB), SourceForge-Download(6.71MB/136.78KB/6.58MB), HTTP-Range(2.35MB/48.49KB/2.30MB), BaiduPlayer(2.07MB/863.93KB/1.23MB), 360Security(1.15MB/274.55KB/908.17KB)

6 Hillstone NIPS Configuration for PCI DSS Compliance

6.1 Security Policies

Security policies control traffic forwarding between security zones or segments—by default all traffic between security zones/segments is denied. Policies can be specified for NAT, session limits, ARP defense, URL filtering, and a global blacklist to block traffic can be configured.



Policy Configuration

Basic | Threat Protection

Name: (0~95) chars

Source

Zone: Any

Source Address: Any

User/User Group:

Destination

Zone: Any

Address: Any

Other

Service/Service Group: Any

APP/APP Group: ------

Action

Log: □ Session start □ Session end

Position:

The higher the position, the higher the priority.

Description: (0-255) chars

6.2 User Authentication

Multi-factored HTTPS-based authentication is supported. When a user logs in via HTTPS, the system verifies the certificate and password. To enable HTTPS-based authentication:

- Enable certificate authentication under System > Device Management > Management Interface. In the Web section, select Enable for Certificate authentication.
- Import the certificate to the Web browser under System > PKI.

User expiration is supported to allow specific users to authenticate into the system only up to a pre-determined date and time.

AAA authentication is supported (select Policy > AAA Server), and local users of the device can be bound to a specific IP or MAC address.

Role-based user configuration is supported to allow certain users access only to certain device capabilities and network resources.

User access can be monitored and logged by configuring Monitor > Authentication User.

6.3 Reporting and Logging

Comprehensive event logs are provided, including:

- System logs: running status of the device, and information for analysis and evidence.
    - o Event: logs about the system, e.g. ARP logs and login logs.
    - o Network: logs about network services, e.g. DHCP logs and route logs.
    - o Configuration: logs about configuration, e.g. interface configuration logs.
- Threat logs: information on behaviors threatening the protected system, e.g. attack defense logs, AV logs, and IPS logs.
- Session: information on session protocols, source and destination IP addresses and ports.
- NAT: information on NAT type, source and destination IP addresses and ports.
- URL: information on network surfing, e.g. Internet site access time, web page access history, and URL filtering logs.

6.4 Encryption

PKI is supported and used in the following situations:

- VPN tunnels
- User access over HTTPS or SSH

6.5 Threat Protection

The Hillstone NIPS device can prevent, detect and block network threats by configuring threat protection policies and rules, including:

- Anti-virus: detect common file and protocol types most likely to contain viruses.
- Intrusion Prevention: detect and protect against application layer protocols, web-based, and common Trojan attacks.
- Attack Defense: detect network attack types and take appropriate actions against the attack.

Threat protection configurations are based on policies, security zones and traffic flows in and out of the zones.

7 Conclusion

Hillstone's Network Intrusion Prevention System (NIPS) appliance provides rich prevention, detection, reporting and security incidents investigation features. These features help your organization comply with the PCI DSS 3.2 standard to provide a safer and more secure environment to cardholders and cardholder transactions.