

TippingPoint Network Access Control (NAC)

IPS-Secured Networks

DATASHEET – NAC



As organizations strive to provide anytime, anywhere access to users throughout the value chain, they expose their networks to malicious threats and targeted attacks. An organization's ability to manage user access and endpoint security is a critical component to ensuring the overall security and availability of its IT infrastructure. To address these challenges, TippingPoint provides an easy to manage, comprehensive network access control (NAC) solution that provides a means to confirm user and endpoint identity and verify device health prior to granting access to the network and its resources. TippingPoint NAC provides multiple methods of enforcement including 802.1X, DHCP and in-line blocking, allowing customers to centrally manage a combination of the appropriate enforcement types given their network topology and access control priorities.

Features and Benefits

- Reduce Network Vulnerabilities
- Reduce the Cost and Complexity of Implementing NAC
- Virtually Transparent to Existing Users Without Network Upgrades
- Improved Visibility and Reporting of Network Usage and Access

Comprehensive NAC Solution

- Identity-Based Policy Management
- Endpoint Posture Checks
- Access Policy Enforcement
- Historical Reporting

"TippingPoint NAC easily integrated into my Novell eDirectory without having to make any changes on the directory server or add additional network equipment. Getting the DHCP enforcement working required very little effort. Students were able to use the system quickly without swamping our support center."

Michael Blaisdell
ITS Network Administrator
Saint Francis University

Reduce Network Vulnerabilities

Keep Unauthorized Users and Devices off the Network

TippingPoint NAC access policies subject each device and user pair to rigorous authentication, authorization and security posture compliance checks. Unauthorized users are prevented from accessing the network and non-compliant devices are directed to remediate based on discovered vulnerabilities before access is granted. These measures give IT administrators granular control over who and what gains access to specific network resources.

Restrict Access Based on Role, Device Type, Posture, Location and Time of Day

Define access policies for individual users and devices or user and device groups. These policies provide the ability to control access by endpoint posture, location and time of day.

Use Multiple Enforcement Options – 802.1X, DHCP and In-Line Blocking

A single TippingPoint NAC Policy Server enables policy management across the entire network using a variety of enforcement methods including 802.1X and DHCP authentication, in-line enforcement with the TippingPoint NAC Policy Enforcer appliance, and any combination thereof.

Eliminate Unauthorized Access in Conference Rooms and Wireless Networks

The NAC Policy Server provides provisioning of internal users, guests and remote employees. The NAC Policy Server spans the entire network and allows administrators to provide appropriate access policies for single-day and/or long-term

guests. Features enabling guest access control include customizable captive login portal, local account creation and a dissolvable posture agent that does not require administrative rights to perform the security compliance checks.

Pre- and Post-Connect Endpoint Monitoring Reduces Risk of Malware Introductions

The TippingPoint NAC solution provides for both pre- and post-connect endpoint posture monitoring to prevent possible malware introductions into the network. Any non-compliant device is directed to remediate based on discovered vulnerabilities before access is granted.

IPS Integration Ensures Post-Connect Inspection of All Data Flows and Content

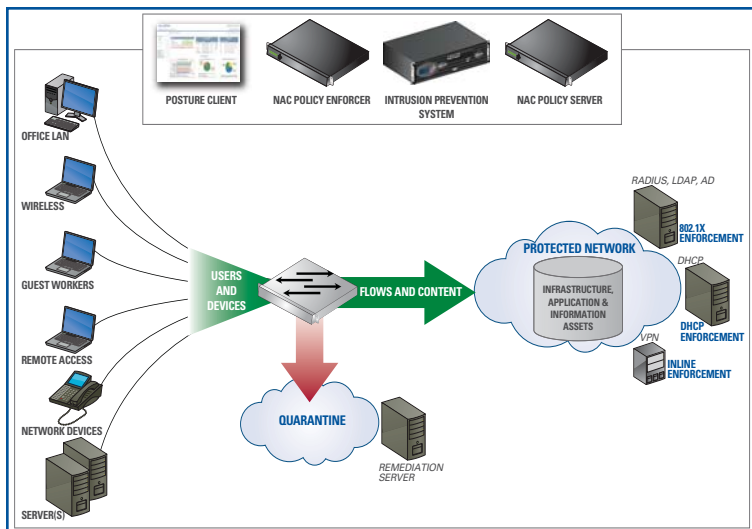
TippingPoint NAC interoperates with the TippingPoint Intrusion Prevention System (IPS) to ensure malicious traffic from any connected endpoint is blocked, and suspect or non-compliant traffic triggers policy-controlled actions including blocking, quarantining, alerting or rate shaping. A layered security approach combining NAC and in-line IPS gives security personnel unprecedented abilities to automatically enforce network access and security policies across all users, devices, traffic flows and content.

Reduce the Cost and Complexity of Implementing NAC

Flexible Deployment Options Ease Implementation and Ramp-Up

The TippingPoint NAC solution provides the flexibility to deploy network access control in an endless variety of configurations so

TippingPoint[®]



organizations can start small with simple deployments in highly exposed or less critical network segments and expand incrementally.

Single Web-Based Management Console
A single Web-based management console allows administrators to easily manage the entire NAC solution regardless of the authentication and enforcement options in use. A single TippingPoint NAC Policy Server appliance can be used to

manage access for up to 10,000 endpoints.

Simple Policy Creation and Management

The NAC Policy Server management console provides a very intuitive, easy-to-use administrator interface for the creation of new access policies and on-going management of existing policies. This minimizes errors in policy creation and speeds the overall deployment time of the solution.

Reduce IT Involvement in Guest Worker Set-Up

Provision intelligent, client-less guest access and create, group and control multiple tiers of guests such as contractor workers, mobile employees, and onsite visitors without making changes to the existing network infrastructure. Set-up of guest worker endpoint remediation reduces on-going IT workloads and costs.

Detailed Alerts Expedite Access Issue Recognition and Resolution

Immediate problem notification coupled with detailed drill-down reports reduce the time required for IT personnel to identify and resolve access issues, such as multiple user authentication failures, unknown devices attempting access or system health issues.

Virtually Transparent to Existing Users Without Network Upgrades

Seamless Active Directory Windows Login and Support for Mac and Linux

The TippingPoint NAC solution supports a seamless Active Directory login process for Windows (2000, XP, and Vista). The solution is also completely compatible with Macintosh (10.x) and Linux operating systems allowing organizations to ensure device compliance. Posture compliance checks verify operating system type, patch levels and hot fixes for these systems prior to granting access.

Support for Hundreds of AV, Anti-Spyware and Personal Firewall Software Packages

The TippingPoint NAC solution provides built-in checks in its posture assessment for hundreds of anti-virus, anti-spyware and personal firewall software packages. Posture compliance checks verify the following:

- AV and Anti-Spyware product, vendor and version
- AV and Anti-Spyware engine version
- AV and Anti-Spyware data file version and time
- Personal Firewall product, vendor and version
- Verification of AV, Anti-Spyware, and Personal Firewall software enabled and actively protecting the endpoint.

Dissolvable Posture Checking Client is Transparent to Users

Posture compliance checks are managed through the Web-based console and can be performed using either persistent or dissolvable posture checking client software. In addition, the posture check can be configured to require only a pre-connect check or both pre-connect and post-connect checks. The post-connect posture compliance check intervals are fully configurable.

No Network Upgrade Requirements

Because the TippingPoint NAC solution integrates with existing authentication databases and leverages existing network enforcement services including 802.1X and DHCP; no costly network upgrades are required.

Integration with RADIUS, Active Directory and LDAP Authentication Services

User access rights are controlled through integration with existing user directories, including Active Directory, LDAP and RADIUS or with local-created users on the RADIUS server within the TippingPoint NAC Policy Server.

The NAC Policy Server works in concert with existing or newly deployed directory infrastructures, including RADIUS, LDAP and Active Directory without requiring changes to the existing directories. Additionally, multiple EAP types and 802.1X supplicants can be supported for using 802.1X as an authentication and enforcement method.

Transparent to Layer 3 Networks

The TippingPoint NAC Policy Enforcer appliance is installed in-line on the network as a Layer 2

Address	IP Address	User	Status	Enforcement	Session	Session	Action
10.10.10.10	10.10.10.10	admin	Success	802.1X	Success	Success	Success
10.10.10.11	10.10.10.11	guest	Success	802.1X	Success	Success	Success
10.10.10.12	10.10.10.12	guest	Failure	802.1X	Failure	Failure	Failure
10.10.10.13	10.10.10.13	guest	Success	802.1X	Success	Success	Success
10.10.10.14	10.10.10.14	guest	Success	802.1X	Success	Success	Success
10.10.10.15	10.10.10.15	guest	Success	802.1X	Success	Success	Success
10.10.10.16	10.10.10.16	guest	Success	802.1X	Success	Success	Success
10.10.10.17	10.10.10.17	guest	Success	802.1X	Success	Success	Success
10.10.10.18	10.10.10.18	guest	Success	802.1X	Success	Success	Success
10.10.10.19	10.10.10.19	guest	Success	802.1X	Success	Success	Success
10.10.10.20	10.10.10.20	guest	Success	802.1X	Success	Success	Success

TippingPoint NAC Active Connections Report

TippingPoint Network Access Control

bridge and is typically deployed at the network core. Operating at Layer 2, the TippingPoint NAC Policy Enforcer is transparent to Layer 3 networks and does not require changes to existing Layer 3 infrastructure or IP address allocations.

Improved Visibility and Reporting of Network Usage and Access

Quickly Scan Current and Past Activity and Status of All Connected Devices

The TippingPoint NAC Policy Server provides advanced reporting capabilities through the centralized Web-based management console allowing network administrators to quickly scan the activity and status of all devices currently or historically connected to the network. Reports may be used for real time system analysis, historical analysis, compliance auditing and system troubleshooting.

A system dashboard displays the current system state, including number of known connections, brief historical authentication charts, and the current state of known attached devices. The dashboard contains a set of charts that give a quick status on various operating components of the NAC Policy Server.



TippingPoint NAC Dashboard

Other Reports include:

- Network connections by MAC address, IP address and username, in addition to the posture assessment of the device
- Real-time monitoring, display and logging of all users, sessions, applications and devices
- Real-time tracking of all user activity, permissions, status and location
- Detailed views of posture information per device or in-aggregate

Keep Audit Records of User and Device Access to Demonstrate Policy Compliance

The NAC Policy Server keeps a complete audit

trail of all user and device access intended to ease internal security policy audit procedures and external regulatory compliance efforts.

TippingPoint NAC Policy Server (NPS)

The TippingPoint NPS is the TippingPoint NAC solution central manager. It holds the main NAC database, interfaces to external back office systems such as LDAP or Active Directory, serves as a RADIUS server for authentication requests, provides logic to determine network policy, and provides the administrative user interface. The NAC database contains all configuration data needed by the NAC system, including the data needed to interface to back office systems, an inventory of 802.1X switches, the data that drives the network policy engine, and detailed records of endpoint connections and the results of their security posture assessments.

The NPS provides all services needed for 802.1X-based NAC enforcement. In addition, the NPS communicates with the TippingPoint DHCP Plug-in installed on the corporate DHCP server to enforce access policies using the endpoint's DHCP lease. With DHCP enforcement, a user's lease can be modified to control name service and set static IP routes to remediation sites.

TippingPoint NAC Policy Enforcer (NPE)

The TippingPoint NPE is an in-line appliance that provides access control enforcement based on user and device criteria. It allows network administrators to designate access rules based on user identity and device type, rather than traditional port based segmentation that may only restrict by location. As more mobile devices are introduced to the network, and enterprise employees become more transient, the network perimeter continues to erode. As consultants, contractors and guests are authorized for internal network access, an inline enforcement tool based on identity is necessary to permit only eligible users onto the network with access to only authorized resources. Working in concert with the NAC Policy Server, the NAC Policy Enforcer receives up-to-date policies for any new connection on the network, and receives any changes in a user's authentication state, and time and location-based rules. A single NAC Policy Enforcer supports approximately 500 users, traffic ~500 Mb/s, and 802.1Q VLAN trunking.

The screenshot shows the TippingPoint NAC Connection History Report. It displays a table with columns for 'Start Time', 'End Time', 'Address', 'User', 'Security Rule', 'Enforcement Action', 'Posture Result', and 'Time Zone'. The table contains multiple rows of connection data, including details like IP addresses, usernames, and security rule names.

TippingPoint NAC Connection History Report

The screenshot shows the TippingPoint NAC Audit Logs. It displays a table with columns for 'User Name', 'Category', 'Message', and 'Timestamp'. The table contains multiple rows of audit events, including details like user names, categories, and messages.

TippingPoint NAC Audit Logs

Identity-Based Policy Management

- NAC Policy Server Web-based management console, and command line interface (CLI) menu via SSH v2
- Access controls based on user role
- Integrates with external user directories - RADIUS, Active Directory and LDAP
- NAC Policy Server supports up to 10,000 users
- Blacklists, whitelists and exceptions
- Tie specific users to specific MAC addresses
- Allow or deny by MAC address
- With inline enforcement, define access rules by Layer 3 and 4 with support for wildcards and ranges

Endpoint Posture Checks

- Persistent and dissolvable posture client
- Configurable interval for continued post connect posture checks
- End user self remediation

- Windows 2000, XP, Vista, Mac OS X, and Linux
- Seamless Active Directory Windows login
- Supports hundreds of AV, anti-spyware and personal firewall software packages
- Posture update service for set and forget policy creation

Access Policy Enforcement

- Multiple enforcement options including 802.1X, DHCP, in-line blocking and any combination thereof
- Support for multiple EAP types / 802.1X authentications
- Customizable captive login Web portal
- HTTP redirection for captive login Web portal
- In-line enforcement appliance – supports 500+ concurrent users
- NAC Policy Enforcer protocols include:
 - 802.1D bridging
 - 802.1D spanning tree

- 802.1Q VLAN trunking / translation
- 802.1X port-authentication
- 802.3 10Base-T
- 802.3u 100Base-TX
- 802.3z 1000Base-SX/T

Historical Reporting

- Real time system analysis, historical analysis, compliance auditing and system troubleshooting
- Correlated live information regarding users, devices and device posture
- Tie all network connections by MAC, IP and username
- Track network usage by user, group, location, posture and destination
- Multiple customizable reports available on the NAC Policy Server
- Syslog, SNMP v1/2 and Traps enable alerting

Product Info	Product	Environment	Concurrent Usage
	NAC Policy Server NPS-250	Small business or office	Up to 250 endpoints
	NAC Policy Server NPS-1000	Mid-sized business	Up to 1,000 endpoints
	NAC Policy Server NPS-2500	Small enterprise	Up to 2,500 endpoints
	NAC Policy Server NPS-5000	Mid-sized enterprise	Up to 5,000 endpoints
	NAC Policy Server NPS-10000	Large enterprise	Up to 10,000 endpoints
	NAC Policy Enforcer NPE-500	In-line enforcement appliance	Up to 500 endpoints
Hardware Specifications		NAC Policy Server	NAC Policy Enforcer
	Processor	• Two Intel® Xeon™ processors (2.8 GHz)	
	Memory	• 4GB RAM DDR-2 400 SDRAM	• 2GB RAM DDR-2 400 SDRAM
	Storage	• Single (1)73GB HD (10,000 rpm) Ultra320 SCSI	
	Interfaces	• 2 x 10/100/1000 copper ports	• 4 x 10/100/1000 copper ports • Auto-media sense, auto-negotiate
	Power	• AC power supply (per power supply) • Wattage: 550 W Hot Plug Redundant Power • Voltage: 84 -264 VAC, auto ranging, 47-63 Hz, 7.6 A • Heat dissipation: 2130 BTU/hr (theoretical maximum) • Maximum inrush current: Under typical line conditions and over the entire system ambient operating range, the inrush current may reach 25 A per power supply for 10 ms or less.	
	Physical Dimensions	Height (in): 1.69 in Height (cm): 4.29 cm Width (in): 19.0 in Width (cm): 48.26 cm Depth (in): 30.0 in Depth (cm): 76.2 cm	
	Weight	Weight (lb): 39 lbs Weight (kg): 17.69 kg	
Environmental	Temperature	• Operating :10° to 35°C (50° to 95°F) • Storage: -40° to 65°C (-40° to 149°F)	
	Relative Humidity	• Operating: 8% to 85% (non-condensing) -maximum humidity gradation of 10% per hour • Storage: 5% to 95% (non-condensing)	

Corporate Headquarters:
7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:
Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:
30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999

TippingPoint®

www.tippingpoint.com