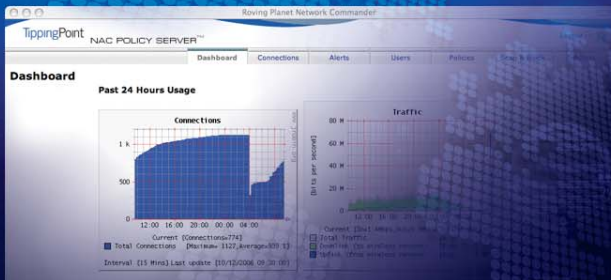


TippingPoint NAC Policy Enforcer

IPS-Secured Networks

DATASHEET – NAC Policy Enforcer



The TippingPoint NAC solution enables enterprises to enforce device and user policies to ensure endpoint compliance and granular network compliance even after initial network entry. This solution goes beyond traditional pre-check and post-check NAC solutions by linking device and user policies to fine-grained, continuous traffic control made possible only by an IPS. By integrating device, user and IPS-based traffic classification and enforcement, enterprises have much greater control over network access and usage, while reducing network security cost and complexity.

Product Features

- Support for 500+ users
- Seamless Active Directory Windows Login
- HTTP Redirection for Captive Web Portal
- Allow or Deny by MAC Address
- Support for multiple EAP types/802.1x authentications
- Tie specific users to specific MAC addresses

Dynamic Policies

- Access controls based on user role
- Integrations with RADIUS, Active Directory and LDAP
- Support for External User Directory Group and User
- Block or redirect traffic to captive portal
- Define access rules by Layer 3 and 4 with support for wildcards and ranges

Statistics Gathering

- Tie all network connections by MAC, IP and username
- Track network usage by user, group and destination
- Multiple customizable reports available on the NAC Policy Server

Management

- Managed by TippingPoint NAC Policy Server
- Command Line Interface Menu (CLI)
- Syslog
- SNMP v1/v2c
- SSH v2

Standards and Protocols

- 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 1000-Base-SX/T

In a TippingPoint NAC environment, access policies subject each device and user pair to rigorous authentication, authorization, posture compliance checks and enforcement. Non-compliant devices are directed to remediate based on policy class. User access rights are controlled through integration with existing rights management systems including Active Directory, LDAP and RADIUS. TippingPoint NAC, including the NAC Policy Enforcer and the NAC Policy Server, then interoperates with the TippingPoint IPS to ensure all malicious traffic is blocked from each endpoint and suspect or non-compliant traffic triggers other policy-controlled actions, including blocking, quarantining, alerting or rate shaping. Now, network and security personnel have unprecedented control over the entire network perimeter with integrated policy-based visibility and control of users, devices and traffic flows.

While network access control combined with the IPS is the ideal protection path, the TippingPoint NAC Policy Enforcer and Policy Server can also be deployed without an IPS.

NAC Policy Enforcer

The TippingPoint NAC Policy Enforcer 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

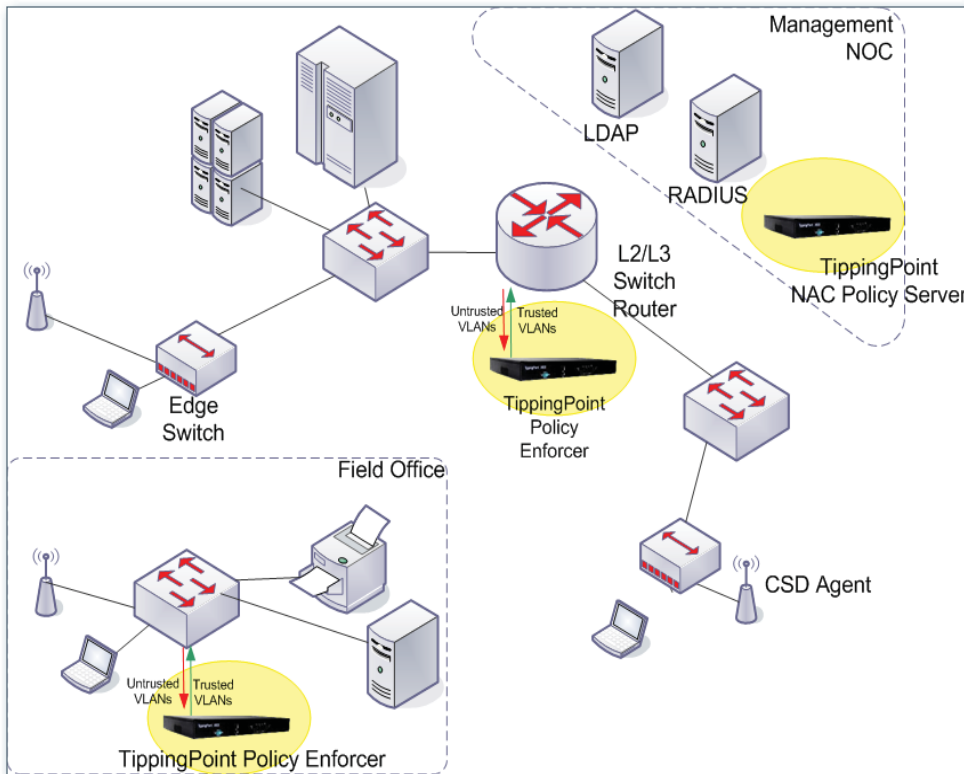
location. As more mobile devices are introduced to the network, and enterprise employees become more transient, the network perimeter continues to erode. As consultants, contractors and guests are authorized for internal network access, an inline enforcement tool based on identity is necessary to permit 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.

The TippingPoint NAC Policy Enforcer sits in-line on the network as a Layer 2 bridge, and is typically deployed at the network core. Operating at Layer 2, the NAC Policy Enforcer is transparent to Layer 3 networks and therefore does not require changes to your existing Layer 3 infrastructure or IP address allocations. A single NAC Policy Enforcer supports approximately 500 users, and has 4 external 10/100/1000 copper ports.

The TippingPoint NAC solution will enable IT professionals to provide valuable access control and security services to their organizations:

- Policy-based employee access control
- Secure guest user access

TippingPoint®



- New device detection: recognize any devices attempting to access your network.
- Threat control: Blocking malicious traffic/malware
- VoIP protection by identifying handsets and applying appropriate access
- Statistics collection to provide compliance reporting for regulatory requirements

Hardware Specifications

Processor, Memory, Storage

- Intel® Xeon™ processor (2.8 GHz)
- 2GB RAM DDR-2 400 SDRAM
- Single (1)73GB HD (10,000 rpm) Ultra320 SCSI

Interfaces

- 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 (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:

World Trade Centre Amsterdam
Zuidplein 36, H-Toren
1077XV Amsterdam
The Netherlands
+31 20 799 7629

Asia Pacific Headquarters:

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