

Enterasys and Palo Alto Networks

Ensuring User and Application Access Control across All Points of Network Access

Introduction

Converged networks, private clouds, public clouds, data center virtualization, virtual desktops, Bring Your Own Device (BYOD) and a host of other changes are transforming the way organizations use networks. Along with the potential for cost savings and increases in productivity comes a new set of security challenges. The best practice for securing this new environment requires fine-grained user and application level access control for networked data and resources. In order to provide this level of granularity a security solution must control all points of access into the network including: the Internet edge, wired access edge and wireless access edge as well as the interior perimeters of critical resources like data centers.



Figure 1. Converged Network

Old style firewalls that control access to data and other resources by IP address and well known port numbers are not well suited for today's environment where many web based applications share a common port. Nor are they flexible enough to permit one user access to an application such as peer to peer file sharing and deny another user access to the same application.

The Security Access Challenge

Before making the decision to grant a user access to an internal or Internet based resource the following need to be considered:

- Who the user is (role in organization)?
- What application is being used?
- Where the user is accessing the network from?
- What is the risk (Botnets, worms, malware)?

Benefits

Increased visibility

Improves security and compliance by extending user / application awareness to the access edge of network

Mitigates internal threats by allowing firewall to trigger user quarantine and blacklist for application based violations

Improves accuracy of firewall by eliminating stale IP Address- to-User Name mappings

Reduced Costs

Simplifies firewall management by eliminating complex LDAP/AD integration

The security solution must be able to identify the user associated with an IP address and the application being used even if it's just one of the ubiquitous web applications that all come in through port 80/443. To be effective for today's networks firewalls must have a way of associating the IP address with the active user and the Network Access Control (NAC) solutions and edge switches need to know which applications the end system is using. Firewalls that rely on LDAP / Active Directory (AD) integration for IP address to user mapping often end up with stale, or misleading information, since LDAP / AD does not know when a user disconnects from the network. These are also no help when trying to identify where the user is connecting to the network from, wired or wireless, secure or public location. Guest access portals that use local authentication also present a problem to LDAP/AD dependent firewalls since they are invisible to LDAP/AD. Finally, LDAP / AD integrations tend to be complex to configure and manage.

The Enterasys/Palo Alto Solution

Integrating Palo Alto's next generation firewall with Enterasys Network Management Suite (NMS) addresses all four considerations for user access. This solution provides seamless application-based policy enforcement at the network edge (wireless and wired), data center edge and Internet edge. Threats originating from internal users will be detected by the Palo Alto firewall which will report the source IP address to Enterasys NMS. The user will be located and quarantined, removing the threat and preventing additional damage. Enterasys NMS provides dynamic real time IP address to user name / asset mapping for the Palo Alto firewall, eliminating complex Active Directory integration. State changes sent from Enterasys NMS when a user disconnects from the network keep the firewall mapping tables current and eliminate stale mappings.

Use Cases

User to IP Mapping at Point of Connection

Enterasys NMS provides the Palo Alto firewalls with accurate and dynamic IP address to user name mapping. Enterasys NMS detects when a user connects to the wired or wireless network, authenticates them and sends the IP address / username / location/policy applied information to the Palo Alto firewall. For locally authenticated guest access the Enterasys NMS guest access portal sends the correct Guest Access username / to IP address mapping to the Palo Alto firewall.

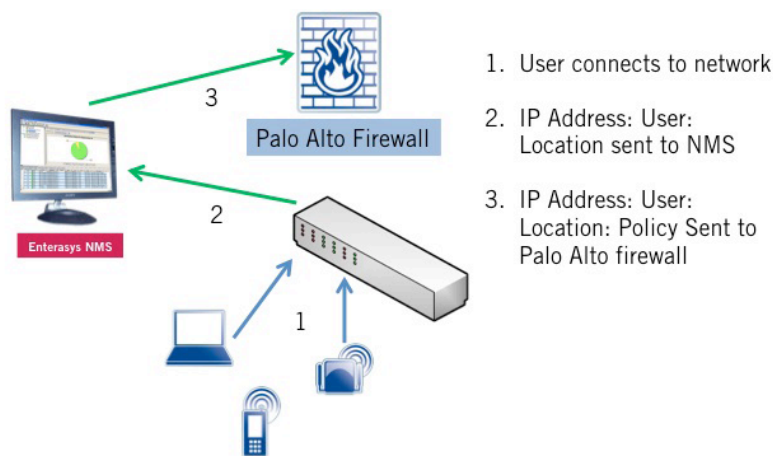


Figure 2. User to IP Address Mapping

The real-time integrity of the IP address / user name mapping is maintained by Enterasys NMS support for RADIUS Accounting. When a user disconnects from the network Enterasys NMS will notify the Palo Alto firewall of the state change. This guarantees that the IP address to username mapping is correctly cleared in the firewall.

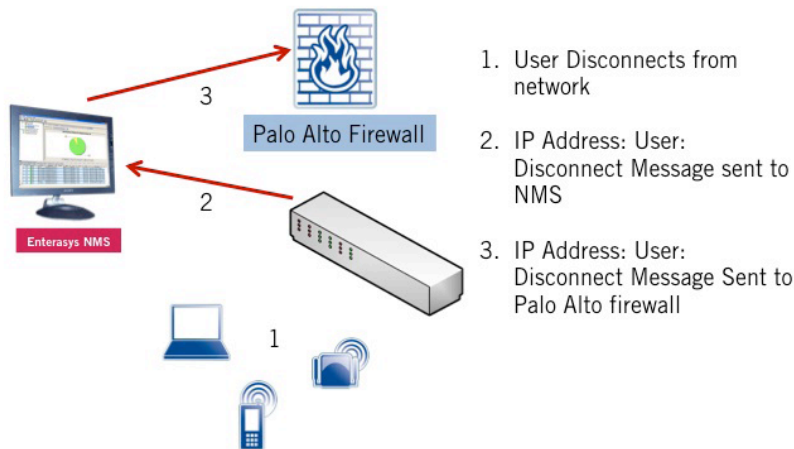


Figure 3. Detecting User Disconnects

The integrated Palo Alto / Enterasys solution offers granular, accurate mapping of user entry and egress from network and creates higher accuracy for dynamic policy enforcement and reporting. It provides seamless access control across wired, wireless and remote access using Enterasys NMS as the central point for authentication, authorization and access (AAA) services.

User Application Visibility at the Edge

In order to offer fine grained access edge security at the wireless and wired edge of the enterprise, Enterasys NMS and the edge switches need to understand which applications the end stations are using.

Future integrations will enable the Palo Alto firewalls to publish user / application mapping to Enterasys NMS.

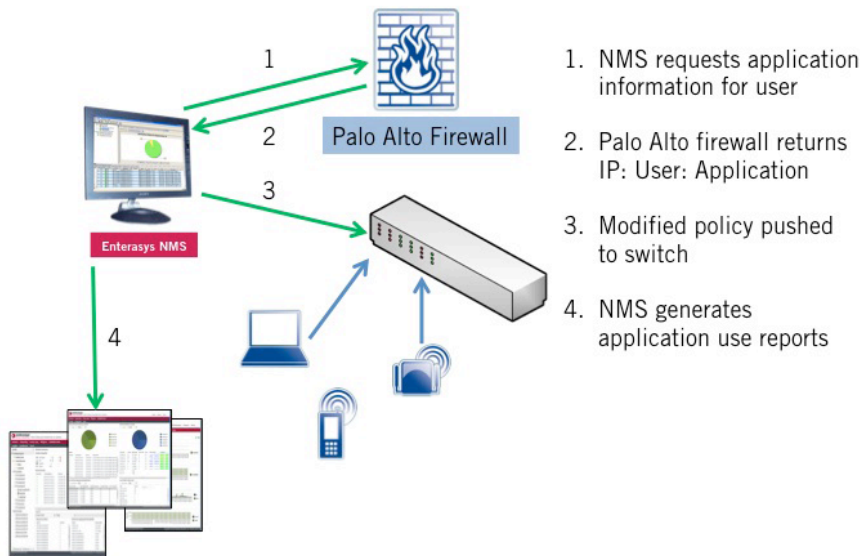


Figure 4. Providing User to Application Mapping

The joint solution will provide the visibility and control that will block unnecessary or malicious applications at the wired or wireless access edge before they can negatively impact the network. Application visibility at the access edge allows Enterasys NMS to report which users are impacted by specific outages or service upgrades, or identify users that are leveraging or abusing specific applications.

Coordinated Enforcement of Security Policy at Wireless Edge, Wired Edge, Data Center Edge and Internet Edge

Integrating Palo Alto's next generation firewall with Enterasys NMS and policy-based switches allows enforcement of security policies at all of the connection points to the network, including wireless edge, wired edge, data center edge and Internet edge.

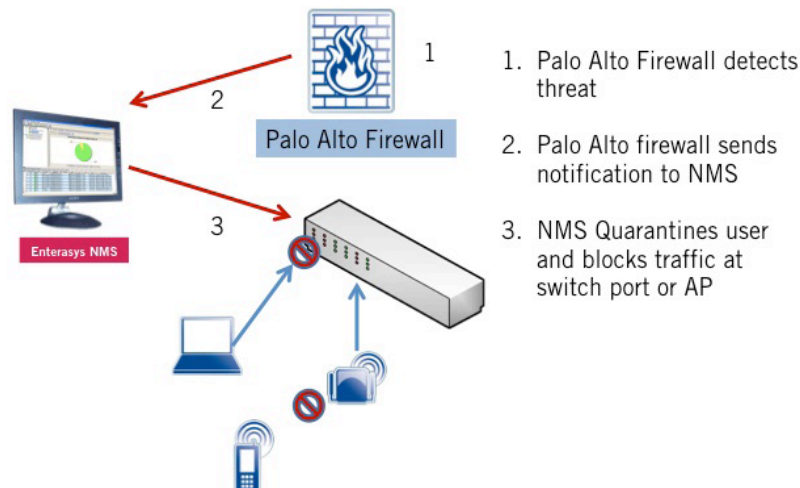


Figure 5. Enforcement at Switch Port or AP

When the Palo Alto firewall detects threats or malicious packets originating from an internal user it notifies Enterasys NMS and supplies the source IP address of the user. Enterasys NMS then locates the access layer port associated with that IP address, blocks the traffic with a quarantine policy, and blacklists the user name. If the user connects to another port they will still be quarantined. If the user is connecting from a wireless access point they will be quarantined from the AP and blacklisted.

Conclusion

The Palo Alto/Enterasys integrated solution delivers the best practices security required by networks rapidly evolving in the face of all the escalating demands of business today. It is the only solution to ensure fine-grained user and application access control at all points of network access – Internet edge, wired/wireless access edge as well as the interior perimeters such as the data center. With the Palo Alto next generation firewall and Enterasys NMS, enterprises can leverage the new network trends to gain the benefits of cost savings and increased productivity without enhancing their risk of compliance failure or a security breach.

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082,
or +1-978-684-1000 and visit us on the Web at enterasys.com



Thought Leadership
Patented Innovation

© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.
Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.



Delivering on our promises. On-time. On-budget.