Establishing a Logical Perimeter

The Evolution of Network Security

October 2011

Palo Alto Networks
3300 Olcott St
Santa Clara, CA
95054
www.paloaltonetworks.com

Table of Contents

Executive Summary

The boundaries of the modern enterprise have undergone massive changes, and these shifts are causing IT, security and networking teams to fundamentally reevaluate the way they think about and manage the network. It is no secret that near-universal Internet connectivity has changed society and user behavior along with it. Users simply assume that they will be able to connect and work (or not) from anywhere, whether using their corporate laptop or increasingly popular platforms such as the iPhone and iPad. From the end-user's perspective being inside or outside the walls of the enterprise is seen as largely incidental. However, while connectivity has become near universal, enterprise security has not, and when users leave the corporate network, they are also leaving behind the enterprise best-practices and best-of-breed security technologies that are the heart of corporate security.

Applications themselves have also undergone dramatic shifts. Applications of all types have evolved to become increasingly adept at evading traditional port and protocol based network controls. Enterprise applications are also migrating to cloud-based or hosted models that reduce the cost and management burden of the application to the business. This shift is largely being driven by the enterprises themselves as a way to make the enterprise healthier and more efficient. As such it will be increasingly important for IT to securely enable these applications regardless of where the application resides.

These examples are part of a broad trend in computing where an enterprise's most basic assets (employees, applications and data) are becoming increasingly flexible and independent from traditional notions of location and hardware. Unfortunately, the same is not true of enterprise security, which remains anchored to the physical perimeter of the enterprise. These shifts present a serious challenge for enterprise IT and security teams. If IT fails to keep pace with these evolving modern computing models, then the overall security of the enterprise will become opportunistic at best, or completely obsolete at worst. To meet this challenge, the enterprise must evolve beyond the outdated notion of a physical perimeter to a model based on logical controls that consistently enforces enterprise policy irrespective of where an asset is located.

The Enterprise Standard of Security

Network security has long stood as the bedrock of enterprise IT security policy. It would be incredibly difficult for any organization to adequately secure an enterprise without the use of their enterprise firewalls, IPS and other network security tools. These solutions have unique strategic importance because they introduce a layer of inspection and control that directly separates enterprise assets from the untrusted outside world. Before risk can find its way into the network or sensitive information can leak out, it must cross this heavily managed barrier where the rules and protections of the network can be enforced. This demarcation of trust and untrust, based on visibility and control of real traffic is a key reason why network security has long been the core component of enterprise security policy. This notion of directly controlling the boundary between trust and untrust is so engrained in the fundamentals of security, that it may seem transparently obvious. Yet it is a concept that is almost universally lost when a user moves outside the walls of the enterprise.

Yet for all the advantages it provides, network security also has significant industry challenges. First and foremost, the classification technology found in network security solutions has become dangerously outdated due to its reliance on port and protocol as the underlying basis for classifying and controlling network traffic. In a very real sense network security solutions no longer speak the same language used by modern applications. This challenge is precisely what led to the need for the next-generation firewall, which modernizes the underlying classification methodology such that all traffic is first classified at the application level (Layer 7) as opposed to port and protocol (Layer 4).

The second major challenge for network security is its reliance on an outdated notion of the perimeter itself. A key value of network security is tied to the ability to sit between and arbitrate traffic between trust levels. This is easily done when trust and untrust are separated by physical boundaries such as being inside or outside of a corporate building. However, as users and applications become more mobile and less reliant on enterprise hardware, this becomes a very dangerous assumption. Security teams must quickly adapt or risk years of best-practices becoming obsolete.

Many Ways to Leave the Network

Both applications and network users themselves are becoming less and less bound to the physical infrastructure of the enterprise. Enterprises are doing everything they can to reduce the cost and management burden associated with their enterprise applications, leading firms to move applications to hosted models either in the public or private cloud and software increasingly being delivered as a service. Such initiatives are mission-critical for the enterprise as they can directly save time, money and manpower.

Users have also migrated beyond the reach of the traditional enterprise network. Users simply expect to be able to take their work with them and to stay connected from anywhere. Unlike in the past, this behavior is no longer limited to the traditional “road-warriors” or home-office employees. Due to the widespread availability new networking technologies such as WiFi and 3G/4G, end-users have become very accustomed to having Internet connectivity literally everywhere they go. The rise of iOS-based devices such as the iPhone and iPad has made users even more mobile, and in some cases, more difficult to recognize and secure. In some cases, these technologies lead to counter-intuitive situations where users may accidentally roam outside of the corporate network even though they may still be physically inside a corporate building.

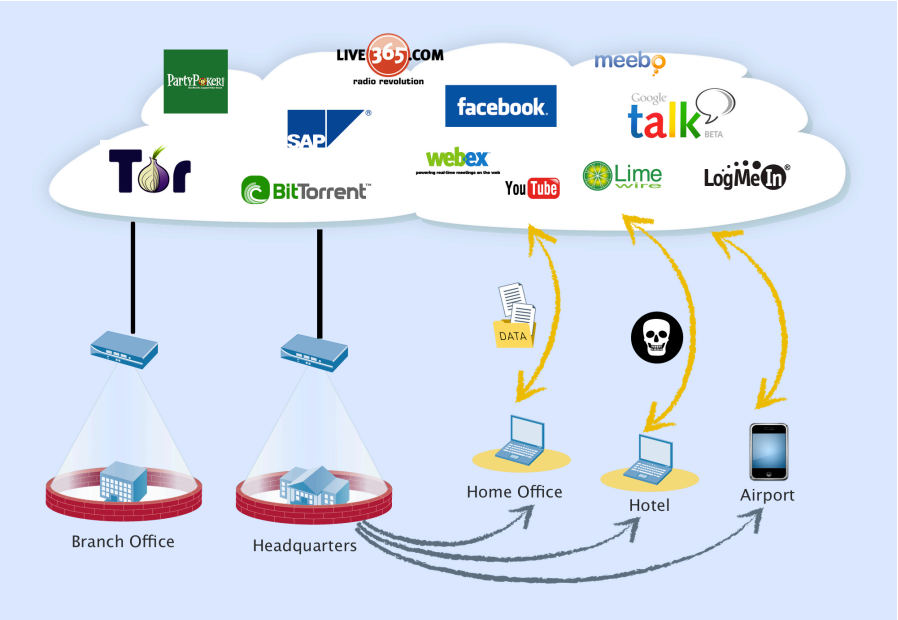

Image 1: Inconsistent security policies expose remote, or traveling users to added security risks.

Collectively, these trends have changed the topology of the enterprise to the point where users and applications can no longer be assumed to be physically located or connected to the enterprise network. When enterprise assets are no longer on the physical network, the enterprise loses the opportunity to directly control the traffic passing between trusted and untrusted resources, leading to an inconsistent and opportunistic approach to security.

A Requiem for Security Policy: Death by a Thousand Cuts

The trends discussed above have led to an identity crisis of sorts for IT teams and the corporate security policy in general. When inside the network, security policy is well defined and based on full-featured network security solutions such as network firewalls, IPS and filtering solutions. When outside the network, IT teams must fall back to a second "best effort" approaches to security.

- **End-Point Agents:** Host-based solutions can be grouped into three general categories and all have failed to meet the standard of security found inside the walls of the enterprise. The most common approach has been to load the end user machine with a variety of host security applications, each with its own unique function (antivirus, firewall, DLP, etc). These solutions tend to remain in narrow silos of functionality and simply fail to live up to the standards of the full-featured network security solutions at the physical network perimeter.
- **VPN:** Another very common approach is the use of VPNs to provide a secure connection back to the enterprise. VPNs typically serve their purpose well, but they do do have the drawback of requiring all traffic to be funneled back to a centralized point, often creating unacceptable performance problems in the process. Additionally, the VPN only provides a secure tunnel, and does nothing to enforce policy on the actual content within the tunnel.
- **Cloud-based Proxies:** The third approach has been to use a client to force user traffic to a cloud-based proxy service. These services have the same limitations of proxy gateways in that they support a limited number of applications and protocols and lack the deep inspection of content needed to prevent threats and data loss.

These approaches, while they do provide some value, are all lacking when compared to the policies and protections that are provided when the user is on-network inside the enterprise. Furthermore, it leads to a massive and ongoing duplication of effort for security teams. They now must support essentially two separate security policies with different capabilities. Management and reporting efforts are also duplicated and additional work is required to correlate between the two. It is important to recognize this as a strategic challenge for the enterprise.

Specifically, the very projects that are creating new efficiencies for the enterprise are simultaneously requiring additional security expense, additional man-hours of effort while ultimately delivering an overall lower standard of security. In short, the efficiencies created on one side of the enterprise are being immediately given back on the other. To properly address this problem, the enterprise must realize that these new use cases are not corner-case exceptions but standard behavior that security policy must support. If the fundamental causes of this imbalance are not addressed, then enterprises will be doomed to perpetual conflict between forward-looking programs and security. To meet this challenge, the enterprise must modernize the perimeter, shifting from a perimeter based on physical assumptions to one that understands the logical relationship of users and applications to the enterprise. By shifting to a logical concept of the perimeter, the enterprise can go back and again design security in as a fundamental part of every connection as opposed to something that is tacked on at the end.

The Logical Perimeter: A Strategic Solution

As most security professionals know from experience, security is not simply a product or a feature that can be added on to a project at the end, but rather a process that must be designed in from the beginning. The logical perimeter provides the requisite framework for integrating a standardized and consistent approach to security into every network connection regardless of location. This means the rules and policies remain consistent and the organization's best intelligence and protections are universally applied.

To meet this goal, the logical perimeter must first standardize on the corporate security policy as the rule of law for all network connections regardless of where they occur. Security policies, like any rules or laws, must be applied consistently if they are expected to serve their purpose. If the rules only apply in certain circumstances, then they cease to be rules in any true sense and exceptions quickly become the norm. This is precisely the situation that security teams find themselves in today. Users have been mobile for many years, and enterprises have gradually become accustomed to settling for a reduced quality of security for these users. The logical perimeter establishes consistent security policy based on applications and users, and in the process clearly sets the bar for new projects and what security levels they will be expected to meet. While this step may seem obvious, it is nevertheless extremely important to have a strong directive in order to push back against a long-established trend of making security exceptions for remote users.

Secondly, network users outside the corporate network should receive the same protections that are provided when inside the physical network. For example, firewalling decisions should provide the same visibility and control of applications, users and content established by the next-generation firewall at the traditional perimeter. In fact, this requirement is particularly important for end-users in the field, as client applications are very likely to be evasive and route around traditional port-based controls. Additionally, users may revert to less strict browsing behaviors when away from the office, exposing them to even more potential threats. As with firewall controls, users should be protected by the full complement of IPS, and threat prevention when they are outside the physical network. This means true network-based IPS, malware and botnet control, as well as a file, URL and content filtering. Obviously, users are exposed to just as many risks and threats when outside the network, so it only makes sense that they should receive the enterprise's best protections.

Last but not least, this logical perimeter must meet the performance and reliability expectations of both end-users and management. Experience has repeatedly shown that security solutions that don't deliver reliable performance have a very limited lifespan in the enterprise. As such the solution must be universally available to end-users and transparent as possible to the user both in the use of the solution and the performance of the network connection itself, all without creating new management burdens.

Key Requirements of the Logical Perimeter:

- Establishes a consistent set of policies based on applications and users that apply to all traffic
- Provides the same protections outside as inside
- Delivers enterprise performance and reliability

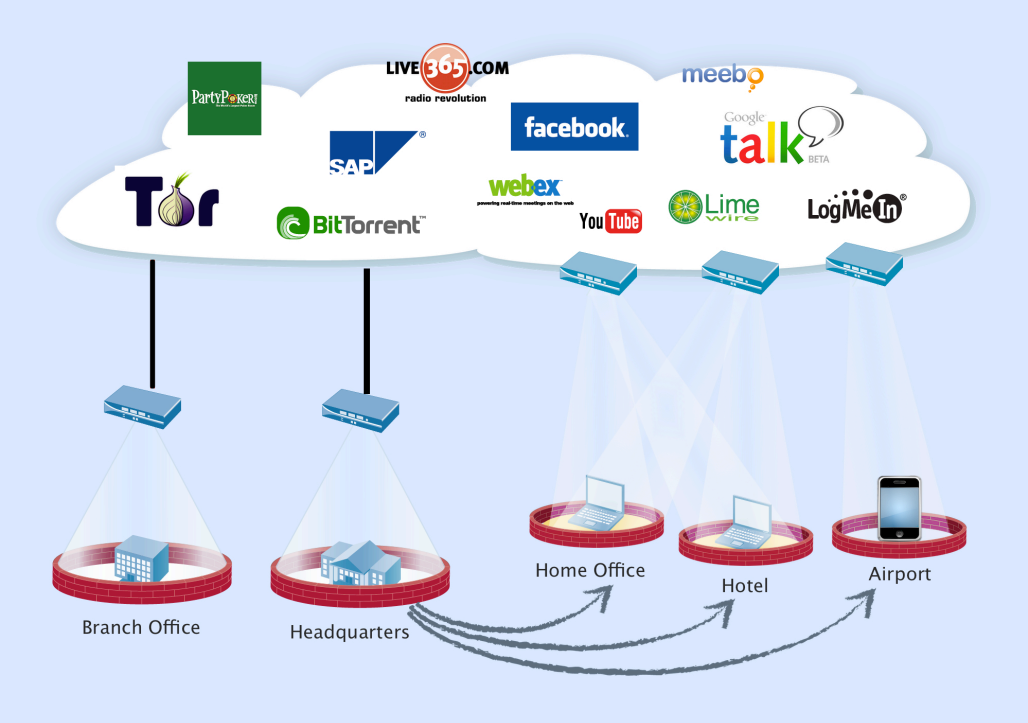

Image 2: GlobalProtect extends consistent network security policies to all users.

GlobalProtect + Next-Generation Firewall = The Logical Perimeter

GlobalProtect introduces a modern approach to enterprise security. Instead of trying to reinvent the entirety of enterprise security on the end-user's laptop, GlobalProtect takes what already works today, the next-generation firewall, and delivers it transparently to all remote connections. Almost as importantly, GlobalProtect takes advantage of the next-generation firewalls that are already deployed and can typically be deployed with no additional hardware required. The solution is comprised of three different components:

- **GlobalProtect Agent:** The GlobalProtect agent is a small piece of software that resides on the end-user's PC. This agent can be delivered to the user automatically via Active Directory, SMS or Microsoft System Configuration Manager or can be downloaded directly from the GlobalProtect Portal. The agent provides secure connectivity between a remote user and the enterprise Palo Alto Networks firewall to ensure secure connectivity as well as next-generation visibility and control of traffic regardless of location. The agent supports Microsoft Windows XP, Vista, Windows 7, and Mac OS X, enabling IT to extend security and connectivity to a wide variety of today's most popular devices. When licensed, the agent can actively test and select for the best performing Palo Alto Networks GlobalProtect Gateway. And lastly it compiles a Host Information Profile (HIP) of the client device including such factors as patch level, disk encryption, antivirus version and many more. Additionally Palo Alto Networks leverages the IPSec VPN client built in to Apple iOS devices. This provides native connectivity and secure access, but does not support HIP profiles or intelligent gateway selection.

GlobalProtect iOS support

With the introduction of GlobalProtect, Palo Alto Networks provides a complete solution for customers to provide the full protection of Palo Alto Networks next generation firewalls to all company computers irrespective of their location. With the popularity of the Apple iPhone and iPad, Palo Alto Networks expands its GlobalProtect feature set to support Apple iOS devices in addition to Mac OS and Microsoft Windows computers.

GlobalProtect gateway introduces a feature set to support the native IPSec capabilities of iOS devices without the need of deploying additional, non user-friendly and battery draining applications to mobile devices. Using the organizations mobile device management, customers are now able to centrally deploy a VPN profile to automatically keep all mobile devices connected to and protected by a next generation firewall regardless of the devices location.

- **GlobalProtect Portal:** The GlobalProtect Portal provides the centralized management for the solution. Any Palo Alto Networks firewall can act as the portal while also performing its everyday duties as a next-generation firewall. However, each GlobalProtect deployment will only have 1 portal at a time. The portal provides three key functions: It delivers the GlobalProtect Agent to users. It provides the GlobalProtect agents with a list of available GlobalProtect Gateways. And lastly, it manages the authentication certificates for the solution. The GlobalProtect Portal, like all Palo Alto Networks can be run as a high-availability pair, to ensure always-on reliability of the solution.

- **GlobalProtect Gateway:** The GlobalProtect Gateways are responsible for the majority of the actual security enforcement in the solution. Similar to the portal, any Palo Alto Networks firewall can be a gateway for the GlobalProtect solution. However, unlike the portal, you can leverage as many gateways simultaneously as you need, ensuring multiple potential routes between an agent and gateway. The Gateway has three core functions: First and foremost, it performs the full breadth of next-generation firewalling functionality including application control, threat prevention, URL filtering, user visibility, etc on all traffic from associated GlobalProtect Agents. It also provides the end of the secure connection established by the Agent. Lastly, it receives the Host Information Profile (HIP) and enforces policies accordingly.

Dynamic and Distributed Architecture

The GlobalProtect architecture leverages the distributed nature of modern enterprises to break the bottlenecks that have traditionally plagued centralized solutions such as SSL VPNs. Instead of sending all traffic back to a single centralized location, the GlobalProtect solution actually adapts to the end-user's location to find the best path to a gateway. The GlobalProtect Agent automatically tests all available gateways to determine the route with the fastest response times. This approach ensures that a user always leverages the fastest option based both on location and relative load on the various gateways. This model avoids the congestion and latency common to backhaul solutions and enables the enterprise to get added value from all of their Palo Alto Networks firewalls as they work together as a virtual hosted security service.

Enforce Network Controls Based on User, Role, and User Profile

One of the key concepts behind the next-generation firewall is the ability to enforce policies based on user or user group. Instead of relying on IP address, the Palo Alto Networks next-generation firewall integrates with the enterprise directory infrastructure to uniquely identify and enforce policy to individual users and machines. The User-ID technology integrates with a variety of directories including Active Directory, eDirectory, Open LDAP, Citrix Terminal Server, Microsoft Terminal Server and XenWorks.

User-ID can also be configured to monitor logon events from clients accessing their Microsoft Exchange mailbox, enabling the solution to identify Mac OS X, Apple iOS, and Linux/UNIX client systems that don't directly authenticate to the domain.

GlobalProtect extends these controls to incorporate the configuration of the end user's device. If the user's end-point is not properly secured, security teams can automatically enforce network controls to compensate. For example, a user may have rights to access certain information on the enterprise network, but the GlobalProtect Gateway can prevent that user from downloading files if his laptop is not using disk encryption. Or alternatively, if the host antivirus is out of date, staff can automatically restrict access to social networking sites where malware tends to propagate. When added to the application, user and content controls available from the Palo Alto Networks next-generation firewall, security teams now have a level of control and flexibility that they have never had from traditional solutions. Just as the next-generation firewall allows for more granular controls of firewall policy, GlobalProtect offers granular control of user rights based on their host configuration. Policies can be based on the following host characteristics.

- Operating System and Application Patch Level
- Host Anti-Malware Version
- Host Firewall Version
- Disk Encryption
- Data Backup Products
- Customized host conditions

Summary

Enterprise security is in the midst of a sea-change. The ways applications behave has changed. The ways that applications are hosted and delivered have changed. The behaviors of end-users have changed. Yet the overall approach to security remains tied to outdated assumptions that fail to account for these shifts, leading to lower security and increased costs. Going forward, the health of the enterprise will be directly tied to how effectively and efficiently can support the evolving nature of users and applications.

Successful companies will require a standard approach to ensure that all enterprise network connections meet the internal standard of security. This will require enterprise security to be flexible, consistent and included in all connections by design, not simply tacked on at the end. A migration to a logical concept of the perimeter provides this foundation. Instead of multiple disconnected policies, the enterprise policy can remain unified and consistent. The cost and management required of one-off security projects can be prevented by simply extending the reach of the next-generation firewalls that are already deployed. This shift will allow enterprises to reverse trends that have plagued security for years and actually improve the overall quality of their security operations, reduce their costs and provide the underlying infrastructure to securely enable new applications and services in the future.