Juniper Networks Secure Access versus F5 FirePass Appliances

Overview

F5 Networks, historically known as a leading supplier of load balancing solutions, began offering SSL VPN functionality through their 2003 acquisition of uRoam. The resulting SSL VPN appliance, FirePass, lacks robust security features, particularly when compared against vendors with core competencies in security. In addition, FirePass is a mix of uRoam's proprietary software and a heavy reliance on open source software, creating a complex and vulnerable architecture. FirePass base pricing starts at $9,990 for 25 concurrent users (FirePass 1000) and grows to $69,990 for 1000 concurrent users (FirePass 4100).

F5 FirePass Product Weaknesses

- **Lacks robust system security.** No third party audits. No encrypted storage. System security weaknesses include: SSH-based login as an alternate access method which can enable attacks from unauthorized remote users. ability for read-only FirePass Administrator to execute backend processes and configuration changes, "root" capabilities in FirePass front-end web service which, if compromised would allow access to the entire system (keys, stored passwords, etc.), no hiding of "fingerprints" of network-based services allowing anyone to determine versions of services and 3rd party code, and ability of Firepass users to bypass admin-configured access controls in layer 3 tunnel.
- **Limited threat control capabilities.** No ability to detect, prevent and quarantine endpoint malware and threats and limited abilities to detect, prevent and quarantine network or application layer threats.
- **Limited clientless and thin-client access.** FirePass's web intermediation technology has difficulty handling advanced web applications, such as Sharepoint, especially those that include complex JavaScript and Java applets. This requires a reliance on a windows only heavy application proxy client (1.0 MB+), or higher administration costs from creating reverse proxy manual mapping workarounds
- **Limited network access.** Firepass's full network access client is limited to a single transport mode making it ill-suited to for applications requiring high performance. Network access and HC clients are not integrated with GINA.
- **Deficient dynamic access privilege management capabilities.** No ability to limit access based on time, directory attributes, Source IP, etc or re-evaluate access or endpoint security during user session.
- **Limited management and scalability.** Lacks comprehensive central management functions for multi-unit deployments. Does not support stateful WAN clustering with seamless failover.

Juniper Networks Secure Access (SA) Key Differentiators

- **Track record of product and customer leadership -** Overwhelming SSL VPN leader as recognized by Gartner Magic Quadrant, META Group MetaSpectrum, and Forrester Wave and market share leadership based on Infonetics Research and Synergy Research Group reports. Over 6,000 customer deployments including over 50% of Global/Fortune 100.
- **End-to-end security** – Most comprehensive endpoint security in industry including most advanced, dynamic, cross-platform host checking, cahce cleaning, malware detection, client- and server-side endpoint software APIs integrated into all access methods and dynamic access privilege management. Proven hardened appliance utilizing AES disk encryption, no shell access and multiple third party audits. In-transit data trapping and obfuscation capabilities. Coordinated Threat Control for detecting, preventing, identifying, quarantining and remediating network and application-level threats.
- **Market leading clientless, thin-client and network access.** Clientless access supports dynamic rewriting of complex web content including JavaScript, VBScript and Java applets that make socket connections – eliminating the need for admins to manually map web pages and links. Java-based, thin-client (~100 KB) application proxy provides cross platform support for client/server applications. Cross-platform, dual transport (IP Sec, SSL) Network Connect client enables high performance/high availability access to all applications.
- **Dynamic Access Privilege Management.** Market leading functionality for creating and enforcing granular, real-time access decisions based on a combination of user, device, network, and time-based conditions. Standards-based integration with leading Access Management vendors using SAML.

Juniper Networks Secure Access versus F5 FirePass Appliances

Feature Comparison Matrix

Feature	Benefit	SA	FirePass
Access Management			
Dynamic Access Privilege Management	Create/ dynamically enforce granular (allow/deny URLs, files, servers, subnets, etc) access decisions based on rich identity, device, network, and time-based conditions in order to provision required resource access while maximizing security.	Yes	No post-auth reevaluation, limited granular controls (no time, directory attributes etc. conditions)
Directory integration (Password Mgt, SSO)	Enables admins to easily integrate existing password policies in directory servers (LDAP, AD, etc.) and improve end-user experience through SSO and leveraging directory attributes in policy formation	Yes	Limited SSO, no SAML, no password management integration, no parameterized policies or bookmarks.
Resource-Based Policies	Ability to define caching and authentication policies at the resource level, as opposed to the user/group level (more granular access control).	Yes	Policies defined at user/group level only
Management			
Centralized Management SSL VPNs	Reduces cost of ownership for multi-unit deployments	Yes	No push config, zero downtime upgrade, or deterministic cluster recovery. Single backup config
Access Methods			
Core Access	Provide lowest cost, anytime, anywhere (clientless) access to web, file and telnet/ssh resources.	Yes	Limited support for advanced content (known sites don't work)
SAM or Port Forwarding	Extends browser-based access to client/server applications via thin-client application proxy	Yes	No Java-based alternative. ActiveX-based alternative does not support dynamic port applications
Network Connect	Cross-platform, high performance, high availability, dual transport (IP Sec, SSL) network access.	Yes	Single mode (not suited for high performance apps); no GINA integration.
Complete End-to-End Security			
Host Checker & Cache Cleaner	Checks for existence of client software, processes, files, registry settings or ports across platforms. Cache Cleaner deletes user session info.	Yes	Limited, No client- or server-side API. No GINA HC integration.
Integrated Malware Protection	Detect, prevent, quarantine and remediate endpoint-level threats (key & screen loggers, spyware, etc.) with dynamically delivered signature- and behavior-based malware protection engine	Yes	No
Coordinated Threat Control	Detect, prevent, identify the source of, quarantine and remediate network/application-level threats (worms, app vulnerabilities, Trojans, etc.) with SA and IDP appliances.	Yes	No
Performance, Scalability and Virtualization			
Multi-Site Clustering	Enables cost-effective scalability and ability to handle traffic bursts and resource intensive application use	Yes	Requires two gateways per site to ensure seamless failover.
End-to-end virtualization	Provides full SSL VPN gateway virtualization (application & network layers and access mgt) to enable hosting of multiple internal/external customers from a single device..	Yes	Only simple VLAN support
Hardware			
Component level redundancy	Dual redundant hot swappable power supplies and hard drives with real time data mirroring ensure optimized uptime in rare event of component failure	Yes	No dual redundant hot swappable hard drives
Secure Meeting			
Online web conferencing	Low cost, secure online web conferencing, application sharing and remote control for internal & external company meetings and customer support interactions.	Yes	No