BIG-IP Secure Access Manager

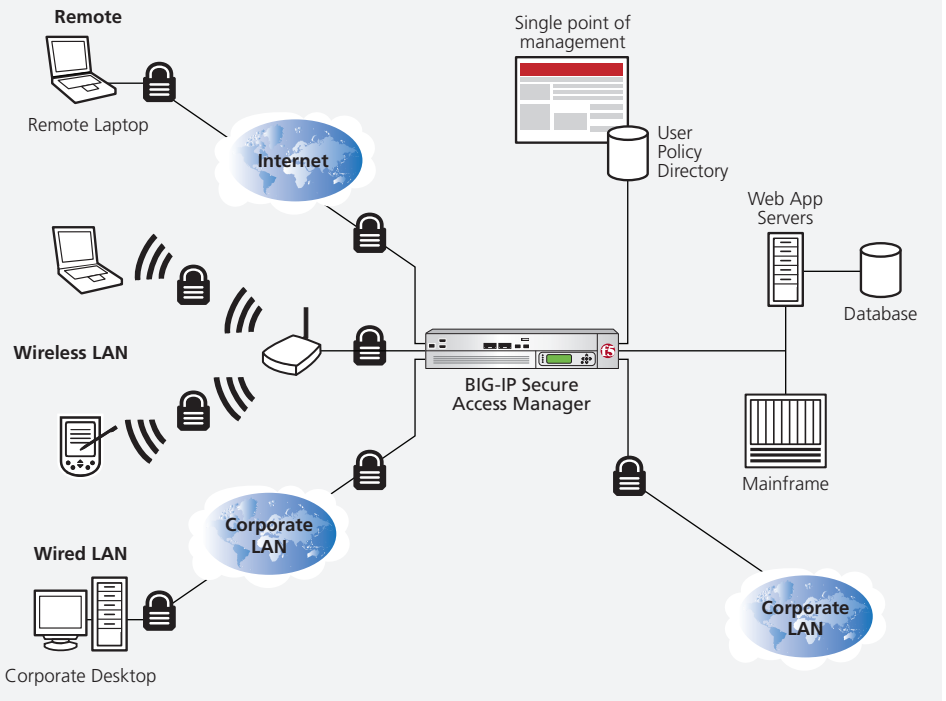
A Flexible and Unified Solution for Secure Access

Enterprises today have a growing need for simplified and unified access control to provide end-to-end data protection. They depend on a multitude of systems and processes to provide secure access from different locations, including IPSec and SSL VPN technologies and network access control (NAC) solutions. Administrators are tasked with defining and deploying multiple product policies to manage functions including: endpoint security checks and control; remediation; access logon; and authentication, authorization, and application access control.

BIG-IP® Secure Access Manager™ (SAM) is a high-performance, flexible security platform, providing a unified secure access solution on a single appliance. Using SSL tunneling for encrypted traffic, BIG-IP Secure Access Manager provides policy-based, secure access to enterprise applications for any client user—from employees, contractors, partners, and suppliers to any corporate resource. BIG-IP Secure Access Manager provides end-to-end data protection for secured web application client connectivity to enterprise applications.

Key Benefits:

- **Unification of Users, Policies, and Management** – Provides a flexible and unified secure access solution for any user, device, and network—including trusted or untrusted VPN access, wireless access, or internal LAN access.
- **Policy-Based Access** – Enables policy-based authentication, authorization, and accounting access to corporate application and data resources.
- **Improved Performance and Scalability** – Uses F5's unique TMOS architecture to dramatically enrich access control performance and scale up to 25,000 concurrent SSL-encrypted user sessions on a single appliance.
- **Industry-Leading Access Policy Management** – Provides a Visual Policy Editor and Virtual Access Policy Management to give you tremendous flexibility in how you organize, scale, and apply access control to your applications, not just the network.
- **Centralized and Cost-effective Management** – Offers a common access platform solution to reduce the need for multiple devices and maximize ROI.
- **Broad Compliance with Existing Authentication Policies** – Integrates with a wide range of user directory and authentication servers and services, including Active Directory, LDAP, RADIUS, 2-factor, RSA SecurID, and client certificate (e.g. smart card) infrastructures.
- **Complete Compliance with Security Regulations** – Provides strong integrated endpoint security checks and controls that ensure complete compliance with enterprise security policies.



Creating multiple virtual BIG-IP Secure Access Manager instances (virtual IPs) enables the consolidation of different unified access groups onto one device.

Flexible Support for All Access Networks

BIG-IP Secure Access Manager provides secure connectivity to corporate applications from all access networks, including remote LAN, internal LAN, and both public and internal wireless. This flexible, easy-to-manage, high-performance platform uses SSL tunneling technology to provide secure access to any user from any location and any client device.

Unprecedented Levels of Performance

BIG-IP Secure Access Manager is built on F5's unique TMOS™ architecture, a purpose-built, scalable, operating system that has been specifically designed to control network traffic at a granular level. The tight integration of BIG-IP Secure Access Manager with TMOS supports a unified network access management system with the capability to support up to 25,000 concurrent users on a single appliance with high ramp-up and throughput performance.

Strong Endpoint Security

To ensure that enterprise network access—from client to enterprise application and data—is fully protected from worms and viruses, BIG-IP Secure Access Manager provides a broad set of endpoint security checking and lock-down features. Endpoint security features include: antivirus and firewall checks; file, process, OS, and registry checks; context-based security, such as assigning access control lists (ACLs) based on endpoint posture; and browser cache cleaning to remove any sensitive data at the end of a user's session.

Encryption Everywhere

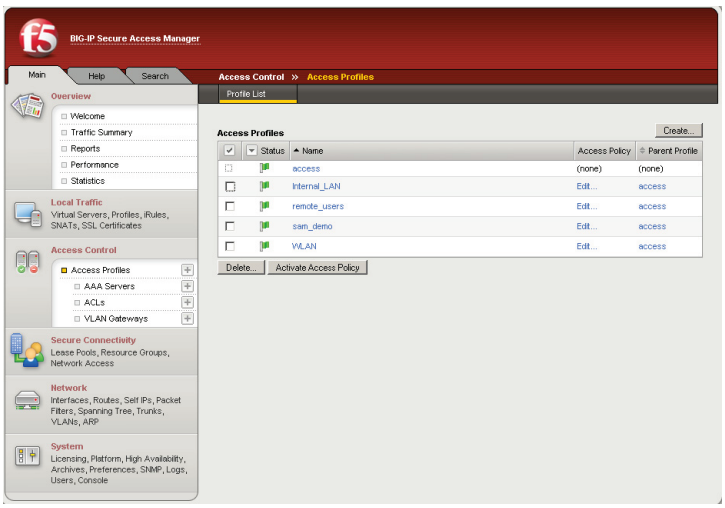
BIG-IP Secure Access Manager supports common encryption technologies, including RC4, Triple DES, and the Advanced Encryption Standard (AES). Standard web browser-based SSL technology is used for secure transactions between the client system and BIG-IP Secure Access Manager. Used in conjunction with wireless infrastructures, BIG-IP Secure Access Manager can add a layer of security, including LAN encryption and granular application access.

Comprehensive, Centralized Access Control Management

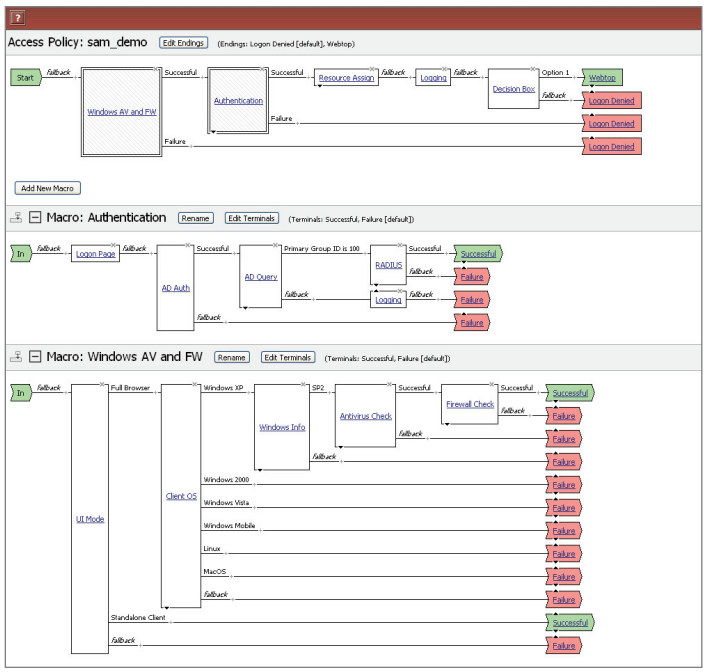
With BIG-IP Secure Access Manager, administrators can maintain complete, granular control over defining access control policies and accompanying profiles. You can create comprehensive policies for endpoint security lockdown and establish authentication and authorization methods for enterprise application access.

Simple and Flexible GUI-Based Policy Management

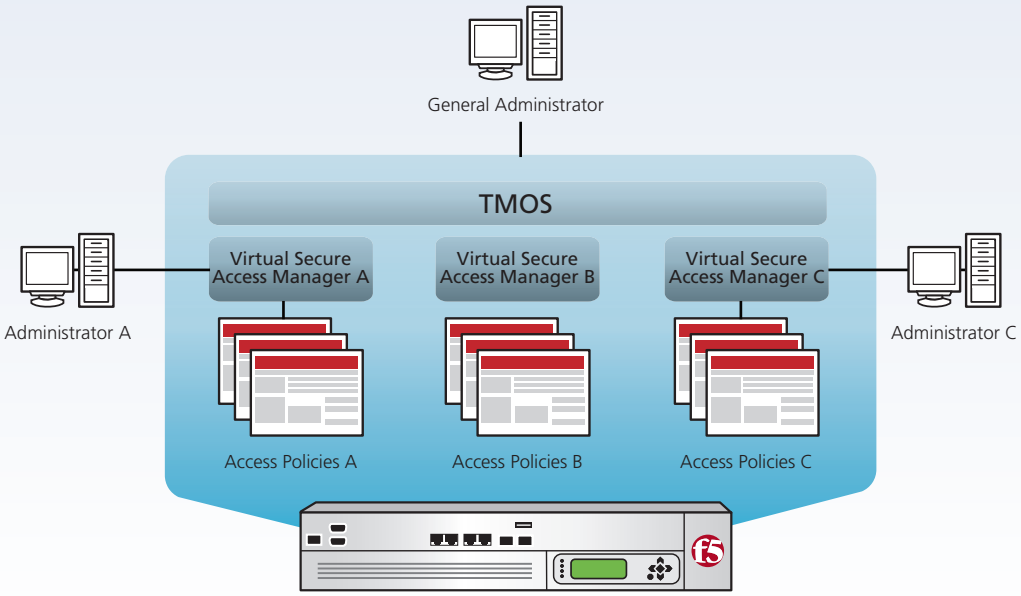
The award-winning, easy-to-use Visual Policy Editor (VPE) simplifies creating, editing, and managing access policies on BIG-IP Secure Access Manager. With the GUI-based VPE, you can define one access profile for all connections coming from any device, or you can create multiple profiles for different access methods, each with their own access policy. For example, you can create a policy for corporate LAN, VPN, or wireless 802.11 connections. VPE is the only policy-editing solution that enables security administrators to efficiently and quickly create and edit entire access policies with a few simple clicks.



BIG-IP Secure Access Manager gives administrators complete control to define and manage access control profiles.



The GUI-based Visual Policy Editor provides intuitive and granular control over multiple access policies.



BIG-IP Secure Access Manager provides end-to-end encryption and access control from a single point of management.

Virtualization Capabilities

With BIG-IP Secure Access Manager, you can create multiple virtual servers by defining and managing access policy groups according to your business or organizational needs. These virtual servers can be administered independently or managed by a global administrator. Ideally suited to enterprises or service providers that require consolidation of different unified access groups for multiple customers onto one device, BIG-IP Secure Access Manager can help reduce hardware needs and improve operational efficiency and costs.

High Availability

By supporting failover mechanisms, BIG-IP Secure Access Manager provides a highly available solution regardless of system, server, or application failure. Two units will support Active/Standby mode and global availability can be achieved with the addition of BIG-IP® Global Traffic Manager™.

Integration with Enterprise Manager

BIG-IP Secure Access Manager also supports F5 Enterprise Manager, which provides a GUI-based interface and a common set of features for centralized management, including: device discovery and inventory management; configuration file management; configuration management; and hot-fix and software update management. Using Enterprise Manager, BIG-IP Secure Access Manager provides enhanced operator efficiency, reduces the likelihood of operator-induced errors, increases network operation efficiency, and helps meet service level agreements while reducing the total cost of ownership (TCO).

Reduced Total Cost of Ownership

The overall operational costs of implementing an effective NAC solution are dramatically reduced with BIG-IP Secure Access Manager. The combination of a high-performance operating system—specially designed for network switching—with advanced and unified secure access features provides a complete solution in a single appliance. The Visual Policy Editor reduces the setup and deployment time for enterprise-wide security enforcement, reduces operator errors, and mitigates business risk, resulting in reduced operating and capital expenses.

Universal Client Security Integration SDK

A universal client development environment adds deep, secure-access integration capabilities to address business, regulatory, and auditing requirements. The SDK (available on F5 DevCentral℠) enables integration directly with applications and is supported on a broad range of client device software, including Microsoft Windows XP, Vista, and Windows Mobile. The combination of F5-supplied client and application access features, plus the ability to develop deeply integrated access control functions, provides a comprehensive, flexible secure access solution.

Control and Flexibility through VPE Rules and iRules

Security administrators can create advanced access policy rules to meet specific security needs using F5's Visual Policy Editor (VPE) Rules. The VPE rules engine can use, manipulate, and assign session variables to make dynamic policy decisions such as access control list (ACL) assignment, client certificate field manipulation, authorization based on session variables, and other advanced functions.

F5's iRules™ scripting language, based on F5's exclusive TMOS architecture, provides unprecedented control to intercept, inspect, transform, and direct inbound or outbound application traffic. An active, collaborative community on F5 DevCentral offers support, tips, and code samples for VPE Rules and iRules.

Platform Specifications

BIG-IP Secure Access Manager 4300 is a 2U standalone or rack-mount appliance designed for medium to large enterprises and Internet service providers. It has an AMD dual-processor, quad-core CPU, offering high performance and supporting up to 25,000 concurrent users on a single appliance. BIG-IP Secure Access Manager 4300 also supports built-in redundant power supplies, a factory-installed FIPS SSL card, and optional gigabit fiber ports. It offers support for FIPS 140 Level-2 enabled tamper-proof storage of SSL keys, as well as FIPS-certified cipher support for encrypting and decrypting SSL traffic in hardware.

Physical Specifications

BIG-IP Secure Access Manager 4300

Base Concurrent User License per Appliance: *Up to 2000*

Max. Concurrent Users per Appliance: *25,000*

Interfaces: *4 x(10/100/1000) BaseT Copper ports plus 2 x SFP Fiber ports (SFP optics not included)*

Dimensions:
3.5" H x 17.5" W x 23.5" D
2U industry standard rack mount chassis

Weight: *43 lbs*

Processor: *Two AMD® Dual Core Processors*

Power Supply: *Dual 460W 90/240 +/- 10% VAC auto switching*

Typical Power Consumption: *275W*

Maximum Heat Output: *939 BTU/hr*

Device Redundancy: *Yes – Device redundancy via watchdog timer and failsafe cable (primary and standby units)*

SSL Acceleration Card:
Yes – Factory installed (FIPS SSL Card – optional)

Hard Drive Capacity: *160 GB*

RAM: *8 GB standard*

Operating Temperature: *41° F to 104° F (5° C to 40° C)*

Non-Operating Ambient Temperature Range: *-40° F to 149° F (-40° C to 65° C)*
Relative humidity: 10% to 95% at 40° C non-condensing

Relative Humidity: *20% to 90% at 40° C*

Safety Agency Approval: *UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950*

Electromagnetic Emissions Certifications:
EN55024 1998 Class A
FCC Part 15B Class A
VCCI Class A

F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
+1-206-272-5555 Phone
(888) 88BIGIP Toll-free
+1-206-272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Phone
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932-582-000 Phone
+44 (0) 1932-582-001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Phone
+81-3-5114-3201 Fax
info@f5networks.co.jp

Part No. DS-BIG-IP_SAM 0508