Alcatel-Lucent OmniAccess SafeGuard

APPLICATION LEVEL NETWORK ACCESS CONTROL

Alcatel-Lucent's OmniAccess Safeguard products enable enterprises to secure their LANs by controlling which users may access the LAN and restricting what they can do while on the LAN. In addition, the OmniAccess SafeGuard products characterize traffic patterns and identify intrusions based on pre-configured heuristics resulting in user and network protection against known or unknown attacks.

These Alcatel-Lucent purpose-built devices can be deployed in-line over an existing and mixed network infrastructure without the need to reconfigure any network elements. The OmniAccess SafeGurad appliances, which are based on custom silicon, offer LAN speed performance and can be deployed in High Availability mode to guarantee overall network availability. The OmniAccess SafeGuard makes it easy for IT to embed security within the LAN with minimal disruption and without compromise on performance or availability.

COMPLETE SET OF CAPABILITIES TO PROTECT ENTERPRISE ASSETS

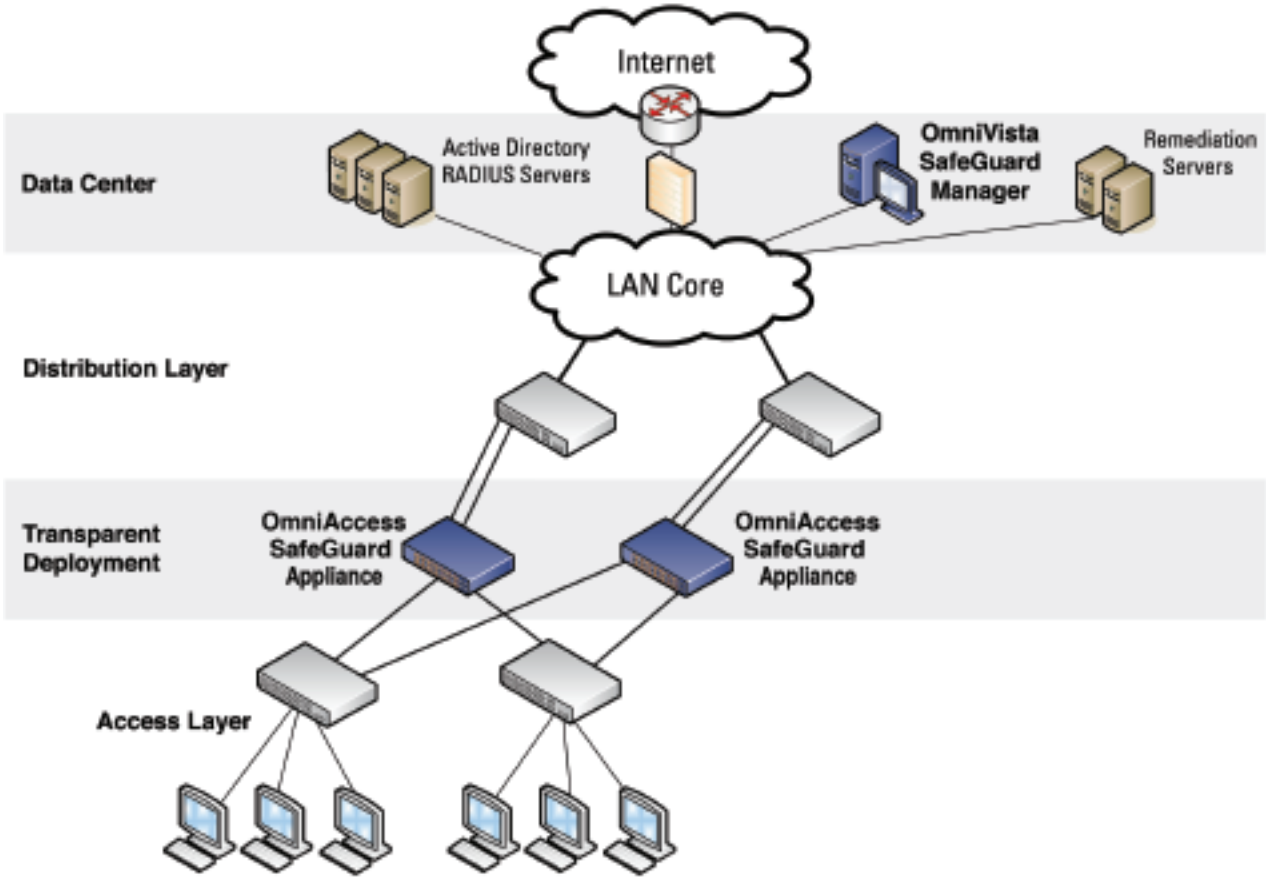
Network Admission Control (NAC) – user authentication and host integrity check to control who may enter the LAN

Visibility – incident- and exception-based information at layer 7, including attributes, such as file name, tied back to the user

User-based access – role-based provisioning to control user activities on the LAN, which includes control over what resources are accessible and what applications can be used by a given user based on the user's credentials.

Intrusion detection and quarantine – anomaly-based detection and containment of worms and other malware to prevent network meltdown and protect network hosts

Visibility – logging of user activity all the way to the application layer (layer 7), including application attributes, such as file name, or URL accessed by the user



The OmniAccess SafeGuard Appliance works with existing LAN infrastructure and authentication databases to provide these control capabilities.

The Alcatel-Lucent OmniAccess SafeGuard silicon architecture provides the foundation for the SafeGuard Appliances' capabilities. This custom hardware includes a 128-core processor and two programmable ASICs that work together to perform deep packet inspection at 10 Gbps. The programmability of the hardware enables Alcatel-Lucent to keep pace with changes in applications and security requirements.

Support for Key IT projects

GUEST / CONTRACTOR ACCESS

Most enterprises are struggling today to provide expected networking services for guests, such as access to the Internet. In addition, contract workers are increasingly present in the enterprise, and these users need a greater level of LAN access than just basic Internet services. The IT department has to support these users without compromising the security of the LAN.

The OmniAccess SafeGuard product family makes it easy to enable guest and contractor access by performing the following:

- automatically recognize guests vs. contractors vs. employees coming onto the LAN
- automatically apply access controls based on user role – "guest", "contactor"
- scan guest and contactor's machines for malware using a dissolvable agent
- restrict the network zones guests can access
- restrict which servers contractors can reach
- limit the applications guests can run (such as blocking IM)
- limit the applications contractors can run (such as allowing only key business applications and the application the contractor is helping to manage)

LAN SEGMENTATION

LAN segmentation is a valuable tool for separating various user groups and restricting access to critical resources. The OmniAccess SafeGuard product family offers a highly granular, application level LAN segmentation solution. The identity-based control at the foundation of the OmniAccess SafeGuard architecture provides the following:

- authenticate users to determine appropriate access to the network
- automatically learn user role during authentication
- enforce access control, to applications and servers for example, based on role
- track the activities of all users
- easily tie incidents to policies for compliance and troubleshooting

LAN segmentation can be implemented with no changes to the LAN. All features are delivered by a single, integrated platform for ease of operations and troubleshooting.

REMOTE VPN ACCESS

One of the groups that presents a particular risk for enterprises is remote users accessing the LAN over a VPN. The OmniAccess SafeGuard product family provides IT with a number of ways to ensure appropriate access for VPN users. The OmniAccess SafeGuard platforms:

- authenticate users over the VPN by providing a second login via a captive portal
- perform a posture check to ensure the device is free of malware
- automatically identify a user's role during authentication
- deploy role-based access controls
- apply universal or location-specific policies (e.g., reduce access to remote vs. local users)

REGULATORY COMPLIANCE

Many regulatory bodies require access control as part of their compliance. Whether it's S-Ox, HIPAA, or PCI, these regulations present the following challenges:

- IT must control access to key data and document those controls
- user-based auditing
  - ¬ access is typically spread out across multiple servers, applications
- IT must complement granular application-level controls with basic network-level "allow" or "deny" access controls

The OmniAccess SafeGuard product line helps IT with the segmentation, access control, and auditing needs demanded by many regulations. The OmniAccess SafeGuard platforms let IT:

- authenticate users for access to the LAN
- tie users to addresses and applications
- apply role-based controls for who can access which data
- document that policies are in place
- provide an audit trail by user, application, or server

MALWARE CONTROL

Frequent hosting of guests and contractors as well as the continuous migration of laptops between trusted and untrusted onramps to the Internet make the LAN susceptible to the propagation of malware. With the OmniAccess SafeGuard product family, IT gets a powerful tool in the fight against malware. The OmniAccess Safeguard platforms can:

- run a scan for malware prior to LAN admission
- use custom algorithms to detect malware after a user is on the LAN
- have algorithms tuned for anomalies based on application
- enable IT to block just an infected application or all traffic from an infected user
- prevent the spread of malware that can affect overall LAN availability

Deployment – Transparency, High Availability

The OmniAccess SafeGuard Appliance sits between access switches and the distribution or core layer, aggregating uplinks from the wiring closets and enforcing access policies on all traffic. It is a transparent device that does not require changes to the network design or user behavior, thus simplifying deployment and IT's cost of operations.

The OmniAccess SafeGuard Appliance supports high availability and resiliency modes. For example, enterprises that have dual-homed their wiring closet switches can deploy two OmniAccess SafeGuard Appliances as peers – the two platforms share authentication state and will preserve user authentication in case of failover. In addition, the appliance itself supports two failure modes. IT

can set the device to fail to pass through, where all LAN traffic will traverse the appliance untouched, or fail to block, where all traffic is stopped. The appliance also includes redundant power supplies and fans.

Operation – User-based Visibility, Central Configuration and Management

The OmniAccess SafeGuard appliances use deep packet inspection to admit users onto the LAN, provide visibility into LAN activities, control access based on identity, and contain malware and other attacks. The Alcatel-Lucent OmniVista SafeGuard Manager provides IT with the means for capturing and viewing all the data as well as for setting policies.

OmniVista SafeGuard Manager aggregates all traffic capture data and presents IT with actionable information, showing key security incidents in at-a-glance summaries and drill-down, detailed views. OmniVista SafeGuard Manager also enables rapid forensic troubleshooting, auditing, and reporting.

OmniVista SafeGuard Manager's GUI-based tools simplify policy creation and distribution. InSight includes templates that make it easy for IT to create policies and deploy them on OmniAccesss SafeGuard devices. The OmniAccess SafeGuard platforms automatically derive users' roles, and OmniVista SafeGuard Manager uses that role information as the basis for security policies.

OmniVista SafeGuard Manager also supports filters that let IT treat policies as building blocks and layer on multiple levels of control more easily. The flexible exception rules, combined with the policy filters, let IT create unique controls by role without creating a separate policy for each variation.

The OmniAccess SafeGuard appliances also integrate into the OmniVista 2500 through topology and event applications. Furthermore, the OmniAccess SafeGuard conforms to OmniVista 2770 Quarantine Manager's Syslog API to report security threats. Integration of the OmniAccess SafeGuard into OmniVista 2500 adds another simplification to the network management tasks.

Product Family

The Alcatel-Lucent OmniAccess SafeGuard Appliance is available in two models – the OmniAccess 1000 SafeGuard (OAG-1000) and the OmniAccess 2400 SafeGuard (OAG-2400). The OAG-1000 supports up to 800 authenticated users across four gigabit uplinks, with deep packet inspection at 4 Gbps. The OAG-2400 supports up to 2,000 authenticated users across ten gigabit uplinks, with 10 Gbps of deep packet inspection.

Security Features – Leveraging OmniAccess SafeGuard Software

USER / MACHINE AUTHENTICATION

- Authentication via captive portal or MAC address
- Active directory authentication snooping
- 802.1x RADIUS authentication snooping

ROLE DERIVATION

- RADIUS attributes
- Active directory attributes
- Physical location
- Combination of above

ROLE-BASED POLIC

Control access by:

- User group
- Application
- Select application attributes
- Destination port
- Resource (e.g., servers)

HOST INTEGRITY CHECK

- Dissolvable agent
- Scans for known threats, anti-virus definition, service packs, and custom registry keys and files

THREAT DETECTION / MITIGATION

- Zero-hour threat detection
- No signature updates necessary
- Drops malformed packets
- Block by: physical port, SRC MAC, offending application

ENFORCEMENT ACTIONS

- Allow
- Deny
- TCP reset
- Mirroring, logging

VISUALIZATION

- Ties usernames to applications and security violations
- Identifies applications and application content
- Reports application details to centralized policy

CENTRALIZED VISUALIZATION

- Ties into Alcatel-Lucent OmniVista SafeGuard Manager
- User and application usage repository
- Real-time alert dashboard
- Fully drillable forensics capability
- Reporting with scheduler
- Full policy and role-derivation configuration GUI

LOGGING AND REPORTING

- Direct syslog reporting
- Detailed security log messages
- Formatted for SIEM integration

MANAGEMENT AND CONTROL

- Industry-standard command line interface (CLI)
- Managed by Alcatel-Lucent OmniVista SafeGuard Manager
- SNMP v1/v2c
- Formatted syslog to multiple destinations
- Telnet
- SSH
- TFTP
- Standard and privileged access modes

ADMINISTRATOR AUTHENTICATION

- RADIUS authentication

Physical Features – Optimized for High Density Resilient Installation

STANDARDS AND PROTOCOLS

- 802.1D bridging
- 802.3 10BaseT
- 802.3u 100BaseTX
- 802.3z 1000BaseSX/T

LAYER-2 FEATURES

- 4,096 VLANs

DATA INTERFACE PORTS

- OAG-1000: 4 secure SFP port pairs
- OAG-2400: 10 secure SFP port pairs

SFPS AVAILABLE

- Single-mode or multimode 1 Gbps fiber, 10/100/1000 copper

NON-DATA INTERFACE PORTS

- OAG-1000: Two extensibility ports for packet mirroring or HA and one rear management port
- OAG-2400: Four extensibility ports for packet mirroring or HA and one rear management port

SECURED PROCESSING THROUGHPUT

- OAG-1000: 4 Gbps
- OAG-2400: 10 Gbps

AUTHENTICATED USERS

- OAG-1000: 400 users base model, 800 users via upgrade license
- OAG-2400: 1000 users base model, 2000 users via upgrade license Resiliency
- Dual active-active high-availability mode
- Fail pass-through (open)
- Fail block (closed)

LATENCY

- Average 30 microseconds

APPLICATIONS CLASSIFIED

- 300+ at Layer 4
- 30+ at Layer 7

DIMENSIONS

- 17.5 in. x 17 in. x 1.7in - 1U (44.5 x 43.2 x 3.8 cm)

WEIGHT

- 15 lbs. (6.9 kg)

OPERATING REQUIREMENTS

- Temperature: 0° – 40°
- Humidity: 5% to 90%, non-condensing

CERTIFICATIONS

- Emissions
- FCC Part 15, sub part B (USA)
- Class A, ICES-003 (Canada)
- EN55022 (CE Mark)
- Class A, EN55024 (CE Mark)
- VCCI Class A (Japan)

SAFETY

- UL 60950-1 (USA)
- CSA C2.22 No. 60950-1 (Canada)
- EN 60950-1 (CE Mark)
- IEC 60950-1 (International)
- NOM (Mexico)
- C-TICK (Australia)

POWER

- Dual redundant 180W 90-264VAC full range, 47-63Hz

COOLING

- Front-to-back air flow

www.alcatel-lucent.com

Alcatel·Lucent