AT-ST

Security Appliance System (SAS)

AT-ST

Security Appliance System (SAS)

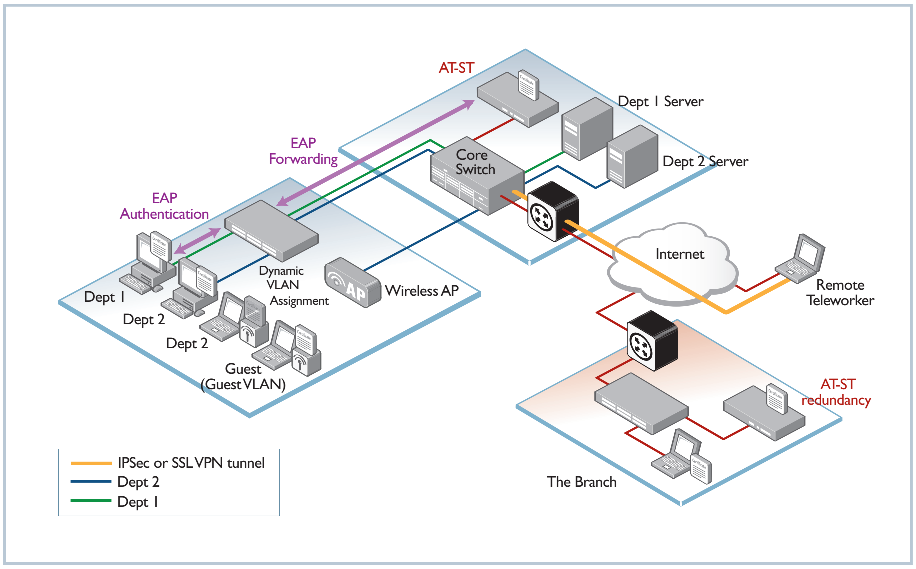
Overview

The Allied Telesis AT-ST is an all-in-one Security Appliance System (SAS).

The AT-ST combines the power and flexibility of a radius server, high-end authentication server (with CA certificates) and IEEE 802.1x manager in a rack-mountable device. Wired LAN, wireless or remote VPN users can be effectively secured, authenticated and managed from a central site.

All-in-one Authentication Server

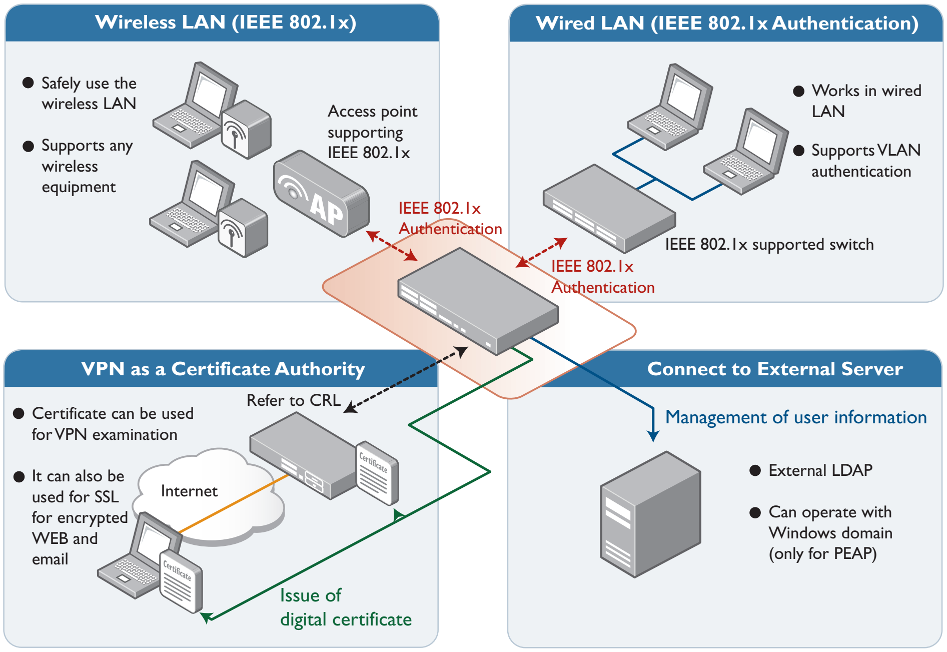
AT-ST SAS integrates multiple functions that include CA (Certification Authority), EAP-RADIUS, LDAP server, DHCP server, SNMP and NTP client, etc. It can work closely with wired or wireless IEEE 802.1x compliant network equipment to achieve EAP-RADIUS authentication, for prevention of unauthorized users accessing the network.



AT-ST Series: Security Appliance System with CA

Key Features

- Supporting full IEEE 802.1x authentication protocols:
  PPP-PAP, PPP-CHAP, EAP-TLS, EAP-TTLS, EAP-PEAP, CISCO-LEAP, MS-PEAP, EAP-MD5
- Supporting CA certificate to achieve a simple and highly secure network
- Supporting certificates issued by external CA server
- Querying external LDAP server as user database
- Working with MS windows domain authentication
- RADIUS agency (roaming)
- Supporting all IEEE 802.1x-compliance equipments of all main vendors
- Working in IPSec/SSL VPN
- Supporting redundant architecture
- Supporting simple DHCP server
- Network Time Protocol (NTP)
- Supporting UPS signaling
- Supporting Web GUI management
- User database import and export
- Local or remote (syslog) log information record
- Account group management


Wireless LAN (IEEE 802.1x)
● Safely use the wireless LAN
● Supports any wireless equipment
Access point supporting IEEE 802.1x
AP
IEEE 802.1x Authentication
Wired LAN (IEEE 802.1x Authentication)
● Works in wired LAN
● Supports VLAN authentication
IEEE 802.1x supported switch
IEEE 802.1x Authentication
VPN as a Certificate Authority
● Certificate can be used for VPN examination
● It can also be used for SSL for encrypted WEB and email
Refer to CRL
Internet
Certificate
Issue of digital certificate
Connect to External Server
Management of user information
● External LDAP
● Can operate with Windows domain (only for PEAP)

Ease-of use and Management

The AT-ST SAS locks down who can access your network from one device. There is no need to have multiple security devices, passwords and authentication policies for different security devices which are often hard to update and manage. This is easily managed from one central source for all your security needs.

Secure Authentication

No longer will unauthorized users be able to access the network via common switch ports. All users will need to pass authentication and be assigned a permission policy. The AT-ST SAS can work together with IEEE 802.1x compliant equipment to authenticate the users who want to access the network. Only the users who passed authentication successfully will be assigned a VLAN to access network resources according to their pre-assigned permission policy.

Guest VLAN assignment

In the event of a user not passing the authentication, the AT-ST SAS can assign this user into a 'guest VLAN', in which the users can access limited resources, such as web surfing or email. This function is very convenient for ad hoc visitors.

Securing Wireless LANs

The AT-ST SAS will provide you with the peace of mind to operate a Wireless LAN in a secure environment. The AT-ST SAS supports EAP-TLS, EAP- TTLS, EAP- PEAP and CISCO-LEAP. With dynamic WEP keys it avoids the risk faced by static WEP key methods which are easily cracked. In addition, the MAC authentication feature further enhances security down to a device level.

Digital Certificates and Certification Authority (CA)

The AT-ST SAS supports Certificate Authorities (CA) whereby all authorized users will be issued a digital certificate. This function negates the dangers faced with older methods dependent on user names and passwords which can be easily cracked or stolen.

USB Tokens

In addition, a client CA can be stored in a USB TOKEN, which can be carried about conveniently. When the USB TOKEN is plugged to the computer, the certificate information can be registered into a MS Windows system automatically. When the USB TOKEN is unplugged from the computer, the registered certificate information will be cleared automatically, to avoid others accessing the network using your certificate.

Remote VPN Users

With AT-ST's CA function, you can issue server certificates to VPN gateways and / or issue client certificates to client PC's. These can then be used to secure remote access by authentication between VPN gateways, or between a VPN gateway and VPN client.

PKI – Spoof Protection

PKI (Public Key Infrastructure) can be used for eliminating the following possible threats via a special security mechanism:

- Hostile users that target to steal important information or attack network by spoofing.
- Email content, credit card number and other sensitive data.

Redundant Architecture and DR Sites

Generally if a radius server fails, all users are denied access to network services. The AT-ST SAS has a redundant architecture option. This establishes a highly reliable security authentication system. Two AT-ST Security Appliance Systems can work as active and standby at different sites, while all management and configuration information is automatically synchronized. In the event that the active equipment fails, the standby equipment can take over all tasks seamlessly.

Simple and Power Management

With Web-based GUI, AT-ST provides simple and easy management. In order to prevent any misconfiguration, a wizard will lead you to set up the system step by step.

In addition, AT-ST provides various management features:

- All log information can be output to external syslog server.
- Simple DHCP server.
- Can be managed by open network management software, such as AT-SNMPc.
- As NTP client, it can synchronize time with NTP server.
- Support various network commands, such as ping and tracert, to help troubleshooting.
- Support UPS simple signaling to monitor the status of UPS.

AT-ST | Security Appliance System (SAS)

Specifications

Product	AT-ST	
No. of user licenses	1000 or less	5000 or less
Radius client	500	500
Redundancy	■	■
CA	■	■
Radius proxy	■	■
Integrated with domain	(option)	■
Group	(option)	■

Authentication

- EAP-MD5
- EAP-TLS
- EAP-LEAP
- EAP-PEAP
- EAP-TTLS
- PAP/CHAP

Private CA

- CA format
- Issue CA client
- Division of CA client
- Issue CA server
- Division of CA server
- CRL failure list

Performance

CPU	Intel P4 2.4GHz
RAM (DDR400)	256MB
Compact flash	512MB

Interface Connections

10/100/1000T	2
RS232C	1

Physical Characteristics

Dimensions	43.5cm x 28cm x 4.4cm
Weight	6.78Kg

Power Characteristics

Input voltage	100 ~ 240V AC
Frequency	50 ~ 60HZ
Power consumption	234W

Environmental Specifications

Operating temp.	0°C to 40°C
Storage temp.	-20°C to 75°C
Relative humidity	5 ~ 80% non-condensing
Storage humidity	5 ~ 95% non-condensing

Electrical/Mechanical Approvals

CE, FCC Class A

Ordering Information

AT-ST
Security Appliance System (SAS)

AT-ST-LIC-250
AT-ST 250 user license

AT-ST-LIC-500
AT-ST 500 user license

AT-ST-LIC-1K
AT-ST 1,000 user license

AT-ST-LIC-5K
AT-ST 5,000 user license

AT-ST-LIC-10K
AT-ST 10,000 user license

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis™