Solutions for LAN Protection

Allied Telesis security features safeguard networks and mitigate attacks
Introduction

The increasing number of connected devices in today's networks has created an insatiable demand for access to information, when and where we need it. This has changed the way we do business, as we are now becoming more and more reliant on Information Technology resources and applications. The security of digital assets has become a principal concern for network administrators, to ensure maximum availability of the corporate network and Internet access.

There are a number of ways to increase the robustness of your modern network. Allied Telesis uses industry leading switching technology to provide a comprehensive security suite, which supports a multi-layered approach to safeguard the network and combat common threats.

This solution document discusses three of the ways Allied Telesis switches ensure a reliable and secure network infrastructure. It also looks at some common network attacks, and how these can be mitigated using Allied Telesis equipment.

Multi-layered security

Providing a secure environment for shared corporate information and broader online access requires a considered approach. Allied Telesis switches support a cohesive solution including:

1. Secure switch management
2. Network security features
3. Network Access Control (NAC)

The outcome is a resilient and reliable environment for access to online resources.

I. Secure switch management

Allied Telesis switches have a number of secure management options.

An out-of-band Ethernet management port is provided to separate management access from network traffic. When remotely logging in to monitor or manage a switch, Secure Shell (SSH) access provides confidentiality and integrity of data by encrypting management sessions. Switches can be further secured by disabling unused access services, for example, HTTP server and Telnet server.

Network management systems often use Simple Network Management Protocol (SNMP) to communicate with network switches and other devices. Allied Telesis support of SNMPv3 provides secure access with authentication and encryption of management data.

Additionally, the Allied Telesis Graphical User Interface (GUI) utilizes SNMPv3 for protected access when using this visual tool for monitoring and management.

To provide a detailed audit trail in the event of a suspected security breach, or other problem, a Syslog server can be configured so switch log messages are stored in a central network repository.
2. Network security features

Allied Telesis switches provide numerous security features to enable a safe environment for sharing information. Let’s have a look at a few of these:

**Port Security**

The ability to limit the number of workstations that can connect to specific ports on the switch is managed with Port Security. If these limits are breached, or access from unknown workstations is attempted, the port can do any or all of the following: drop the untrusted data, notify the network administrator, or disable the port. Further to this, specific ports can be set to only allow network access at specific times of day. In this way, for example, a school can keep tight control over network access and application availability for students.

Advanced port security options allow this school to control the times of day that access to online resources and the Internet is available.
Secure configuration of Spanning Tree Protocol (STP)

STP is the most commonly used means of preventing loops in Layer 2 networks. There are two protection mechanisms that must be enabled to maximize robustness, since STP has no inbuilt security:

1. **STP Root Guard** - prevents a malicious user from accessing inappropriate data on the network, by allowing the network administrator to securely enforce the topology of the spanning tree.

2. **Bridge Protocol Data Unit (BPDU) Guard** - similarly increases the security of STP by allowing the network administrator to enforce the borders of the spanning tree, keeping the active topology predictable.

Storm Protection

Storm Protection reduces the adverse effects of any network loop that would potentially swamp the network. There are three facets that work together to protect the network from storms:

1. **Loop detection** - monitors traffic for the return of a loop detection probe packet. In the event of a problem, it can take a variety of actions including logging a fault, alerting the network administrator, or disabling a link.

2. **Thrash limiting** - detects a loop if certain device hardware addresses are being rapidly relearned on different ports. In the event of a problem, similar actions to those of loop detection can be taken.

3. **Storm control** - limits the rate at which a port will forward broadcast, multicast or unknown unicast packets. This controls the level of traffic that a loop may cause to be flooded in the network.

Control Plane Prioritization (CPP)

CPP prevents the Control Plane from becoming flooded in the event of a network storm or Denial of Service (DoS) attack, ensuring critical network control traffic always reaches its destination.

Denial of Service (DoS) attack prevention

A DoS attack is an attempt to make online resources unavailable to users. There are a number of known DoS attacks that can be monitored. When detected, the options are to notify network administration, and/or shut down the affected switch port.

Dynamic Host Configuration Protocol (DHCP) Snooping

DHCP servers allocate IP addresses to clients, and the switch keeps a record of addresses issued on each port. IP Source Guard checks against this DHCP snooping database to ensure only clients with specific IP and/or MAC address can access the network.

DHCP snooping can be combined with other features, like Dynamic ARP Inspection, to increase security in Layer 2 switched environments. It also provides a traceable history, which meets the growing legal requirements placed on Service Providers.

Access Control Lists (ACLs) and Filters

Managing traffic volume and the types of traffic allowed on the network is essential to ensure high performance, guard against unwanted traffic, and provide continuous access to important data. Allied Telesis powerful ACLs and filtering capability provide a mechanism for network traffic control, all handled in the switches hardware so wire-speed performance is maintained.
3. Network Access Control (NAC)

The security issues facing Enterprise networks have evolved over the years, with the focus moving from mitigating outward attacks, to reducing internal breaches and infiltration of malicious software. This internal defense requires significant involvement with individual devices on a network, which creates greater overhead on network administrators.

Allied Telesis lower this overhead and provide an effective solution to internal network security by integrating advanced switching technology as a part of Network Access Control (NAC). In conjunction with NAC, tri-authentication provides options for managing network access for all devices.

Network Access Control (NAC)

NAC allows for unprecedented control over user access to the network, in order to mitigate threats to network infrastructure. Allied Telesis switches use 802.1x port-based authentication in partnership with standards-compliant dynamic VLAN assignment, to asses a user’s adherence to network security policies and either grant authentication or offer remediation. Furthermore, if multiple users share a port then multi-authentication can be used. Different users on the same port can be assigned into different VLANs, and so given different levels of network access. Additionally, a Guest VLAN can be configured to provide a catch-all for users who aren’t authenticated.

Tri-authentication

Authentication options include alternatives to 802.1x port based authentication, such as web authentication to enable guest access, and MAC authentication for end points that do not have an 802.1x supplicant. All three authentication methods - 802.1x, MAC-based and Web-based, can be enabled simultaneously on the same port (tri-authentication).

Roaming authentication

Allied Telesis supports wireless connectivity with roaming authentication, which ensures mobile users are not inconvenienced by the need to re-authenticate as they roam. Their authentication information simply moves with them.

Two-step authentication

To maximize network access security, two-step authentication requires devices and users to be separately authenticated, to prevent sophisticated attempts to circumvent access control.

Strong Access Shield

By providing powerful authentication options as part of an integrated NAC solution, Allied Telesis switches constitute a secure wall around the edge of your LAN, allowing no infected or rogue devices to get network access.

For more information on Allied Telesis NAC and authentication options, search for our NAC solution guide online at alliedtelesis.com.
Mitigating common network attacks

Network security is significantly increased with the Allied Telesis superior multi-layer security suite that we’ve discussed. However, due to increased mobility and the wide availability of various hacking tools, attacks can still occur from within the LAN itself. Wired and wireless connections on the inside of the network constitute an ‘attack plane’ that cyber criminals will gladly exploit. Even a strong physical security system, preventing intruders from entering the building, is no guarantee of immunity from internally-launched attacks, and malware can easily enter the system through the unthinking actions of valid network users. Careful, thorough protection of the internal points of your network is an essential element of an effective data security system.

This section considers six of the more common information stealing and denial of service attacks, and explains how the Allied Telesis switch security suite protects your LAN, preserving the safety of both your mission-critical applications and your productivity.

1. MAC flooding attack

What are MAC flooding attacks?
MAC flooding attacks facilitate information stealing by providing a source of accessible data. In a MAC flooding attack, a malicious host sends packets from thousands of different bogus source MAC addresses, which then fill the forwarding database. Once full, legitimate traffic is flooded and becomes widely accessible, as the switch does not have room to learn any more specific destination addresses in the forwarding database. The malicious user has essentially turned the switch into a low intelligence pseudo-hub, allowing them to sniff all flooded traffic, thereby stealing data and passwords.

How do Allied Telesis switches protect you?
Allied Telesis switches provide two security measures to protect your LAN from MAC flooding attacks. The first is host authentication, whereby authenticating ports will only accept traffic from the MAC addresses of authenticated hosts. The second is port security, which controls how many MAC addresses can be learnt on a specific port. When a limit is breached, the switch will take one of three user-configurable actions — drop the un-trusted data, notify the network administrator, or disable the port while the intrusion is investigated.
2. Address Resolution Protocol (ARP) spoofing attacks

What are ARP spoofing attacks?
An ARP spoofing attack is another form of information stealing attack. A malicious host sends an ARP reply to a host’s ARP request for a server. The hacker falsely claims to be that server by tying their own MAC address to the IP address owned by the server. The bogus ARP message then also adds an entry into the switch ARP table. When workstation A sends a message destined for server B, then the bogus ARP entry diverts that message to hacker C. This enables the hacker to steal data and passwords.

How do Allied Telesis switches protect you?
Allied Telesis switches use DHCP Snooping with ARP Security to protect your network from ARP spoofing attacks. All ARP replies from un-trusted ports are checked to ensure they contain legitimate network addressing information, safeguarding the network and the business.
3. VLAN hopping attacks

What is a basic VLAN hopping attack?
A malicious user in one VLAN gains unauthorized access to another VLAN by sending tagged packets into the network with the VID of the target VLAN. By default, many switches will simply look at the tag on the packet, and pass the packet to the corresponding VLAN, even if the ingress port is not a member of that VLAN.

How do Allied Telesis switches protect you?
To eliminate basic VLAN hopping attacks, Allied Telesis switches use Ingress Filtering to drop packets tagged with VIDs that do not correspond to the VLAN of the ingress port, as workstations attached to edge ports should not send tagged packets into the network.
What is a double-tag VLAN hopping attack?
A malicious user sends a packet that is tagged twice. In the outer tag is their own VID, and in the inner tag is the VID of an unauthorized VLAN, to which the attacker is trying to gain access. The switch removes the outer tag and passes the packet to the next switch. The packet’s inner VLAN tag – the unauthorized VLAN’s VID – then becomes the sole VLAN identifier, and the packet makes its way to the target VLAN.

How do Allied Telesis switches protect you?
To eliminate double-tag VLAN hopping attacks, Allied Telesis switches employ the same solution as for basic VLAN hopping attacks. Ingress Filtering drops all tagged packets, since workstations attached to edge ports should not send tagged packets into your network.

Double-tag VLAN hopping attack:
1. Attacker sends double-tagged packets with an outer tag of the local VLAN, and inner tag of the target VLAN.
2. The switch strips off the first tag and sends back out.
3. Victim receives the packet.

Double-tag VLAN hopping defense:
1. Configure the switch’s edge ports with ingress filtering to accept ONLY untagged packets.
2. Double-tagged packets sent with an outer tag of the local VLAN, and inner tag of the target VLAN are dropped.
3. Tagged packets are dropped.
4. Spanning Tree Protocol (STP) Attack

What is an STP attack?
STP prevents loops in Layer 2 networks, while allowing path redundancy. Switch ports are designated as being either in a forwarding state or a blocked state. If a path becomes unavailable, the network responds by unblocking a previously blocked path to allow traffic to flow. STP is reliant on the establishment of a 'root bridge', which is the unique root of the network tree. In an STP attack, a malicious user sends an STP message - a Bridge Protocol Data Unit (BPDU) - with a priority value that makes it the root bridge, and thus compromises the network topology by forcing it to reconfigure.

How do Allied Telesis switches protect you?
Allied Telesis switches prevent Spanning Tree attacks by using BPDU guard on their edge ports, preventing bogus STP messages originating from a workstation. Additionally, the root guard feature can be used to narrow down the region of the network within which the root bridge must reside.
5. Dynamic Host Configuration Protocol (DHCP) attacks

DHCP servers allocate IP network addresses to hosts, allowing them to access resources on the network. There are two forms of DHCP attack which can compromise your network access: DHCP starvation attacks, and DHCP rogue server attacks.

What is a DHCP starvation attack?
In a DHCP Starvation attack, a malicious user inundates the DHCP server with countless DHCP requests from different bogus MAC addresses. The DHCP server eventually runs out of IP addresses. As a result, valid users are unable to obtain an IP address, effectively blocking their network access.

How do Allied Telesis switches protect you?
Allied Telesis switches prevent this specialized Denial-of-Service (DoS) attack with port security. Edge ports are configured with a MAC learn limit. Once the learn limit is reached, no further different MAC addresses are allowed on the port. Notifications can be sent to a network management station when the limit is reached to alert the network manager of excessive MAC activity on a port. Additionally, the port can be automatically disabled, to lock down that connection while the intrusion is investigated.
What is a DHCP rogue server attack?
A malicious user’s computer disguises itself as a DHCP server and responds to DHCP requests with bogus information. At the very least, this results in compromised network access. In more sophisticated attacks, it can be used to direct users to websites masquerading as secure sites, for example a bank, and thereby steal passwords and personal information.

How do Allied Telesis switches protect you?
Allied Telesis switches avoid DHCP rogue server attacks by using DHCP Snooping. Edge ports are designated as ‘untrusted’ ports. The switch will not accept and DHCP-server traffic on untrusted ports, so the rogue server is blocked from interacting with DHCP clients.
6. Denial of Service (DoS) attacks

What is a DoS attack?
There are many different types of DoS attacks that can threaten your network. Some attacks exploit invalid packet formats, causing target devices to ‘hang’ – e.g. the Tear Drop, IP Options or Ping of Death attacks. Other attacks initiate a packet storm targeted at a specific ‘victim’ – e.g. Smurf attacks. Still others initiate numerous TCP connections with a victim, to consume resources on the victim device – e.g. SYN flood attacks.

How do Allied Telesis switches protect you?
Allied Telesis switches are capable of mitigating all of the above attacks using DoS defence. Furthermore, the DoS defence for the majority of these attacks is implemented in the switch silicon, so it does not affect network performance.

Summary
With a powerful feature-set that ensures secure switch management, secure network infrastructure, and full user access control, Allied Telesis switches guarantee trouble-free access to online resources and applications.

The added benefit of mitigating many common LAN based attacks provides network administrators and business owners with peace of mind, and the knowledge that the network will continue its integral role in today’s business activities.
About Allied Telesis, Inc.
Founded in 1987, and with offices worldwide, Allied Telesis is a leading provider of networking infrastructure and flexible, interoperable network solutions. The Company provides reliable video, voice and data network solutions to clients in multiple markets including government, healthcare, defense, education, retail, hospitality, and network service providers.

Allied Telesis is committed to innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at alliedtelesis.com