Cisco TrustSec

PB616556

There are many challenges facing today's organizations. With outsourcing and mobile workforces, physical network boundaries are disappearing, giving way to "borderless networks." An increased threat environment demands more effective protection for business infrastructure and valuable information assets. Regulatory and industry mandates also impose strict security requirements. To protect their networks and data, organizations must establish visibility and appropriate access control for all users, and must discover and monitor IP-enabled devices.

Cisco TrustSec™ is an identity-enabled network access architecture that helps customers enable secure collaboration, strengthen security, and address compliance requirements. TrustSec components include the following:

- **Infrastructure:** Cisco Catalyst® 2960, 2960S, 3560, 3560E, 3560X, 3750, 3750E, 3750X, 4500E, and 6500E Series Switches and Cisco Nexus® 7000 Series Switches interact with network users for authentication and authorization.
- **Identity:** Flexible authentication methods include 802.1X, web authentication, and MAC authentication bypass, all controlled in a single configuration for each switch port.
  - **Authorization and enforcement options:** Besides VLAN and discretionary access control list (DACL) enforcement options, Cisco switches can tag each data packet with user identity information so that further controls can be deployed anywhere in the network. Accessing security groups using security group tags (SGTs) or security group access control lists (SGACLs) eliminates dependence on network topology, adding flexibility and significantly reducing traffic segmentation ACL management and overhead.
- **Security services:** Once users or devices are authenticated, additional security services can be applied to them. TrustSec integrates with Cisco NAC Guest Server for guest network access and with Cisco NAC Profiler for profiling and discovery of non-authenticating user devices, such as printers and IP phones. Data integrity via MACSec (802.1AE) address compliance by providing an encrypted link from the Catalyst 3750X or 3560X to the endpoint, or between data centers on the Nexus 7000.
- **Client:** TrustSec integrates with Cisco NAC Agent and the Cisco Secure Services Client (SSC). Cisco SSC provides 802.1X user and device authentication and manages user and device identity and network access protocols for secure wired and wireless access. Cisco NAC Agent is an optional lightweight agent running on an endpoint device. It performs deep inspection of the device's security profile by analyzing applications, registry settings, services, and files.
- **Policy and management:** In addition to handling the management of dynamic policies, Cisco Secure Access Control System (ACS) improves operations through its monitoring and troubleshooting features.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

TrustSec Feature Highlights

- **Flexible authentication:** Cisco supports the most flexible authentication options in the market. Businesses can support multiple methods of authentication, including 802.1X for managed devices and users, web authentication for guests or non-802.1X users, and MAC authentication bypass for unmanaged or non-802.1X devices. Additionally, the order and priority of authentication methods can be configured, along with configurable behavior after 802.1X or AAA server failures.
- **Flexible deployment modes:** Cisco supports three deployment modes - monitor mode, low-impact mode, and high-security mode - providing a phased approach for 802.1X deployment. In particular, monitor mode enables 802.1X to be enabled but without enforcement; this allows businesses to monitor the network authentications, evaluate their risks, and prepare the network for access control in later phases.
- **Multi-Domain Authentication Host Mode:** Cisco supports secure 802.1X or MAC authentication bypass of the IP phone and of the PC behind an IP phone on the switch infrastructure. This allows authentication of an IP phone in the voice VLAN and multiple hosts on the data VLAN on each switch port.
- **Unified guest access:** Cisco offers guest access integration via the NAC Guest Server. This provides the same user experience for guest access, regardless of whether the connectivity is wired or wireless.
- **Profiler:** The ability to identify and profile non-authenticating devices in the network is an important component of a complete NAC architecture. TrustSec integrates with NAC Profiler to enable automatic endpoint discovery and real-time and historic visibility for all endpoints.
- **Security group access:** SGTs enable user traffic to be tagged with identity/role information once authenticated at the ingress of the network. This creates a flexible, scalable, role-based architecture that uses SGACLs to control this traffic deeper in the network. For businesses using legacy platforms, Cisco offers the Security Group Tag Exchange Protocol (SXP), which enables identity information to be propagated to an SGT-capable device.
- **Monitoring and troubleshooting:** Monitoring and troubleshooting features in Cisco Secure ACS 5.2 allow IT administrators to quickly debug and troubleshoot authentication and security group access features, from live authentication results and statistics of endpoints to SGACL views when policies are triggered.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Deployment Topology

Figure 1. TrustSec Deployment Topology - Campus/Branch Wired and Wireless

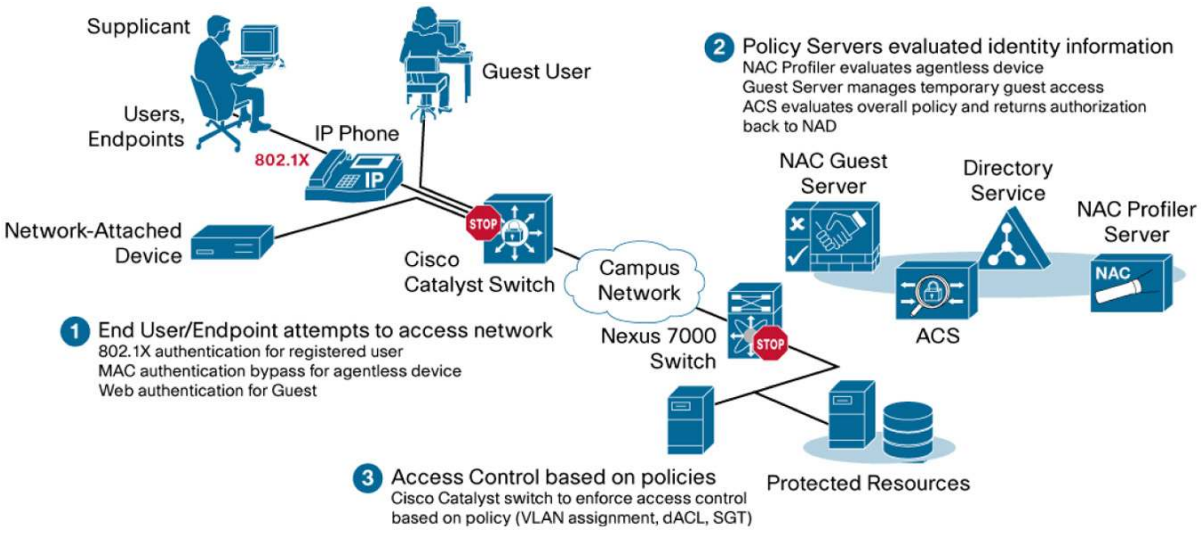

Figure 1 shows the 802.1X TrustSec deployment for wired and wireless users. Security group access is currently supported only for wired users (i.e., wired user access on campus or branch sites, with data center switch enforcement). TrustSec also supports an appliance-based model with Cisco NAC Agent and Server.

Platform Support Matrix

Platforms	Identity-Enabled Release (802.1X etc)	Security Group Access Release	Security Group Access Features	Now Orderable
Cisco Nexus 7000 Series	Cisco NX-OS 5.0(2) or later release. Base image	Cisco NX-OS 5.0(2) or later release. Advanced Service Package is required	SGACL, 802.1AE + SAP, NDAC, SXP, IPM	Yes
Cisco Catalyst 6500E Series (Supervisor 32, 720, 720-VSS)	Cisco IOS® Software Release 12.2(33)SXI7. IP Base image	Cisco IOS Software Release 12.2(33)SXI7. IP Base K9 image is required	NDAC (no SAP), SXP	Yes
Catalyst 4500E Series (Supervisor 6L-E or 6-E)	Cisco IOS Software Release 12.2(53)SG5. IP Base image	Cisco IOS Software Release 12.2(53)SG5. IP Base K9 image is required	SXP	Yes
Cisco Catalyst 3750X Series	Cisco IOS Software Release 12.2(55)SE3. IP Base image	Cisco IOS Software Release 12.2(55)SE3. IP Base K9 image is required	-	Yes
Cisco Catalyst 3560, 3560E, 3750, and 3750E Series	Cisco IOS Software Release 12.2(55)SE3. IP Base image	Cisco IOS Software Release 12.2(55)SE3. IP Base K9 image is required	SXP	Yes
Cisco EtherSwitch Services Module for Integrated Services Routers	Cisco IOS Software Release 12.2(55)SE3. IP Base image	Cisco IOS Software Release 12.2(55)SE3. IP Base K9 image is required	SXP	Yes
Blade Modules for Cisco Catalyst Switches	Cisco IOS Software Release 12.2(55)SE3. IP Base image	Cisco IOS Software Release 12.2(55)SE3. IP Base K9 image is required	SXP	Yes
Cisco Catalyst 2960 Series	Cisco IOS Software Release 12.2(55)SE3. IP Base image	Not supported	Not supported	Yes
Cisco Secure ACS	Cisco Secure ACS Version 5.2 Patch 3	Cisco Secure ACS Version 5.2 with TrustSec license required. Cisco 1120 Secure Access Server Appliance or ESX Server 3.5 or 4.0 is supported	Centralized policy management for TrustSec/NDAC authentication	Yes

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Platforms	Identity-Enabled Release (802.1X etc)	Security Group Access Release	Security Group Access Features	Now Orderable
Cisco NAC Guest Server	NGS version 2.0.3	-	-	Yes
Cisco Secure Services Client	Cisco SSC Version 5.1	SSC Version 5.1	802.1X client	Yes
Cisco NAC	Cisco NAC Agent, Server/Manager Version 4.7.2	-	-	Yes

Glossary: SXP = Security Exchange Protocol (IP-SGT binding), NDAC = Network Device Admission Control, IPM = Identity port mapping, SAP = Security Association Protocol

Cisco Services

Cisco Services maintain network health, protect and enhance infrastructure investments, and help businesses create intelligent, trusted, resilient networks that allow them to collaborate with confidence. Cisco Services address all aspects of planning, deploying, operating, and optimizing the network to help shorten implementation times and lower operating costs in building networks that support business goals.

For More Information

For more information about Cisco TrustSec, visit http://www.cisco.com/go/trustsec.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA C25-616556-01 08/11

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.