TrustSec Planning and Deployment Checklist

This checklist serves as a guide to help you understand the various components, technologies, and organizational efforts required for a successful Cisco TrustSec deployment. This document contains the following sections:

- Planning Considerations, page 1
- Deployment Checklist, page 4
- Test Scenarios, page 7
- References, page 8

Planning Considerations

Answering the following organizational and operational questions will help you understand some of the security requirements, business processes, and group dynamics that impact the integration and deployment of Cisco TrustSec in your network.

Security Policy Creation and Maintenance

[ ] Describe your desired network access policy. Include the authorization and handling of the following:

- Managed users including unique requirements for different groups and roles
- Unmanaged users—Contractors, extranets, labs, and so on
- Different access methods—Wired, wireless, VPN, virtual desktops, and so on
- Different locations—Sites, buildings, floors, and other locations
- Guests and visitors
- Agentless devices—IP phones, printers, and other devices

[ ] Is creating security policy and enforcing it performed by the same group within your organization or by different groups?

[ ] What does a quorum of policy decision-makers for making changes at your organization look like?

[ ] Will network access authorizations be based on endpoint or user identity, endpoint posture, or both?

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Public Key Infrastructure (PKI)

Certificates should be based on the fully-qualified domain name (FQDN) of the ACS server. Self-signed certificates are not recommended for production deployments.

[ ] Have you already deployed an enterprise PKI? Which one?

[ ] If not, do you expect to install and manage a PKI or purchase individual certificates from a CA vendor?

[ ] What is the process at your organization for obtaining a digital certificate?

[ ] What is your annual budget per server certificate?

[ ] If unable to use public or enterprise CA-signed certificates, does your organization fully understand the long-term usability, support, migration, and scaling issues?

Directory Services

[ ] Will you require identity for network authorization?

[ ] Will you use username/passwords, digital certificates, tokens, all of the above, or something different?

[ ] Will you integrate with existing identity stores such as Microsoft Active Directory, LDAP, Novell, or ODBC?

[ ] Do you have multiple identity domains to authenticate against, and if so, how many?

[ ] Will your existing identity store clusters scale to support the load from network authentication?

Network Access Devices (NADs)

[ ] Which edges of your network do you want to authenticate with Cisco Secure ACS and RADIUS? Wired? Wireless? VPN? Remote offices?

[ ] Does your existing hardware support the desired 802.1X functionality? Must you upgrade?

[ ] Do you plan to upgrade from Cisco CatOS to Cisco IOS to get the latest 802.1X features?

[ ] Do your NADs have enough memory for the latest Cisco IOS images and security features, or is a RAM upgrade required?

Managed Endpoints

[ ] Do you have an inventory of the number and types of network endpoints on your network today?

[ ] Do you already use 802.1X supplicants from Cisco or Microsoft? Wired or wireless or both?

[ ] Will the desired 802.1X supplicant require a software purchase, upgrade, or OS service pack?

[ ] Which authentication types are required or preferred?Agentless Endpoints

[ ] Do you have a method for automatically identifying and authorizing agentless endpoints on your network?

[ ] Have you identified the total number of agentless devices and device types in your network, which can include the following?

- No 802.1X supplicant (unsupported or hardened OS, such as phones or printers)
- Pre-execution Environment (PXE) network booting and reimaging
- Otherwise unmanaged/uncontrolled devices (guests, labs, and so on)

[ ] What is your method of identifying, classifying, and authorizing agentless endpoints?

- Upgrade to 802.1X capabilities in hardware and/or OS
- Whitelisting in NAD per MAC or IP
- Whitelisting in ACS (MAC Authentication Bypass [MAB], MAC wildcards)
- Whitelisting in LDAP or other identity store or database

[ ] What is your budget for administrative and management costs for manual MAB or endpoint registration system?

Cisco Secure Access Control Server (ACS)

[ ] Cisco Secure ACS v5.2 + patch 3 is currently recommended. Will you need to upgrade or purchase?

[ ] How many ACSes will you need to scale the deployment based on your organization size, availability requirements, revalidation frequency, and protocol choice?

[ ] How will you replicate policy changes: manually, periodically, scheduled, instantly?

[ ] Will any load balancing hardware or software be necessary for handling high numbers of concurrent authorizations?

Guest Services

[ ] What is your security policy for guests, visitors, or employees that cannot authenticate via 802.1X or MAB?

[ ] If you want to allow guests, do you have an existing guest portal such as the Cisco NAC Guest Server?

[ ] Who will be allowed to sponsor the guest accounts? Lobby staff or any employee in your directory?

[ ] What are the various guest service profiles that sponsors will be allowed to provision?

[ ] Will session length be based on the time-of-day or time-from-first-login?

[ ] What information will you require guests to provide in exchange for network access?

[ ] How will you audit sponsors, provisioned accounts, and account usage?

Monitoring, Reporting, and Troubleshooting

[ ] What is your existing monitoring and reporting application or toolset?

[ ] What are the long-term storage requirements for all of these new logs and events?

Communications

It is best to clearly communicate a change in your network access policy so that users are not surprised by new security and software requirements, access restrictions, or URL redirections.

[ ] Do you have clear authority from management to block, limit, and redirect non-compliant endpoints and users?

[ ] Have you raised awareness by discussing the needs and benefits with stakeholders and users for changes in network access policy?

[ ] Are the responsible groups ready for a unified response to non-compliant users?

[ ] Have you communicated with all users via multiple channels including email, intranet, a remediation website, and support desks?

Support Desk

[ ] Is the support staff trained for the new security technology, process, and policy?

[ ] How will the support staff troubleshoot support calls related to ACS-based RADIUS authentications?

[ ] Is any internal tool or application development required for ACS-related support?

Deployment Checklist

Based on your answers to the questions above as well as your existing network architecture, complete the tables on the following pages. This will be needed for RADIUS-based access control configuration and will be a valuable reference that speeds initial configuration in your deployment.

Security Policy

Describe your major network access scenarios and how you will use contextual, network-based attributes to authorize them (see Table 1). The total unique authorization states will determine your final ACS authorization policies.

Table 1 Security Policy

Scenario	Who (User)	What (Endpoint)	Where (Location)	When (Time)	How (Authorization)
Employee	AD Domain Users	Windows XPSP3 supplicant	Any	Any	Allow_All

Enforcement States

From the unique authorization states you determined in Table 1, document the specific RADIUS attribute settings for each state (see Table 2). This will help you understand the subtle differences between each enforcement state and identify the number of unique ACLs you must create.

Table 2 Enforcement States

RADIUS Attribute	Allow_All				
VLAN ID/Name	ACCESS				
URL for Redirect	-				
URL Redirect ACL	-				

Table 2 Enforcement States

Downloadable ACL Name	ACL-ALLOW-ALL				
Voice VLAN Permission	No				
Reauthentication: Timer	28800 (8 hours)				
Reauthentication: Maintain Connectivity	Yes				

Digital Certificates

Create and use CA-signed certificates for your TrustSec infrastructure to minimize long-term problems due to untrusted, self-signed certificates (see Table 3).

Table 3 Digital Certificates

Component	FQDN	Org Unit	Org	City	State	Country (2 letter)	Key Size (max)	Cert Format
Certificate Authority								
ACS								
NAC Guest Server								

Network Services

List all basic network services and the hosts that provide these services in your network (see Table 4). This will help with access control list (ACL) exceptions and TrustSec service configuration.

Table 4 Network Services

Role	DNS Names	Network Address(es)	Details
CA Server(s)			
DNS Server(s)			
DHCP Server(s)			
NTP Server(s)			
FTP Servers			username:password
Proxy Servers (to Internet)			username:password
TFTP/PXE Boot Servers			username:password
Syslog Servers			username:password
Identity Store: Active Directory			username:password
Identity Store: LDAP			
Identity Store: OTP			
ACS RADIUS Server			CLI: admin: password Web: acsadmin: password AD: username:password
NAC Guest Server		IP: eth0 MAC:	CLI: root:password Web: admin:password

Endpoints

How will all of the various network endpoints be authenticated when TrustSec is enabled? Possible authentication methods include 802.1X, MAB, and Web Authentication. Use Table 5 to record endpoint information.

Table 5 *Endpoints*

Endpoint	Authentication Method	Notes
Windows XP SP# (Native Supplicant)		
Windows Vista SP# (Native Supplicant)		
Windows 7 (Native Supplicant)		
Windows 7 (AnyConnect)		
Windows XP SP3 (Secure Services Client)		
Apple MacOSX 10.6.x (Native Supplicant)		
Linux (No Supplicant)		
Cisco 79xx Phones		
Cisco APxxxx		
Printers		
Servers		
Guests		
PXE Boot		

Network Devices

Document the network access devices in your network by model, supervisor (if appropriate), and software version (see Table 6). Each network device IP address must be added to ACS unless you use wildcard entries. It is highly recommended that you upgrade all switches to the latest tested and validated version in the Cisco Validated Design (CVD) to avoid feature and behavior inconsistencies.

Table 6 *Network Devices*

Model	Cisco IOS Version	Management IP Address	Management DNS Name

Common TrustSec RADIUS Authorization Attributes

Table 7 lists the most commonly used RADIUS attributes for TrustSec with campus access switches.

Table 7 Common TrustSec RADIUS Authorization Attributes

Vendor Name	Attributes	Value	Description
IETF	Session-Timeout (27)	28800	8 hours
IETF	Idle-Timeout (28)	300	5 minutes
IETF	Termination-Action (29)	RADIUS-Request (1)	Maintain connection while re-authenticating
IETF	Tunnel-Type (64)	[T1] VLAN (13)	
IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)	
IETF	Tunnel-Private-Group-ID (81)	[T1] <name or number>	VLAN name or number
Cisco	cisco-av-pair (1)	device-traffic-class=voice	Enable Voice Domain
Cisco	cisco-av-pair (1)	url-redirect= http://server.mycompany.com/directory/file.html	Redirection URL
Cisco	cisco-av-pair (1)	url-redirect-acl=url_redir_acl	ACL to match URL redirection or not

Test Scenarios

Based on your security policy, anticipated endpoints, and enforcement states, create a list of scenarios to test in your lab or small proof-of-concept deployment before production deployment. Table 8 lists some suggested scenarios to get you started.

Table 8 Test Scenarios

Scenario	Notes (Pass/Fail/Other)
802.1X	
802.1X allows host to join Windows domain	
802.1X machine authentication	
802.1X user login to Windows domain	
802.1X sngle sign on (SSO): username/password	
802.1X user-initiated password change	
802.1X Active Directory required user password change	
802.1X login successful for all user groups and VLANs	
Guest sponsorship	
Guest access	
Supplicants	
Validate VLAN changes for ACCESS <=> GUEST (if used)	
EAPoL-Logoff sent on user logoff	
EAPoL-Start sent on new user logon	
GPOs works for wired	
Login scripts work	
SSO works for wired	
New machine can join domain with supplicant	
New AD user can login on host	

Table 8 Test Scenarios

Cisco ACS	
ACS access service: 802.1X	
ACS access service: machine authentication	
Appliance: remote syslog	
Replication configuration and success	
Verify existing AAA infrastructure works on new ACSes	
ACS redundancy: RADIUS failover to secondary ACS	
AD redundancy: ACS failover to secondary domain controller	

References

TrustSec 1.99 Documents

- Wired 802.1X Deployment Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Dot1X_Deployment/Dot1x_Dep_Guide.html
- IP Telephony for 802.1X Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/IP_Tele/IP_Telephony_DIG.html
- MAC Authentication Bypass Deployment Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/MAB/MAB_Dep_Guide.html
- TrustSec Phased Deployment Configuration Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Phased_Deploy/Phased_Dep_Guide.html
- Local WebAuth Deployment Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/WebAuth/WebAuth_Dep_Guide.html
- Scenario-Based TrustSec Deployments Application Note—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Scenario_based_AppNote/Scenario_based_AN.html
- TrustSec 1.99 Deployment Note: FlexAuth Order, Priority, and Failed Authentication—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/FlexAuthNote/flexauth-note.html
- TrustSec Planning and Deployment Checklist—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/TrustSec_Checklist/trustsec-199_checklist.html

Related Documents

- Configuring WebAuth on the Cisco Catalyst 3750 Series Switches—http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3750/software/release/12.2_55_se/configuration/guide/sw8021x.html
- Configuring WebAuth on the Cisco Catalyst 4500 Series Switches—http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst4500/12.2/53SG/configuration/webauth.html
- Configuring WebAuth on the Cisco Catalyst 6500 Series Switches—http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html
- Cisco IOS Firewall authentication proxy—http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0.shtml
- WebAuth with Cisco Wireless LAN Controllers—http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml#external-process