BYOD Smart Solutions: Suggested RFP Questions

BYOD Overview

Bring Your Own Device (BYOD) has become one of the most impactful trends that has or will touch each and every IT organization. The term has come to define a megatrend occurring in IT that requires sweeping changes to the way devices are used in the workplace.

BYOD allows end users to use the compute and communication devices they choose, to increase productivity and mobility. These can be devices purchased by the employer, purchased by the employee, or both. BYOD means any device, with any ownership, used anywhere.

Several groups within the enterprise are being challenged by the BYOD issue and want to be involved (see Figure: BYOD: A Enterprise-Wide Project). Implementing a BYOD solution can bring in representatives from the endpoint team, the compliance team, the security team and very interestingly, some customers are also bringing in the human resources (HR) group.

Figure 1: BYOD: An Enterprise-Wide Project

Devices/Endpoints

1. How does the BYOD solution provide and support a broad range of device choices?
2. What are the device types that will be supported for provisioning?
3. Does the solution provide the ability to “whitelist” a device as well as “blacklist” it?
4. Is Integrated Device Profiling and Posture Assessment supported? If so, how?
5. What tools are available to discover and profile end devices automatically?
6. Are flexible device deployment models such as virtual desktop infrastructure (VDI) and collaboration applications such as instant messaging (IM), telephony, and conferencing supported to provide a consistent and rich user experience?
7. Is it simple to onboard and apply corporate policy to new devices accessing the network resources, whether wired or wireless?
8. Can I apply and manage one corporate policy across the entire network?
9. What components are necessary to implement your BYOD solution?
10. What is the strategy for identifying a corporate-owned or personal device?

Security/Authentication

11. What tools are in place to maintain secure access to authorized information in my corporate network from any device?
12. How are users and devices authenticated to the network?
13. How does the onboarding process for new devices begin?
14. What steps are followed when a device connects to the network?
15. How is different access allowed to the user?
16. What happens if devices are not part of the whitelist identity group?
17. How are digital certificates securely deployed on the network?
18. To provision digital certificates using your BYOD solution, what steps need to be followed?
19. How does a user gain access to the network from a personal device?
20. Does the solution provide role-based access and can I manage this within an existing logical design?
21. How is secure remote access capability integrated with the solution? Some examples include automatic VPN connection, identity-based access control, data loss protection, and acceptable use policy.
22. Are mobile device management (MDM) capabilities provided? What if I already have an MDM deployed?
23. How is authentication control provided in a flexible and comprehensive manner in the solution?

Unified Infrastructure

24. Does the BYOD solution integrate with and leverage the capabilities of my existing network, both wired and wireless?

25. What does your BYOD solution use to gain visibility and control of the wired/wireless endpoints?

26. Can I use the security, visibility, policy management, and monitoring/ forensics capabilities of my existing wired network in the BYOD solution? Will I have to deploy all new gear to deploy and benefit from the solution?

27. Is 802.1X capability integrated into the BYOD solution?

28. How is information from users, devices, infrastructure, and network services gathered to enforce contextual-based business policies across the network: wireless, wired, or VPN?

29. What specific capabilities in the wired and wireless network are key to supporting the full range of BYOD deployment scenarios? Explain the role of these services and the infrastructure providing them.

30. How is the wireless network optimized for performance, scalability, and user experience for clients?

31. Does your wireless infrastructure include access points (APs) with dedicated hardware for Spectrum Intelligence?

32. Does your wireless infrastructure include APs with dedicated hardware for Beamforming?

33. Does your wireless infrastructure include APs that support 4x4:3 multiple-input multiple-output (MIMO)?

34. Can your wireless infrastructure be upgraded to support 802.11ac?

Management

35. With the increase in connected devices, what tools are in the BYOD solution to manage security and policy enforcement?

36. What management tools does your solution provide to find and solve problems quickly regardless of whether the issues are with the wired, wireless, or other sub-systems within the network?

37. Does the management system provide a view of all devices, by user, across wired and wireless networks?

38. Does the system consolidate system-wide data (wired, wireless, and identity) for monitoring and troubleshooting purposes?

References

Cisco BYOD Smart Solution: http://www.cisco.com/go/byod/

Cisco BYOD Smart Solution Design Guide (July 13, 2012):
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html

Unified Access Design Guide (October 18, 2011):
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/Unified_Access_Book.html

TrustSec 2.0 Design Guide:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf

Cisco Borderless Campus 1.0 Cisco Validated Design Guide:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1.0/Borderless_Campus_1.0_Design_Guide.html

Cisco AnyConnect 3.0:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac01intro.html

Configuring Certificates:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

Configuring Tunnel Groups, Group Policies, and Users:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/vpngrp.html

Adaptive Security Device Manager (ASDM) User Guide:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/usrguide.html

Deploying the AnyConnect Secure Mobility Client:
http://www.cisco.com/en/US/partner/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac02asaconfig.html#wpxref89319

SSL VPN Security: http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html

Setting Up Secure Device Provisioning (SDP) for Enrollment in a Public-key Infrastructure (PKI):
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_setup_SDP_piki.html#wp1054812

iPhone® Configuration Utility: http://www.apple.com/support/iphone/enterprise/

iPhone OS Enterprise Deployment Guide:
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

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.