Secure Access Architecture Talking Points

Overview

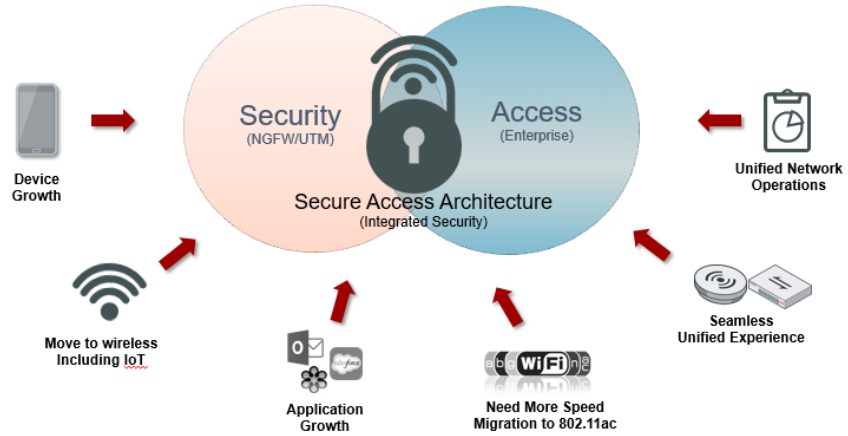
- Technology and market trends are rapidly changing the way enterprise organizations deploy local area networks, connect end devices and enable business applications of every type. But the implication of these changes and the following trends impact how networks must be secured.
- The number and types of network-connected wireless devices continues to grow exponentially.
- Wi-Fi is becoming the primary access medium for many of these network devices.
- The growth of mobile applications goes hand in hand with the growth in the number of devices.
- On top of this unprecedented growth in applications and device diversity, users expect a unified access experience – one that ensures consistent secure, application and device policies across both wired and wireless environments.
- Fortinet's network access solutions offer the best of next-generation firewall capabilities together with enterprise access. As opposed to traditional wireless solutions which only address connectivity, Fortinet's secure access solutions have robust network security at their core in addition to connectivity.

Did you know?

- **Growth in Unsecured Connected Devices and apps**
  - 33 billion endpoints will be connected by 2020.
  - The exponential increase in connected devices present new vulnerabilities and a growing attack surface which hackers can use to exploit.
  - IoT devices in particular such as wireless sensor nodes, location based beacons and other small devices often are not capable of supporting a suite of security solutions.
  - New vulnerabilities that stem from applications never seen before on the network.
- **Wireless network vulnerabilities are coming into question**
  - Recent Fortinet surveys indicate strong concern from CIO and IT administrators about the vulnerabilities of their wireless access network.
  - US FAA cites In-flight wireless entertainment systems open to cyberattacks. - 2015
  - Hackers breach Wi-Fi to keylog targeted executive's devices – specifically those in the defense industry. - 2015

The Highlights

- **Security + Access:** Fortinet's secure access solutions have robust network security at their core in addition to connectivity.
- **Deployment Flexibility:** Fortinet offers three solutions: Infrastructure, Integrated and Cloud



Target customers

- Organizations that have traditionally deployed access or security without much coordination between the two.
- Enterprise/SMB customers looking to refresh wireless LAN
- Enterprise/SMB customers looking to refresh wired network
- Enterprise customers looking to integrate management of network access and security infrastructure.

FORTINET®

Secure Access Architecture Talking Points

Key Resources

- Secure Access Architecture Presentation
- Secure Access Architecture Solutions Guide
- Connect and Secure Solutions Guide
- Competitive Brief – Aruba-Ruckus-Cisco
- Secure Access Architecture - First Call Script
- Secure Access Architecture Video
- Secure Access Architecture FAQ

Qualification Questions to Ask Customers and Prospects

1. Have you heard of any recently publicized network breaches?
    a. If NO mention: An alarming gap exist today between our networks and cybersecurity protections. A number of reports and articles which I will send to you after the call from Consumer Affairs, The U.S. Government Accountability Office, recently publicized breaches and even Fortinet's own independent research highlight the risks.
2. Are you looking to gain more control over the security of your access network?
    a. Mention: Companies NEED protection across their entire network, ESPECIALLY at the access layer, to guard against internal and external threats.
3. Are you looking to refresh your wireless network? Refresh your wired network?
    a. If yes, use Call Script to further qualify opportunity.
4. Do you have a policy permitting personal devices to access the network? Do people use their personal devices on your network, whether or not it is explicitly allowed?
    a. If yes, mention proliferation of devices and unsecured applications open attack surface of network.
5. How much time do you think the IT staff spends provisioning and managing network access for guests or employees' personal mobile devices? How much does this add up to over the course of the year?
    a. If this is a problem, cite the need for a more integrated management solution that covers wired, wireless and security. – Secure Access Architecture.
6. Do you have business-critical or life-critical applications that must receive priority delivery over the network?
    a. If yes, (ie; healthcare) cite the need for uninterrupted network service layers that span to the physical layer. Secure Access Architecture.
7. Would you like to be able to offer differentiated services based on the location of user's mobile device?
    a. Mention – FortiPresence
8. How are you planning additions to your existing wireless network? What tools are you using?
    a. Mention: FREE FortiPlanner tool available for download

Secure Access Architecture Diagram