Google for Education

Google Education – panduan infrastruktur akses

Daftar Isi

Google for Education

Google Education – panduan infrastruktur akses

Ikhtisar
Dokumen ini disusun untuk memberi panduan dalam membangun infrastruktur akses internet (jaringan) kampus yang akan mendukung layanan komputasi awan. Dokumen ini memandu Anda melalui berbagai elemen akses yang harus dipertimbangkan, standar yang diperlukan untuk jaringan fungsional yang dapat digunakan untuk mengakses layanan komputasi awan, serta hal-hal yang harus dilakukan saat membangun infrastruktur. Dokumen ini mengarahkan Anda ke beberapa solusi yang tersedia saat ini dan mitra di berbagai belahan dunia yang dapat membantu Anda membangun jaringan yang baik. Terakhir, dokumen ini memberikan kerangka untuk mengembangkan action plan Anda.

Disclaimer
Google tidak menyediakan dukungan teknis untuk mengonfigurasi produk pihak ketiga. Apabila terjadi masalah pada produk pihak ketiga, Anda harus menghubungi administrator jaringan. GOOGLE TIDAK BERTANGGUNG JAWAB ATAS PRODUK PIHAK KETIGA. Anda juga dapat menghubungi Penyedia Solusi Google untuk berkonsultasi mengenai layanan yang dapat mereka berikan. Tautan ke situs web pihak ketiga disediakan untuk kemudahan Anda. Tautan dan kontennya dapat berubah tanpa pemberitahuan. Kunjungi situs web produk yang sesuai untuk mendapatkan informasi konfigurasi dan dukungan terbaru.

Elemen infrastruktur akses
Di bawah ini adalah semua area jaringan akses yang berkontribusi pada keberhasilan dan ketangguhan deployment di kampus

a. Bandwidth di kampus (termasuk redundansi)
b. Firewall
c. WAN / link intrakampus
d. LAN
    i. Router
    ii. Sakelar
    iii. VLANS
    iv. Wired ports
    v. WiFi
        1. Perancangan Radio AP
        2. Daya AP
    vi. Pengontrol akses
    vii. DHCP
    viii. DNS
e. Perangkat lunak Pengelolaan Jaringan
f. Perangkat lunak Pemantauan
g. Pemfilteran konten
h. Kontrol akses / Keamanan
    i. SSO
    ii. RADIUS

Dokumen ini membahas semua area yang dicetak tebal di atas. Area lainnya dibahas di dokumen Google "Praktik terbaik jaringan untuk deployment skala besar".

Standar minimum untuk mengakses layanan awan Google
Tabel di bawah ini mencantumkan kecepatan minimum yang diperlukan user pengguna secara serentak untuk setidaknya dapat bekerja dengan cukup baik. Singkatnya Anda membutuhkan antara 64kbps hingga 1Mbps per pengguna secara serentak, bergantung pada layanan yang digunakan pengguna. Rumus sederhananya:

$TBWx = (\%C * CCUx * SBWx)_1 + (\%C * CCUx * SBWx)_2 + \ldots\ldots + (\%C * CCUx * SBWx)_n$

- TBWx = Total BW pada tingkat X dari jaringan Anda
- CCUx = Jumlah pengguna secara serentak pada tingkat X dari jaringan Anda
- %C = Persentase pengguna secara serentak yang menggunakan layanan khusus pada tingkat x dari jaringan Anda
- SBWx = Kbps yang disarankan berdasarkan layanan (lihat tabel di bawah)
- n = jumlah layanan yang diakses pada tingkat x dari jaringan Anda

Pengalaman pengguna juga akan sangat dipengaruhi oleh latensi server Google,

Layanan Google Apps	Sambungan 12Kbps	Sambungan 32Kbps	Sambungan 64Kbps	Sambungan 128Kbps +
Gmail	2 menit untuk memuat atau tidak memuat sama sekali	Laman awal 8-20 detik pemuatan penuh > 1 menit	- pemuatan penuh 2 - 5 detik	Lebih baik dari 64kbs
Chat di Gmail	Tidak dapat memuat	> 1 menit untuk memuat jika dimuat	Memuat dalam 4 - 10 detik	Lebih baik dari 64kbs
Dokumen / Spreadsheet (Buka dokumen)	Tidak dapat memuat	- Laman awal 5-20 detik - pemuatan penuh > 1 menit	4 - 10 detik	Lebih baik dari 64kbs
Dokumen / Spreadsheet (pengeditan kolaboratif)	Tidak dapat memuat	Terasa lebih lambat untuk menampilkan hasil edit dibandingkan dengan 64K	Perubahan tampil cukup cepat untuk menirukan percakapan, yaitu waktu nyata	Lebih baik dari 64kbs
Pengeditan situs	Tidak diuji	Tidak diuji	Laman teks dimuat dalam 3 - 5 detik, Editor memuat Gambar yang sama untuk file jpeg berukuran 385KB membutuhkan waktu ~1 menit	Laman teks dimuat dalam 2 - 4 detik. Editor memuat Gambar yang sama untuk file jpeg berukuran 385KB membutuhkan waktu ~25 detik
Slide			Kecepatan 4 - 10 detik hanya cukup untuk pengeditan	lebih baik dari 64kbps
Hangouts	T/A	T/A	Khusus Audio : 35kbps unggah/ unduh	Video : mulai pada 150kbps untuk unggahan / 500kbps untuk unduhan hingga kecepatan ideal = 1 Mbps unggah/unduh
Drive			4 - 8 detik Kecepatan hanya cukup untuk memuat daftar file/folder di Drive drive	lebih baik dari 64kbps
Youtube				500kbps dan lebih besar
Chromebook & Tablet				200kbps sampai 512kbps disarankan per pengguna secara serentak Tablet

Panduan deployment

Untuk Elemen jaringan akses yang tidak dibahas di dokumen Google "praktik terbaik jaringan untuk deployment skala besar", tabel di bawah ini akan memandu Anda dalam membangun jaringan berskala kecil, menengah, dan besar.

Area akses	Jaringan kecil	Jaringan medium	Jaringan besar
	Melayani < 500 pengguna secara serentak - Total pengguna hingga 2000 - 1 atau 2 bangunan - < 1000 meter persegi	Melayani 500 - 2000 pengguna secara serentak - Total pengguna 2Rb -> 10Rb - 3 sampai 15 bangunan - Satu kampus	Melayani 2000 - 5000 pengguna secara serentak - Total pengguna 10Rb -> 50Rb - 16 sampai 100 bangunan - Beberapa kampus
Bandwidth di kampus (tidak termasuk redundansi) 64kbps, 128kbps, atau 512kbps per pengguna secara serentak	Terendah = 32 Mbps Sedang = 64 Mbps Tinggi = 256 Mbps	Terendah = 32 Mbps Sedang = 256 Mbps Tinggi = 1 Gbps	Terendah = 320 Mbps Sedang = 640 Mbps Tinggi = 2.5 Gbps
Firewall	Jika Anda tidak masalah dengan tidak menggunakan kontrol firewall L7 yang granular (rinci), maka Anda dapat menggunakan router ACL untuk perintah menolak / menerima sederhana. Atau belilah firewall kecil yang sesuai (lihat ukurannya di kotak utama jaringan)."	Jika Anda tidak masalah dengan tidak menggunakan kontrol firewall L7 yang granular (rinci), maka Anda dapat menggunakan router ACL untuk perintah menolak / menerima sederhana. Atau belilah firewall kecil yang sesuai (lihat ukurannya di kotak utama jaringan)."	Biasanya Anda membutuhkan firewall berukuran besar, yang sesuai untuk - Kapasitas jaringan - Sambungan per detik - Sambungan secara serentak - Paket per detik - throughput VPN (jika diperlukan) - throughput IPS (jika diperlukan) - berbagai metrik kapasitas lainnya
LAN : Router	Pilih router yang memiliki kapasitas (CPU, Memori, Backplane...) untuk: - merutekan kecepatan tautan Anda - Memiliki variasi antarmuka yang akan digunakan sekarang dan dalam waktu dekat (T3/E3, GbE Copper atau Fiber (SFP)	Pilih router yang memiliki kapasitas (CPU, Memori, Backplane...) untuk: - merutekan kecepatan tautan Anda - Memiliki variasi antarmuka yang akan digunakan sekarang dan dalam waktu dekat (T3/E3, GbE Copper atau Fiber (SFP)	Pilih router yang memiliki kapasitas (CPU, Memori, Backplane...) untuk: - merutekan kecepatan tautan Anda - Memiliki variasi antarmuka yang akan digunakan sekarang dan dalam waktu dekat (GbE Tembaga atau Fiber (SFP)
LAN : Sakelar	Pertimbangkan elemen berikut dalam artikel ini saat memilih bahan sakelar	Pertimbangkan elemen berikut dalam artikel ini saat memilih bahan sakelar	Pertimbangkan elemen berikut dalam artikel ini saat memilih bahan sakelar
LAN : VLANS	Untuk mengurangi ukuran domain-domain broadcast Anda sebaiknya gunakan VLAN (lihat artikel & tutorial mudah) pemberian tag VLAN juga dapat diterapkan pada lalu lintas nirkabel selama AP dan pengontrol nirkabel mendukungnya. Selain itu, setiap SSID disarankan memiliki VLAN sendiri.	Untuk mengurangi ukuran domain-domain broadcast Anda sebaiknya gunakan VLAN (lihat artikel & tutorial mudah) pemberian tag VLAN juga dapat diterapkan pada lalu lintas nirkabel selama AP dan pengontrol nirkabel mendukungnya. Selain itu, setiap SSID disarankan memiliki VLAN sendiri.	Untuk mengurangi ukuran domain-domain broadcast Anda sebaiknya gunakan VLAN (lihat artikel & tutorial mudah) pemberian tag VLAN juga dapat diterapkan pada lalu lintas nirkabel selama AP dan pengontrol nirkabel mendukungnya. Selain itu, setiap SSID disarankan memiliki VLAN sendiri.

berlanjut

Area akses	Jaringan kecil	Jaringan medium	Jaringan besar
LAN : Port kabel	Pertimbangkan apakah port jaringan kabel dibutuhkan dan di area mana Berapa banyak port per area untuk pengguna dan berapa banyak untuk AP dan perangkat lainnya Pemasangan kabel - setidaknya CAT 5 (hingga 100Mbps)	Pertimbangkan apakah port jaringan kabel dibutuhkan dan di area mana Berapa banyak port per area untuk pengguna dan berapa banyak untuk AP dan perangkat lainnya Pemasangan kabel - setidaknya CAT 5e. Pertimbangkan fiber jika jarak antara node > 100m (hingga 1Gbps)	Pertimbangkan apakah port jaringan kabel dibutuhkan dan di area mana Berapa banyak port per area untuk pengguna dan berapa banyak untuk AP dan perangkat lainnya Pemasangan kabel - setidaknya CAT 6. Gunakan fiber untuk menghubungkan kampus (hingga 10Gbps)
LAN : WiFi : perancangan radio AP	Perancangan radio sangat penting untuk keberhasilan deployment WiFi. Rancangan menggunakan multi radio - 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n & ac) Sebaiknya gunakan radio 5Ghz bila pemasangan lebih besar karena memiliki lebih banyak saluran untuk pemisahan saluran sehingga dapat mendukung lebih banyak radio AP dan pengguna Langkah-langkah perancangan dasar direferensikan dalam artikel ini Untuk semua kasus, sebaiknya gunakan alat perancangan, kemungkinan besar akan disediakan oleh vendor perlengkapan Anda	Perancangan radio sangat penting untuk keberhasilan deployment WiFi. Rancangan menggunakan multi radio - 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n & ac) Sebaiknya gunakan radio 5Ghz bila pemasangan lebih besar karena memiliki lebih banyak saluran untuk pemisahan saluran sehingga dapat mendukung lebih banyak radio AP dan pengguna Langkah-langkah perancangan dasar direferensikan dalam artikel ini Untuk semua kasus, sebaiknya gunakan alat perancangan, yang sebagian besar disediakan oleh vendor perlengkapan Anda	Perancangan radio sangat penting untuk keberhasilan deployment WiFi. Rancangan menggunakan multi radio - 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n & ac) Sebaiknya gunakan radio 5Ghz bila pemasangan lebih besar karena memiliki lebih banyak saluran untuk pemisahan saluran sehingga dapat mendukung lebih banyak radio AP dan pengguna Langkah-langkah perancangan dasar direferensikan dalam artikel ini Untuk semua kasus sebaiknya gunakan alat perancangan, yang sebagian besar disediakan oleh vendor perlengkapan Anda
LAN : WiFi : Daya AP	Pertimbangkan Power over Ethernet (PoE) untuk mengaktifkan AP dan perangkat lainnya. Dengan begitu, Anda tidak perlu memiliki saluran/port daya terpisah untuk setiap AP, telepon IP, kamera, dll. PoE: 15.4 W per port. Dapat mengaktifkan AP. Biasanya daya tidak cukup untuk mengaktifkan kamera atau telepon IP. PoE+: 25.5 W per port. Lebih mahal, namun dapat mengaktifkan telepon, kamera, dan perangkat lainnya. * Perhatikan bahwa sakelar LAN Anda harus mendukung standar PoE yang dipilih. Tidak semua port sakelar mendukung PoE. Anda dapat menggabungkan sakelar dari kedua standar yang menghantarkan daya berbeda untuk area tertentu.	Pertimbangkan Power over Ethernet (PoE) untuk mengaktifkan AP dan perangkat lainnya. Dengan begitu, Anda tidak perlu memiliki saluran/port daya terpisah untuk setiap AP, telepon IP, kamera, dll. PoE: 15.4 W per port. Dapat mengaktifkan AP. Biasanya daya tidak cukup untuk mengaktifkan kamera atau telepon IP. PoE+: 25.5 W per port. Lebih mahal, namun dapat mengaktifkan telepon, kamera, dan perangkat lainnya. * Perhatikan bahwa sakelar LAN Anda harus mendukung standar PoE yang dipilih. Tidak semua port sakelar mendukung PoE. Anda dapat menggabungkan sakelar dari kedua standar yang menghantarkan daya berbeda untuk area tertentu.	Pertimbangkan Power over Ethernet (PoE) untuk mengaktifkan AP dan perangkat lainnya. Dengan begitu, Anda tidak perlu memiliki saluran/port daya terpisah untuk setiap AP, telepon IP, kamera, dll. PoE: 15.4 W per port. Dapat mengaktifkan AP. Biasanya daya tidak cukup untuk mengaktifkan kamera atau telepon IP. PoE+: 25.5 W per port. Lebih mahal, namun dapat mengaktifkan telepon, kamera, dan perangkat lainnya. * Perhatikan bahwa sakelar LAN Anda harus mendukung standar PoE yang dipilih. Tidak semua port sakelar mendukung PoE. Anda dapat menggabungkan sakelar dari kedua standar yang menghantarkan daya berbeda untuk area tertentu.

berlanjut

Area akses	Jaringan kecil	Jaringan medium	Jaringan besar
LAN : Pengontrol Akses WiFi	Untuk jaringan yang sangat kecil dengan titik akses < 10 Anda dapat membangun tanpa pengontrol akses Jika menggunakan pengontrol akses, Anda memiliki pilihan antara - Pengontrol SW yang dapat dipasang di PC (misal: ubiquiti Unifi) - Perangkat (misal: Rukus, model CCR Mikrotik) - Pengontrol awan (misal: Meraki) Untuk semua kasus, hanya gunakan pengontrol akses yang dibuat dan cocok dengan penyedia AP Anda. Selain itu, apabila Anda memiliki jaringan hibrida dengan dua atau beberapa jenis AP berbeda yang dikelola oleh dua atau beberapa pengontrol akses PASTIKAN Anda menyertakan 1 kumpulan AP dan pengontrol akses terkait ke ruang yang terpisah yang berdampingan. JANGAN gabungkan AP dan fungsionalitas pengontrol dalam ruang fisik yang sama karena ini akan meniadakan kemampuan / efektivitas pengontrol	Untuk ukuran jaringan ini, Anda harus memiliki lebih dari 10 AP sehingga sebaiknya Anda memiliki pengontrol akses yang cocok dengan merek AP yang diterapkan. Anda memiliki pilihan di antara - Pengontrol SW yang dapat dipasang di PC (misal: ubiquiti Unifi) - Peralatan (misal: Rukus) - Pengontrol awan (misalnya Meraki) Untuk semua kasus, hanya gunakan pengontrol akses yang dibuat oleh dan cocok dengan penyedia AP Anda. Selain itu, jika Anda memiliki jaringan hibrida dengan dua atau beberapa jenis AP berbeda yang dikelola oleh dua atau beberapa pengontrol AP, PASTIKAN Anda menyertakan 1 rangkaian AP dan dan pengontrol akses terkait ke ruang yang terpisah yang berdampingan. JANGAN gabungkan AP dan fungsionalitas pengontrol dalam ruang fisik yang sama karena ini akan meniadakan kemampuan / efektivitas pengontrol	Secara virtual, Anda harus memiliki pengontrol akses yang cocok dengan merek AP yang diterapkan. Anda memiliki pilihan di antara - Pengontrol SW yang dapat dipasang di PC (misal: ubiquiti Unifi) - Peralatan (misal: Rukus) - Pengontrol awan (misalnya Meraki) Untuk semua kasus, hanya gunakan pengontrol akses yang dibuat oleh dan cocok dengan penyedia AP Anda. Selain itu, apabila Anda memiliki jaringan hibrida dengan dua atau beberapa jenis AP berbeda yang dikelola oleh dua atau beberapa pengontrol akses PASTIKAN Anda menyertakan 1 kumpulan AP dan pengontrol akses terkait ke ruang yang terpisah yang berdampingan. JANGAN gabungkan AP dan fungsionalitas pengontrol dalam ruang fisik yang sama karena ini akan meniadakan kemampuan / efektivitas pengontrol

berlanjut

Area akses	Jaringan kecil	Jaringan medium	Jaringan besar
DHCP LAN	Gunakan server DHCP di jaringan Anda untuk menetapkan alamat IP dinamis ke setiap perangkat. Sebagian besar router dan sakelar telah memiliki server DHCP yang terintegrasi. Jika belum memiliki server DHCP, Anda dapat menggunakan server DHCP di komputer Linux (dhcpd). Tetapkan IP dinamis kepada klien (desktop, laptop, perangkat seluler, dll.) namun tetapkan alamat IP statis untuk server dan router. Pertahankan rentang alamat IP di luar rentang DHCP untuk kasus tersebut. Atur konfigurasi DHCP sehingga rentang alamat IP yang dapat dikeluarkan cukup besar untuk mendukung semua klien dalam jaringan saat ini + tamu + perkembangan selanjutnya. Sebaiknya konfigurasi rentang IP yang berbeda untuk klien kabel dan nirkabel.	Gunakan server DHCP di jaringan Anda untuk menetapkan alamat IP dinamis ke setiap perangkat. Sebagian besar router dan sakelar telah memiliki server DHCP yang terintegrasi. Jika belum memiliki server DHCP, Anda dapat menggunakan server DHCP di komputer Linux (dhcpd). Tetapkan IP dinamis kepada klien (desktop, laptop, perangkat seluler, dll.) namun tetapkan alamat IP statis kepada server dan router. Pertahankan rentang alamat IP di luar rentang DHCP untuk kasus tersebut. Atur konfigurasi DHCP sehingga rentang alamat IP yang dapat dikeluarkan cukup besar untuk mendukung semua klien dalam jaringan saat ini + tamu + perkembangan selanjutnya. Sebaiknya konfigurasi rentang IP yang berbeda untuk klien kabel dan nirkabel. Anda juga dapat mengkonfigurasi berbagai rentang berbeda untuk setiap subjaringan. Untuk jaringan medium Anda dapat memiliki redundansi DHCP.	Gunakan server DHCP di jaringan Anda untuk menetapkan alamat IP dinamis ke setiap perangkat. Sebagian besar router dan sakelar telah memiliki server DHCP yang terintegrasi. Jika belum memiliki server DHCP, Anda dapat menggunakan server DHCP di komputer Linux (dhcpd). Tetapkan IP dinamis kepada klien (desktop, laptop, perangkat seluler, dll.) namun tetapkan alamat IP statis kepada server dan router. Pertahankan rentang alamat IP di luar rentang DHCP untuk kasus tersebut. Atur konfigurasi DHCP sehingga rentang alamat IP yang dapat dikeluarkan cukup besar untuk mendukung semua klien dalam jaringan saat ini + tamu + perkembangan selanjutnya. Sebaiknya konfigurasi rentang IP yang berbeda untuk klien kabel dan nirkabel. Anda juga dapat mengkonfigurasi berbagai rentang berbeda untuk setiap subjaringan. Untuk jaringan besar Anda harus memiliki redundansi DHCP. Jika Anda memiliki banyak tamu, Anda dapat mengurangi waktu penggunaan.
LAN : DNS	Kecuali Anda memiliki perangkat < 5 (komputer, Sakelar, router, AP ....) pada jaringan, Anda menentukan DNS internal untuk menentukan nama komputer. Sebagian besar server DHCP juga memiliki server DNS yang memudahkan konfigurasi untuk menentukan IP statis dan dinamis pada jaringan internal Untuk resolusi nama Eksternal (misal: www.google.com) Anda harus menggunakan DNS ISP atau DNS publik Google berdasarkan dokumen ini Jika mungkin, Anda harus memiliki beberapa server DNS (bersifat redundan) untuk menghindari masalah resolusi nama yang membuat jaringan Anda seolah-olah tidak beroperasi untuk pengguna	Anda membutuhkan DNS internal untuk menentukan nama komputer. Sebagian besar server DHCP juga memiliki server DNS yang memudahkan konfigurasi untuk menentukan IP statis dan dinamis pada jaringan internal Untuk resolusi nama Eksternal (misal: www.google.com) Anda harus menggunakan DNS ISP atau DNS publik Google berdasarkan dokumen ini Pastikan Anda memiliki beberapa server DNS (bersifat redundan) untuk menghindari masalah resolusi nama yang membuat jaringan Anda seolah-olah tidak beroperasi untuk pengguna	Anda membutuhkan DNS internal untuk menentukan nama komputer. Sebagian besar server DHCP juga memiliki server DNS yang memudahkan konfigurasi untuk menentukan IP statis dan dinamis pada jaringan internal Untuk resolusi nama Eksternal (misal: www.google.com) Anda harus menggunakan DNS ISP atau DNS publik Google berdasarkan dokumen ini Pastikan Anda memiliki beberapa server DNS (bersifat redundan) untuk menghindari masalah resolusi nama yang membuat jaringan Anda seolah-olah tidak beroperasi untuk pengguna

berlanjut

Area akses	Jaringan kecil	Jaringan medium	Jaringan besar
Perangkat lunak Pengelolaan Jaringan & SW pemantauan	Sebuah software dengan program manajemen jaringan akan membantu Anda mengelola dari satu titik, seringkali dengan GUI. Lihat checklist alat pengelolaan jaringan di artikel ini untuk pertimbangan. Saat mengevaluasi alat tersebut, pertimbangkan perangkat mana dan jumlah perangkat yang dapat Anda kelola. Spiceworks (gratis) OpenNMS Cacti MRTG GFI (gratis) Saat memilih software manajemen jaringan, periksa fitur mana yang tersedia secara gratis dan berbayar. Selain itu, periksa juga apakah ada versi yang tersedia untuk platform Anda. Sebagian besar solusi manajemen jaringan juga memiliki fungsi pemantauan. Namun Anda juga dapat menemukan software pemantauan jaringan mandiri seperti Solarwinds (uji coba gratis)	Untuk jaringan medium dan besar dapat menggunakan sebuah software dengan program manajemen dan pemantauan jaringan yang sama. Perhatikan bahwa lisensi untuk beberapa solusi berbayar ini didasarkan pada jumlah perangkat yang dikelola/dipantau. Jadi, semakin besar jaringan, semakin mahal lisensi perangkat lunaknya.	Untuk jaringan medium dan besar dapat menggunakan sebuah software dengan program manajemen dan pemantauan jaringan yang sama. Perhatikan bahwa lisensi untuk beberapa solusi berbayar ini didasarkan pada jumlah perangkat yang dikelola/dipantau. Jadi, semakin besar jaringan, semakin mahal lisensi perangkat lunaknya.
Pemfilteran konten	Dalam institusi pendidikan, pemfilteran konten merupakan hal yang harus dilakukan. Hal ini dilakukan untuk memastikan bahwa Anda dapat memblokir konten pornografi, tidak terlanggar hak ciptanya karena orang-orang menggunakan torrent untuk mengunduh SW dan film, san untuk mengoptimalkan bandwidth bandwidth. Contoh filter web open source adalah squidproxy Jika Anda menggunakan filter web open source, atau proxy / filter komersial pertimbangkan hal berikut: 1) Penggunaan proxy transparan sehingga tidak perlu mengonfigurasi proxy di semua klien 2) Pastikan proxy dapat mengatasi semua lalu lintas internet yang melintasinya jika tidak ingin lalu lintas tersumbat. 3) Pertimbangkan redundansi atau virtualisasi mesin sehingga proxy bukan satu-satunya penyebab kegagalan.	Dalam institusi pendidikan, pemfilteran konten merupakan hal yang harus dilakukan. Hal ini dilakukan untuk memastikan bahwa Anda dapat memblokir konten pornografi, tidak terlanggar hak ciptanya karena orang-orang menggunakan torrent untuk mengunduh SW dan film, san untuk mengoptimalkan bandwidth bandwidth. Contoh filter web open source adalah squidproxy Jika Anda menggunakan filter web open source, atau proxy / filter komersial pertimbangkan hal berikut: 1) Penggunaan proxy transparan sehingga tidak perlu mengonfigurasi proxy di semua klien 2) Pastikan proxy dapat mengatasi semua lalu lintas internet yang melintasinya jika tidak ingin lalu lintas tersumbat. 3) Pertimbangkan redundansi atau virtualisasi mesin sehingga proxy bukan satu-satunya penyebab kegagalan.	Dalam institusi pendidikan, pemfilteran konten merupakan hal yang harus dilakukan. Hal ini dilakukan untuk memastikan bahwa Anda dapat memblokir konten pornografi, tidak terlanggar hak ciptanya karena orang-orang menggunakan torrent untuk mengunduh SW dan film, san untuk mengoptimalkan bandwidth bandwidth. Contoh filter web open source adalah squidproxy Jika Anda menggunakan filter web open source, atau proxy / filter komersial pertimbangkan hal berikut: 1) Penggunaan proxy transparan sehingga tidak perlu mengonfigurasi proxy di semua klien 2) Pastikan proxy dapat mengatasi semua lalu lintas internet yang melintasinya jika tidak ingin lalu lintas tersumbat. 3) Pertimbangkan redundansi atau virtualisasi mesin sehingga proxy bukan satu-satunya penyebab kegagalan.

berlanjut

Area akses	Jaringan kecil	Jaringan medium	Jaringan besar
Kontrol akses / Keamanan : Radius / SSO	Akses ke jaringan Anda, khususnya WiFi, harus dikontrol. Hal ini dapat dilakukan dengan menggunakan server radius dan mengonfigurasi AP WiFi agar menggunakan infrastruktur AAA Radius Anda untuk autentikasi dan akuntabilitas Agar dapat menggunakan kredensial Google untuk akses WiFi (disarankan) Anda harus mengalihkan autentikasi WiFi ke portal penahan yang mengalihkan ke proses masuk Google yang mendukung Oauth melalui layanan seperti Cloudessa	Akses ke jaringan Anda, khususnya WiFi, harus dikontrol. Hal ini dapat dilakukan dengan menggunakan server radius dan mengonfigurasi AP WiFi agar menggunakan infrastruktur AAA Radius Anda untuk autentikasi dan akuntabilitas Agar dapat menggunakan kredensial Google untuk akses WiFi (disarankan) Anda harus mengalihkan autentikasi WiFi ke portal penahan yang mengalihkan ke proses masuk Google yang mendukung Oauth melalui layanan seperti Cloudessa	Akses ke jaringan Anda, khususnya WiFi, harus dikontrol. Hal ini dapat dilakukan dengan menggunakan server radius dan mengonfigurasi AP WiFi agar menggunakan infrastruktur AAA Radius Anda untuk autentikasi dan akuntabilitas Agar dapat menggunakan kredensial Google untuk akses WiFi (disarankan) Anda harus mengalihkan autentikasi WiFi ke portal penahan yang mengalihkan ke proses masuk Google yang mendukung Oauth melalui layanan seperti Cloudessa

Dokumen perancangan radio yang sangat detail (Ini adalah dokumen berukuran besar yang dapat digunakan untuk topik referensi bila diperlukan)

Solusi

Tautan di bawah ini disediakan SEBAGAIMANA ADANYA dan Google tidak menjamin atau menyarankan solusi pihak ketiga daripada solusi yang lain. Keputusan mengenai solusi yang paling memenuhi kebutuhan institusi diserahkan kepada institusi.

1. Bandwidth di kampus (termasuk redundansi) , sambungan WAN, dan link intrakampus
   a. Ini semua akan disediakan oleh ISP / perusahaan telekomunikasi lokal.

2. Firewall
   a. Checkpoint
   b. McAFee
   c. Juniper
   d. Cisco
   e. Barracuda
   f. MicroTik
   g. Fortinet - fortigate

3. LAN : Router, Sakelar
   a. Cisco
   b. Dell
   c. HP
   d. Juniper
   e. Brocade
   f. Netgear
   g. Huawei
   h. ZyXel
   i. Frotinet
   j. MicroTik (papan router)
   k. Dlink

4. LAN : WiFi (termasuk pengontrol akses)
   a. Cisco
   b. Ubiquiti
   c. Dell
   d. HP
   e. Juniper
   f. Huawei
   g. ZyXel
   h. MicroTik (Papan router)
   i. DLink
   j. Fortinet
   k. Aruba
   l. Ruckus
   m. Aerohive
   n. Meru
   o. Xirrus (Berkinerja Tinggi)

5. DHCP & DNS
   Sebagian besar produk Sakelar di atas juga memiliki opsi server DHCP / DNS bawaan atau mandiri. Hal lainnya yang perlu dipertimbangkan:

   a. ISC.org
   b. Solarwinds

6. Software Manajemen & Pemantauan Jaringan
   Sebagian besar produk Sakelar di atas juga memiliki platform Software Manajemen dan pemantauan dan biasanya Anda akan menggunakan SW produsen yang sama untuk mengelola perangkat kerasnya, meskipun ada beberapa solusi SNMP umum

   a. MRTG (pemantauan SNMP) (Gratis)
   b. Nagios (Pemantauan umum)
   c. CACTI
   d. Spiceworks (Gratis)
   e. OpenNMS
   f. GFI (Gratis)
   g. Brocade
   h. Cisco
   i. Juniper
   j. HP
   k. Dell
   l. Huawei
   m. Ubiquiti
   n. Fortinet

7. Pemfilteran konten
   a. Squid proxy (Gratis)
   b. Cisco
   c. Barracuda
   d. Fortinet
   e. MicroTik
   f. Checkpoint
   g. Mcafee

8. Kontrol akses / Keamanan (SSO, RADIUS)
   a. Freeradius (Gratis)
   b. Zeroshell (Gratis)
   c. Cloudessa (Berbasis awan)
   d. Clearbox
   e. Server radius Microsoft
   f. Aradial

Mengembangkan action plan

1. Buat cakupan ukuran jaringan
   a. Rencanakan jangka waktu untuk jaringan ini (1, 2, 3, 4, 5 ...10 tahun)
   b. Jumlah total pengguna dan perangkat
   c. Jumlah pengguna secara serentak, perhitungkan waktu penggunaan ringan dan puncak
   d. % pengguna kabel dan nirkabel
   e. jenis aplikasi lainnya selain layanan berbasis awan yang akan dijalankan di jaringan Anda
   f. Diskusikan dan putuskan masalah kebijakan, pemfilteran konten, siapa saja yang memiliki akses dan kapan
2. Rencanakan elemen jaringan yang akan Anda tambahkan / tingkatkan untuk memenuhi persyaratan cakupan
3. Dapatkan dukungan interna untuk cakupan dan rencana
4. Dapatkan RFP dari vendor (Gunakan proses ini untuk mendidik diri Anda tentang beberapa solusi yang tersedia)
5. Pilih dari pengiriman RFP Vendor
6. Tinjauan pemangku kepentingan terhadap Solusi yang dipilih dan persetujuan pembelian
7. Buat purchase order
8. Sediakan peralatan dan laksanakan deployment (termasuk majemen perubahan jika berlaku)
9. Uji deployment
10. Perbaiki semua masalah
11. Luncurkan

WP2051-1408