



# Сегментация сети в условиях цифровой трансформации

Июнь 2018

[www.risk.az](http://www.risk.az)

# Содержание

Основные цели сегментации сети .....	3
Пример плоской сети и её недостатки .....	4
Сбор информации о текущей инфраструктуре и сервисах .....	6
Анализ собранных данных, логическое сегментирование (разделение на функциональные группы) и подготовка политики доступов .....	7
Проектирование сети с учётом новых требований сегментированной сети .....	14
Фазовая имплементация и документация .....	15

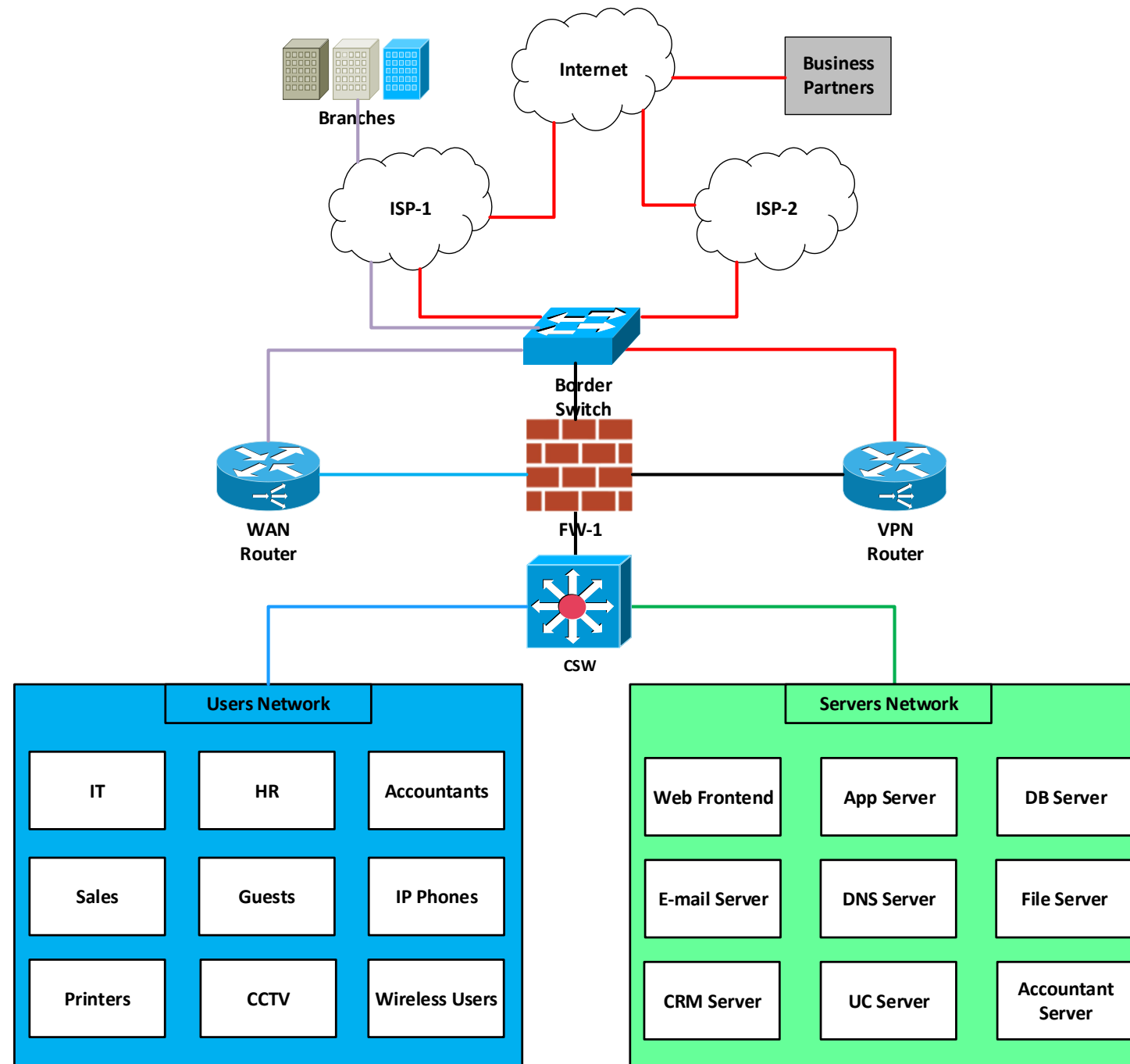
# Основные цели

3

- ✓ Снижение риска компрометации всей сети при компрометации одного хоста
- ✓ Разделение участников сети на функциональные группы
- ✓ Создание возможности применения различных политик безопасности к различным функциональным группам
- ✓ Контроль и видение сети
- ✓ Создание условий для самой сети реагировать на угрозы и изолировать скомпрометированные системы

# Пример плоской сети

4



# Недостатки плоской сети

5

- ✘ Риск компрометации других систем при компрометации одной
- ✘ Отсутствие видения сети (логирования соединений, попыток несанкционированного доступа к ресурсам, распространения вредоносных файлов между сегментами сети и т.д.)
- ✘ Возможность сканирования сети «любопытными» пользователями или злоумышленниками

# Сбор информации о текущей инфраструктуре и сервисах

6

Для сбора информации о сервисах целесообразно воспользоваться порт-сканерами (при условии, что на сканируемых системах временно отключены ПО, блокирующие трафик с хостов, заподозренных в сканировании)

# Таблица хостов и сервисов

7

NETWORK INFRASTRUCTURE DEVICE	SERVICES
Access-Switch-1	tcp/23(telnet), tcp/80(http)
CSW	tcp/22(ssh), tcp/23(telnet), tcp/80(http)
WAN Router	tcp/22(ssh), tcp/23(telnet), tcp/80(http)
VPN Router	tcp/22(ssh), tcp/23(telnet), tcp/80(http)
FW-1	tcp/22(ssh),tcp/443(https),udp/161(snmp)
FW-2	tcp/22(ssh),tcp/443(https),udp/161(snmp)
SERVER	SERVICES
DC Server	tcp/udp/53(dns),tcp/udp/88(kerberos), tcp/udp/389(ldap), tcp/udp/3268(ldap gc)
File Server	tcp/21(ftp), tcp/445(smb)
Web Frontend Server	tcp/80(http), tcp/443(https)
Web Backend Server	tcp/8080, tcp/8443
DB Server	tcp/3306(sql)
E-mail Server	tcp/25(smtp), tcp/110(pop, tcp/143(imap4)
HR Server	tcp/443(https), tcp/8448(https)
Accountants Server	tcp/80(http), tcp/443(https)
CRM Server	tcp/80(http), tcp/443(https)

# Разделение на группы

8

INSIDE USERS/ENDPOINTS		
GROUP NAME	VLAN ID	SUBNET/MASK
IT administrators	10	172.16.10.0/24
HR	11	172.16.11.0/24
Accountants	12	172.16.12.0/24
Sales	13	172.16.13.0/24
Executives	14	172.16.14.0/24
IP Phones	15	172.16.15.0/24
CCTV	16	172.16.16.0/24
Guests	50	192.168.50.0/24
Branch-1 Users	10 (local in Branch-1)	172.31.10.0/24
Branch-1 IP Phones	11 (local in Branch-1)	172.31.11.0/24
Branch-1 CCTV	12 (local in Branch-1)	172.31.12.0/24
Branch-2 Users	10 (local in Branch-2)	172.31.20.0/24
Branch-2 IP Phones	11 (local in Branch-2)	172.31.21.0/24
Branch-2 CCTV	12 (local in Branch-2)	172.31.22.0/24



# Разделение на группы

9

DATACENTER		
GROUP NAME	VLAN ID	SUBNET/MASK
DVR Servers	16	172.16.16.0/24
Domain Controllers	100	172.16.100.0/24
File Servers	101	172.16.101.0/24
E-mail Servers	102	172.16.102.0/24
HR Servers	103	172.16.103.0/24
Accountants Servers	104	172.16.104.0/24
CRM Servers	105	172.16.105.0/24
Voice Servers	106	172.16.106.0/24
Web Backend Servers	108	172.16.108.0/24
DB Servers	109	172.16.109.0/24
Management	110	172.16.110.0/24

DMZ		
GROUP NAME	VLAN ID	SUBNET/MASK
WAF (outside)	200	172.17.0.0/24
WAF (inside)	201	172.17.1.0/24
Web Frontend Servers	201	172.17.1.0/24
E-mail Proxy	202	172.17.2.0/24
External DNS Server	203	172.17.3.0/24

# Анализ потенциальных угроз

10

- Сканеры портов/служб
- Протокольные аномалии
- MITM-атаки
- DoS-атаки
- Уязвимости ОС
- Уязвимости приложений
- Malware (вирусы, трояны, черви, т.д.)
- Спам и вредоносные ссылки в письмах
- Посещение вредоносных URL
- Ботнеты

# Оценка критичности

11

## VERY HIGH

Системы и данные, компрометация которых может привести к утечке коммерческих тайн, конкурентных преимуществ, данных о клиентах, нанести непоправимый ущерб репутации компании (DB Server, CRM Server, File Server storing sensitive information)

## HIGH

Системы и данные, компрометация которых может привести к утечке данных о структуре компании, помешать нормальной работе инфраструктуры, привести к простоям (DC Server, E-mail Server, HR Server, etc.)

## NORMAL

Системы и данные, компрометация которых не приводит непосредственно к утечке особо важных данных, но могут служить «трамплином» для последующих атак на эти особо важные сервера (Users, IP Phones, Cameras, etc.)

# Системы защиты

12

- Раздельные внешний (на периметре сети) и внутренний фаервол с функциями контроля приложений, SSL-дешифрации, IPS (с функциями сигнатурного и поведенческого анализа), выявления и блокировки вредоносных файлов
- Система защиты web-трафика с функциями блокировки URL-адресов по категориям и репутации
- Система защиты от спама, вредоносных вложений и ссылок в письме
- Endpoint Protection системы
- Дополнительные системы защиты (WAF, DLP, PAM, DDoS Protection, NAC, Vulnerability Management Systems, etc.)

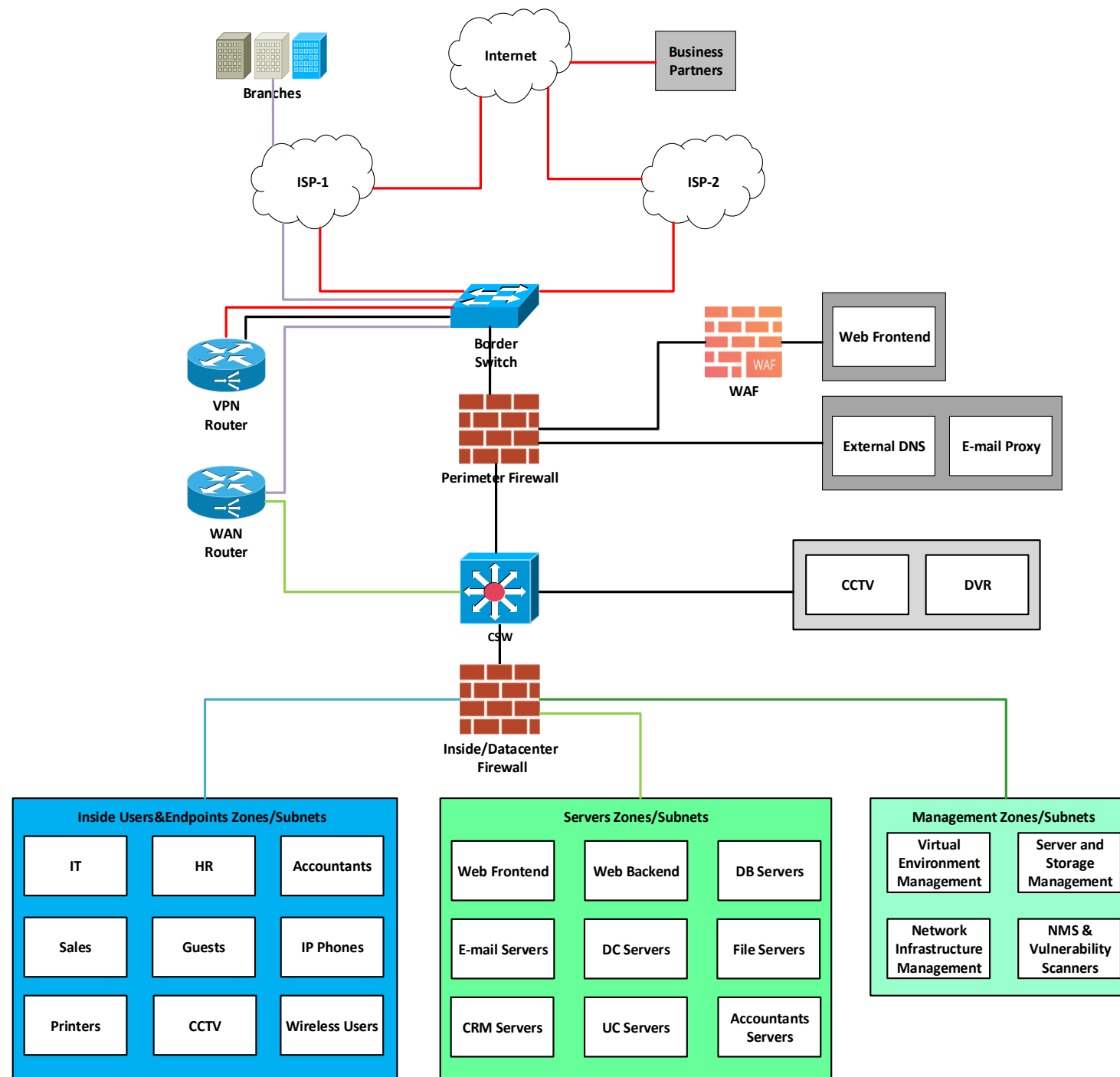
# Матрица доступа

13

	IT ADMINS	SALES	IP PHONES	GUESTS	DC SERVERS	E-MAIL SERVERS	WEB FRONTEND	WEB BACKEND	DB SERVER	UC SERVER	MANAGEMENT	INTERNET
IT ADMINS	Permit: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS), TCP/389(LDAP), TCP/88(Kerberos)	Permit: TCP/25(SMTP), TCP/110(POP), TCP/143(IMAP4)	Permit: TCP/443(HTTPS)	Deny: Any	Deny: Any	Deny: Any	Permit: Any	Permit: Any
SALES	Deny: Any	Permit: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS), TCP/389(LDAP), TCP/88(Kerberos)	Permit: TCP/25(SMTP), TCP/110(POP), TCP/143(IMAP4)	Permit: TCP/443(HTTPS)	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: Any
IP PHONES	Deny: Any	Deny: Any	Permit: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/69(TFTP), TCP/5060(SIP),	Deny: Any	Deny: Any
GUESTS	Deny: Any	Deny: Any	Deny: Any	Permit: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: Any
DC SERVERS	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: Any	Permit: TCP/25(SMTP), TCP/110(POP), TCP/143(IMAP4)	Permit: TCP/443(HTTPS)	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: Any
E-MAIL SERVERS	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS)	Permit: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any
WEB FRONTEND	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS)	Deny: Any	Permit: Any	Permit: TCP/8080, TCP/8443	Deny: Any	Deny: Any	Deny: Any	Permit: Any
WEB BACKEND	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS)	Deny: Any	Deny: Any	Permit: Any	Permit: TCP/3306(SQL)	Deny: Any	Deny: Any	Deny: Any
DB SERVER	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: Any	Deny: Any	Deny: Any	Deny: Any
UC SERVER	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS)	Permit: TCP/25(SMTP)	Deny: Any	Deny: Any	Deny: Any	Permit: Any	Deny: Any	Permit: Any
MANAGEMENT	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: UDP/53(DNS)	Permit: TCP/25(SMTP)	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: Any	Deny: Any
INTERNET	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Deny: Any	Permit: TCP/443(HTTPS)	Deny: Any	Deny: Any	Deny: Any	Deny: Any	

# Проектирование сети

14



# Фазовая имплементация и документация

15

- Рекомендуется заранее создать зоны на фаерволах и настроить политики доступа между зонами в режиме мониторинга (когда политики доступа не влияют на трафик, но логируют соединения)
- Поэтапный перевод систем в новые зоны (подсети)
- Фазовая имплементация IPS и File-Control политик в режиме мониторинга с последующим тюнингом IPS-политик под конкретные системы
- Документация каждой стадии внедрения



Спасибо за внимание!

ул. Рашида Бехбудова 59,  
AZ1022, Баку, Азербайджан

+99412 4973737  
+99412 4981993 (Факс)

[www.risk.az](http://www.risk.az)