Отчет о тестировании ЛВС АКБ

Исполнитель:

Ифатов Д.С/

Москва 2004

# Содержание

Содержание

1. Введение

2. Методика мониторинга и критерии оценки

2.1 Методика тестирования

2.2 Критерии оценки

3. Сбор информации об объекте

3.1 Информация о топологии сети

3.2 Суточная загрузка интерфейсов центрального коммутатора

3.3 Распределение трафика по протоколам

4. Сервера

ADMIRAL

BREEZE

CRUISER

Captain

Boatsman

Exchserv

Concord

Main2K

Backup

Nterm

Ntserver

Proxy\_cs

Skipper

Результаты сканирования на уязвимость

5. Выводы

5.1 Состояние сетевой инфраструктуры

5.2 Состояние серверов

5.3 Состояние безопасности

5.4 Общая оценка

Приложение 1

Отчет для руководителя

Отчет по состоянию сервера ADMIRAL

Отчет по состоянию сервера BREEZE

Отчет по состоянию сервера CRUISER

Отчет по состоянию сервера Captain

Отчет по состоянию сервера Boatsman

Отчет по состоянию сервера Exchserv

Отчет по состоянию сервера Concord

Отчет по состоянию сервера Main2K

Отчет по состоянию сервера BackUp

Отчет по состоянию сервера Nterm

Отчет по состоянию сервера Ntserver

Отчет по состоянию сервера Proxy\_CS

Отчет по состоянию сети

Приложение 2

Предложения и рекомендации

Предложение по обеспечению защиты периметра сети

Общая схема

Организация почтовой системы

Организация доступа в Интернет

Подключение внешних пользователей к RS-Bank

Symantec AntiVirus for Microsoft Internet Security and Acceleration (ISA) Server

Предложение по организации Exchange сервера

Информация для заказа:

Рекомендации по средствам управления сетью

Комплексное решение

Обеспечение высокой доступности сети и балансировка нагрузки.

Высокоскоростная коммутация пакетов.

Средства безопасности.

Подключение серверов.

1 этап

2 этап

# Введение

Основной задаче данного мониторинга является составление полноценной картины ЛВС АКБ «Банк», выявление узких мест и возможных проблем способных привести к неработоспособности всей сети или ее части, потере критичных для бизнеса заказчика данных. Избежание неоправданных расходов на модернизацию. Выявить причины неудовлетворительной производительности работы сети, анализ антивирусной защиты сети и защищенности от НСД, а также общий анализ топологии и масштабируемости.

При разработке методики мониторинга сети, учитывая то, что основополагающим фактом успешного функционирования сети считалась ее стабильная работа, приоритетной учитывалась политика наименьшего вмешательства в ее работу и работу сетевого оборудования.

# Методика мониторинга и критерии оценки

## 

## Методика тестирования

Для построения карты сети – схемы соединения коммутаторов и рабочих станций, скорость каналов – использовалась программа 3COM Network Director .

С помощью программы MRTG [ http://people.ee.ethz.ch/~oetiker/webtools/mrtg/ ]была снята статистика загруженности портов с корневого коммутатора сети.

Поскольку обе программы используют для получения необходимой информации протокол SNMP, то он был включен на коммутаторе Cisco 3750, на остальных коммутаторах SNMP уже был включен.

Анализ трафика производился с помощью программы Sniffer Pro [ http://www.mcafee.ru/products/sniffer/ ] установленной на компьютере подключенном к порту коммутатора Cisco 3750 настроенного в качестве порта SPAN.

При включении этой технологии пакеты проходящие через выбранные порты дублируются на порт к которому подключен сетевой анализатор.

На серверах были включены счетчики загруженности процессора памяти и жестких дисков.

Внешние IP адреса были просканированы на поиск возможных уязвимостей с помощью программы XSpider [ http://www.ptsecurity.ru/ ] .

## Критерии оценки

Для описания состояния сети был выбран метод пороговых значений суть которого заключается в сравнении каждого измеряемого значения с табличным рекомендуемым значением.

\* Рассчитывается по счетчику Memory: Commited bytes

|  |  |  |  |
| --- | --- | --- | --- |
| п/н | Измеряемый параметр | Критичное значение | Удовлетворительное |
| 1 | Processor: % Processor Time | >75 | <30 |
| 2 | Memory: Available Bytes\* | <4MB | >64MB |
| 3 | Memory: Fault Pages/sec | >120 | <40 |
| 4 | Physical Disk: Avg. Queue Length | >1 | 0 |

По результату сравнения состояние подсистемы признается удовлетворительны, неудовлетворительным или критичным.

Оценка различных компонентов ЛВС будет производится в результате интегральной оценки состояний ее подсистем. Весовые коэффициенты оценки здоровья подсистем будут выбираться в зависимости их значимости для выполняемых задач и критичности этих задач для бизнеса заказчика.

# Сбор информации об объекте

## 

## Информация о топологии сети

Топология локальной сети представлена на рисунке 1.

Карта была построена с помощью программы 3Com Network Director.

<РИС1>



## Суточная загрузка интерфейсов центрального коммутатора

Загрузка портов центрального коммутатора в течении суток.

Загрузка снималась с помощью программы MRTG по протоколу SNMP.

Как видно на графиках ни на одном порту нагрузка не превышает 5% от предельной.

|  |  |
| --- | --- |
| № порта | Суточная загрузка |
| 1 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 312.0 B/ (0.0%) |  | Average In: | 119.0 B/s (0.0%) |  | Current In: | 144.0 B/s (0.0%) | | Max Out: | 66.0 B/s (0.0%) |  | Average Out: | 12.0 B/s (0.0%) |  | Current Out: | 12.0 B/s (0.0%) | |
| 2 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 104.4 kB/s (0.8%) |  | Average In: | 5141.0 B/s (0.0%) |  | Current In: | 17.1 kB/s (0.1%) | | Max Out: | 432.2 kB/s (3.5%) |  | Average Out: | 21.0 kB/s (0.2%) |  | Current Out: | 46.4 kB/s (0.4%) |   Подключена сеть «Частные вклады»  100 MB |
| 3 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 25.1 kB/s (0.2%) |  | Average In: | 422.0 B/s (0.0%) |  | Current In: | 17.0 B/s (0.0%) | | Max Out: | 2865.0 kB/s (22.9%) |  | Average Out: | 79.5 kB/s (0.6%) |  | Current Out: | 374.0 B/s (0.0%) |   Подключен сервер SKIPPER (IP 192.168.2.6)  100MB |
| 4 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 5415.0 kB/s (4.3%) |  | Average In: | 915.9 kB/s (0.7%) |  | Current In: | 1784.3 kB/s (1.4%) | | Max Out: | 3071.7 kB/s (2.5%) |  | Average Out: | 206.0 kB/s (0.2%) |  | Current Out: | 511.6 kB/s (0.4%) |   Подключен сервер CRUISER (IP 192.168.2.18)  1 GB |
| 5 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 3097.5 kB/s (24.8%) |  | Average In: | 80.1 kB/s (0.6%) |  | Current In: | 117.5 kB/s (0.9%) | | Max Out: | 2992.8 kB/s (23.9%) |  | Average Out: | 103.2 kB/s (0.8%) |  | Current Out: | 363.2 kB/s (2.9%) |   Подключен узел 192.168.2.93  100 MB |
| 6 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 21.3 B/s (0.2%) |  | Average In: | 474.0 B/s (0.0%) |  | Current In: | 715.0 B/s (0.0%) | | Max Out: | 45.6 kB/s (0.4%) |  | Average Out: | 1479.0 B/s (0.0%) |  | Current Out: | 2135.0 B/s (0.0%) |   Подключена сеть «Руководство, Секретари»  100 MB |
| 7 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 145.1 kB/s (0.1%) |  | Average In: | 3013.0 B/s (0.0%) |  | Current In: | 327.0 B/s (0.0%) | | Max Out: | 4325.6 kB/s (3.5%) |  | Average Out: | 100.8 kB/s (0.1%) |  | Current Out: | 657.0 B/s (0.0%) | |
| 8 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 109.0 kB/s (0.9%) |  | Average In: | 15.3 kB/s (0.1%) |  | Current In: | 32.1 kB/s (0.3%) | | Max Out: | 354.5 kB/s (2.8%) |  | Average Out: | 43.7 kB/s (0.3%) |  | Current Out: | 64.5 kB/s (0.5%) |   Подключен сервер BREEZE (IP 192.168.2.7)  1 GB |
| 9 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 109.0 kB/s (0.9%) |  | Average In: | 15.3 kB/s (0.1%) |  | Current In: | 32.1 kB/s (0.3%) | | Max Out: | 354.5 kB/s (2.8%) |  | Average Out: | 43.7 kB/s (0.3%) |  | Current Out: | 64.5 kB/s (0.5%) |   Подключена сеть «Оперзал»  100 MB |
| 10 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 37.7 kB/s (0.3%) |  | Average In: | 2462.0 B/s (0.0%) |  | Current In: | 517.0 B/s (0.0%) | | Max Out: | 246.6 kB/s (2.0%) |  | Average Out: | 6284.0 B/s (0.1%) |  | Current Out: | 1743.0 B/s (0.0%) |   Подключена сеть «Казначейство»  100 MB |
| 11 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 13.3 kB/s (1.1%) |  | Average In: | 7965.0 B/s (0.1%) |  | Current In: | 1318.0 B/s (0.0%) | | Max Out: | 4269.9 kB/s (34.2%) |  | Average Out: | 51.3 kB/s (0.4%) |  | Current Out: | 773.0 B/s (0.0%) |   Подключен узел 192.168.2.246  100 MB |
| 12 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 31.5 kB/s (0.3%) |  | Average In: | 2022.0 B/s (0.0%) |  | Current In: | 514.0 B/s (0.0%) | | Max Out: | 244.5 kB/s (2.0%) |  | Average Out: | 11.6 kB/s (0.1%) |  | Current Out: | 1251.0 B/s (0.0%) |   Подключена сеть «Казначейство»  100 MB |
| 13 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 7800.0 kB/s (62.4%) |  | Average In: | 76.9 kB/s (0.6%) |  | Current In: | 15.0 B/s (0.0%) | | Max Out: | 179.3 kB/s (1.4%) |  | Average Out: | 2342.0 B/s (0.0%) |  | Current Out: | 376.0 B/s (0.0%) |   Подключен узел 192.168.2.245  100 MB |
| 14 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 18.1 kB/s (0.1%) |  | Average In: | 270.0 B/s (0.0%) |  | Current In: | 23.0 B/s (0.0%) | | Max Ot: | 13.9 kB/s (0.1%) |  | Average Out: | 410.0 B/s (0.0%) |  | Current Out: | 393.0 B/s (0.0%) |   Подключен узел 192.168.2.157  100 MB |
| 16 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 9408.0 B/s (0.1%) |  | Average In: | 161.0 B/s (0.0%) |  | Current In: | 26.0 B/s (0.0%) | | Max Out: | 6499.0 B/s (0.1%) |  | Average Ot: | 448.0 B/s (0.0%) |  | Current Out: | 409.0 B/s (0.0%) |   Подключена сеть «Bloomberg»  100 MB |
| 17 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 2060.0 B/s (0.2%) |  | Average In: | 623.0 B/s (0.0%) |  | Current In: | 884.0 B/s (0.1%) | | Max Out: | 5273.0 B/s (0.4%) |  | Average Out: | 388.0 B/s (0.0%) |  | Current Ou: | 370.0 B/s (0.0%) | |
| 18 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 165.1 kB/s (1.3%) |  | Average In: | 16.3 kB/s (0.1%) |  | Current In: | 117.4 kB/s (0.9%) | | Max Out: | 711.2 kB/s (5.7%) |  | Average Out: | 53.2 kB/s (0.4%) |  | Current Out: | 610.9 kB/s (4.9%) |   Подключена сеть «Операционный зал., отдел валютного контроля»  100 MB |
| 19 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 43.5 kB/s (0.3%) |  | Average In: | 1121.0 B/s (0.0%) |  | Current In: | 32.0 B/s (0.0%) | | Max Out: | 384.1 kB/s (3.1%) |  | Average Out: | 3040.0 B/s (0.0%) |  | Current Out: | 377.0 B/s (0.0%) |   Подключен узел 192.168.2.15  100 MB |
| 20 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 741.0 B/s (0.1%) |  | Average In: | 115.0 B/s (0.0%) |  | Current In: | 208.0 B/s (0.0%) | | Max Out: | 5093.0 B/s (0.4%) |  | Average Out: | 1124.0 B/s (0.1%) |  | Current Out: | 1639.0 B/s (0.1%) | |
| 21 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 386.0 kB/s (3.1%) |  | Average In: | 3826.0 B/s (0.0%) |  | Current In: | 616.0 B/s (0.0%) | | Max Out: | 179.5 kB/s (1.4%) |  | Average Out: | 9446.0 B/s (0.1%) |  | Current Out: | 7552.0 B/s (0.1%) |   Подключена сеть «Служба автоматизации»  100 MB |
| 22 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 75.9 kB/s (0.6%) |  | Average In: | 4299.0 B/s (0.0%) |  | Current In: | 4386.0 B/s (0.0%) | | Max Out: | 166.9 kB/s (1.3%) |  | Average Out: | 15.5 kB/s (0.1%) |  | Current Out: | 5229.0 B/s (0.0%) |   Подключена сеть «Юридический и Кредитный отделы»  100 MB |
| 24 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 42.2 kB/s (0.3%) |  | Average In: | 1110.0 B/s (0.0%) |  | Current In: | 86.0 B/s (0.0%) | | Max Out: | 186.9 kB/s (1.5%) |  | Average Out: | 4031.0 B/s (0.0%) |  | Current Out: | 527.0 B/s (0.0%) |   Подключена сеть «Bloomberg»  100 MB |
| 25 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In: | 4406.2 kB/s (3.5%) |  | Average In: | 247.0 kB/s (0.2%) |  | Current In: | 140.6 kB/s (0.1%) | | Max Out: | 7805.1 kB/s (6.2%) |  | Average Out: | 618.8 kB/s (0.5%) |  | Current Out: | 365.0 kB/s (0.3%) |   Подключена сеть «Служба атоматизации»  1 GB |
| 26 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Max In | 296.2 kB/s (0.2%) |  | Average In: | 23.0 kB/s (0.0%) |  | Current In: | 101.5 kB/s (0.1%) | | Max Out: | 725.4 kB/s (0.6%) |  | Average Out: | 73.2 kB/s (0.1%) |  | Current Out: | 337.2 kB/s (0.3%) |   Подключена сеть «Бухгалтерия»  1 GB |

## Распределение трафика по протоколам

Диаграммы были построены на основе данных собранных Sniffer в течении рабочего дня и отражают процентное содержание различных протоколов в трафике.

Диаграмма показывает распределение протоколов между IP и IPX.



Процент распределения протоколов внутри IPX. Протокол NCP используется для служебной информации и печати.



Процент распределения протоколов внутри IP.



Из диаграмм можно сделать вывод, что печать занимает около 15%-20% процентов сетевого трафика.

HTTP – около 1 %

Почта – чуть более 0.5%

На графике изброжено отношение широковещательного трафика к общему.

Из графика можно сделать вывод, суммарный широковещательный трафик ничтожен и практически не занимает полосу пропускания.



Графическое изображение потоков трафика в локальной сети по устройствам.

Данные диаграммы построены с помощью программы Sniffer. С их помощью можно определить устройства создающие излишне большой трафик в сети (таких устройств не найдено), так же они позволяют полнее представить общую картину сети.

4. Сервера

## ADMIRAL

### Описание

BackUp сервер для Cruiser.

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | ADMIRAL |
| ОS | Novell NetWare 6.0 |
| Производитель | Астра |
| Процессор |  |
| Память | 512 Кб |
|  |  |
| Контроллер | RAID5 |
| SYS |  |
| Size | 6 GB |
| Free Space | 4 GB |
| SKLAD |  |
| Size | 31 GB |
| Free Space | 6,65 GB |
| BANKIR |  |
| Size | 28,21 GB |
| Free Space | 5,48 GB |

### Загрузка

### Память

Allocated memory pool, In bytes: 276 488 192 52%

Cache buffer memory, In bytes: 133 640 192 25%

Cache movable memory, In bytes: 0 0%

Cache non-movable memory, In bytes: 81 920 0%

Code and data memory, In bytes: 126 199 808 23%

Total server work memory, In bytes: 536 410 112 100%

### Процессор

### Дисковая система

## BREEZE

### 

### Описание

Копия Cruiser

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | BREEZE |
| ОS | Novell NetWare 6.0 |
| Производитель | HP |
| Процессор | Intel Xeon 3.2 GHz |
| Память | 4 GB |
|  |  |
| Контроллер | U320 |
| Drive Model | 6x 72GB 15K U320 HotPlug Universal HDD |

### Загрузка

### Память

Allocated memory pool, In bytes: 1 041 891 328 26%

Cache buffer memory, In bytes: 2 087 510 016 52%

Cache movable memory, In bytes: 0 0%

Cache non-movable memory, In bytes: 86 016 0%

Code and data memory, In bytes: 40 167 323 1%

Miscellaneous memory, In bytes: 822 901 861 21%

Total server work memory, In bytes: 4 293 914 624 100%

## CRUISER

Файловый сервер, RS Bank, сервер баз данных (Pervasiv SQL).

### Описание

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | CRUISER |
| ОS | Novell NetWare 6.0 |
| Производитель | Dell |
| Процессор |  |
| Память | 2 GB |
|  |  |
| Контроллер | RAID 5 |
| SYS |  |
| Size | 5,81 GB |
| Free Space | 1,04 GB |
| WORK |  |
| Size | 25 GB |
| Free Space | 4,16 GB |
| BANK |  |
| Size | 24 GB |
| Free Space | 2,9 GB |
| ARCH |  |
| Size | 20 GB |
| Free Space | 2,9 GB |
| OTLADKA |  |
| Size | 20 GB |
| Free Space | 6,9 GB |

### 

### Загрузка

### Память

Allocated memory pool, In bytes: 1 037 438 976 48%

Cache buffer memory, In bytes: 940 204 032 44%

Cache movable memory, In bytes: 0 0%

Cache non-movable memory, In bytes: 77 824 0%

Code and data memory, In bytes: 169 236 480 8%

Total server work memory, In bytes: 2 146 957 312 100%

### 

### Captain

### 

### Описание

Выполняет функции сервера баз данных Oracle. Так же на него происходит backup баз данных с SQL сервера Boatsman

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | CAPTAIN |
| ОS | Microsoft Windows 2000 Server  Version 5.0.2195 Service Pack 4 Build 2195 |
| Производитель | Supermicro |
| Процессор | x86 Family 15 Model 2 Stepping 7 GenuineIntel ~1999 Mhz |
| Память | 2 096 096 KB |
| NIC | Intel(R) PRO/1000 MT Network Connection |
| IP | 192.168.2.245 |
| MASK | 255.255.255.0 |
| DG | 192.168.2.239 |
| MAC | 00:30:48:70:0A:AA |
| Контроллер | MegaRAID SCSI 320-1 Controller |
| C: | Disk #0, Partition #0 |
| File System | NTFS |
| Size | 9.77 GB |
| Free Space | 6.12 GB |
| Drive Model | MEGARAID LD 0 MEGARAID SCSI Disk Device |
| D: | Disk #0, Partition #1 |
| File System | NTFS |
| Size | 58.59 GB |
| Free Space | 32.61 GB |
| Drive Model | MEGARAID LD 0 MEGARAID SCSI Disk Device |

### Boatsman

### Описание

Выполняет функции сервера баз данных Miscrosoft SQL. Так же на него происходит backup баз данных с Oracle сервера Captain

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | BOATSMAN |
| ОS | Microsoft Windows 2000 Server  Version 5.0.2195 Service Pack 4 Build 2195 |
| Производитель | Supermicro |
| Процессор | x86 Family 15 Model 2 Stepping 7 GenuineIntel ~1999 Mhz |
| Память | 2 096 096 KB |
| NIC | Intel(R) PRO/1000 MT Network Connection |
| IP | 192.168.2.246 |
| MASK | 255.255.255.0 |
| DG | 192.168.2.254 |
| MAC | 00:30:48:70:4B:2E |
| Контроллер | MegaRAID SCSI 320-1 Controller |
| C: | Disk #0, Partition #0 |
| File System | NTFS |
| Size | 9.77 GB |
| Free Space | 6.64 GB |
| Drive Model | MEGARAID LD 0 MEGARAID SCSI Disk Device |
| E: | Disk #0, Partition #1 |
| File System | NTFS |
| Size | 58.59 GB |
| Free Space | 42. 15 GB |
| Drive Model | MEGARAID LD 0 MEGARAID SCSI Disk Device |

## Exchserv

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | EXCHSERV |
| ОS | Microsoft Windows 2000 Server  Version 5.0.2195 Service Pack 4 Build 2195 |
| Производитель | Dell Computer Corporation |
| Процессор | x86 Family 6 Model 8 Stepping 6 GenuineIntel ~860 Mhz |
| Память | 523 436 KB |
| NIC | Intel(R) PRO/1000 MT Network Connection |
| IP | 192.168.2.17 |
| MASK | 255.255.255.0 |
| DG | none |
| MAC | 00:B0:D0:7E:02:B9 |
| Контроллер | Adaptec AIC-7892 Ultra160/m PCI SCSI Card |
| C: | Disk #0, Partition #0 |
| File System | FAT |
| Size | 2.00 GB |
| Free Space | 331.75 MB |
| Drive Model | IBM IC35L018UWD210-0 SCSI Disk Device |
| D: | Disk #0, Partition #1 |
| File System | NTFS |
| Size | 15.08 GB |
| Free Space | 13.21 GB |
| Drive Model | IBM IC35L018UWD210-0 SCSI Disk Device |
| H: | Disk #1, Partition #0 |
| File System | NTFS |
| Size | 34.18 GB |
| Free Space | 25.39 GB |
| Drive Model | IBM IC35L036UWD210-0 SCSI Disk Device |
| I: | Disk #2, Partition #0 |
| File System | NTFS |
| Size | 34.18 GB |
| Free Space | 17.95 GB |
| Drive Model | IBM IC35L036UWD210-0 SCSI Disk Device |

### 

## Concord

### 

### Описание

Сервер обеспечивает трехзвенный режим работы RS Bank (в стадии внедрения).

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | CONCORD |
| ОS | Microsoft Windows 2000 Professional  Версия 5.0.2195 Service Pack 4 сборка 2195 |
| Производитель | Supermicro |
| Процессор | x86 Family 15 Model 2 Stepping 7 GenuineIntel ~1999 МГц |
| Память | 2 096 096 КБ |
| NIC | Intel(R) PRO/1000 MT Network Connection |
| IP | 192.168.2.93 (DHCP) |
| MASK | DHCP |
| DG | DHCP |
| MAC | 00:30:48:70:92:2D |
| Контроллер | Adaptec AIC-7902B - Ultra320 SCSI |
| C: | Диск #0, раздел #0 |
| File System | NTFS |
| Size | 17.09 ГБ |
| Free Space | 13.19 ГБ |
| Drive Model | SEAGATE ST318453LW SCSI Disk Device |

### 

## Main2K

### 

### Описание

Active Directory, WINS, DHCP.

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | MAIN2K |
| ОS | Microsoft Windows 2000 Advanced Server  Version 5.0.2195 Service Pack 4 Build 2195 |
| Производитель | noname |
| Процессор | x86 Family 15 Model 1 Stepping 3 GenuineIntel ~1715 Mhz |
| Память | 522 776 KB |
| NIC | Intel(R) PRO/100 VE Network Connection |
| IP | 192.168.2.253 |
| MASK | 255.255.255.0 |
| DG | None |
| MAC | 00:E0:18:7D:2D:4D |
| Контроллер | IDE |
| C: | Disk #0, Partition #0 |
| File System | NTFS |
| Size | 37.26 GB |
| Free Space | 33.12 GB |
| Drive Model | ST340016A |

## Backup

### 

### Описание

Arc Serve, технологическая функция «закрытие дня» для RS Bank.

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | BACKUP |
| ОS | Microsoft Windows 2000 Professional  Версия 5.0.2195 Service Pack 3 сборка 2195 |
| Производитель | Dell Computer Corporation |
| Процессор | x86 Family 6 Model 8 Stepping 10 GenuineIntel ~864 МГц |
| Память | 261 356 КБ |
| NIC | 3Com 3C920 Integrated Fast Ethernet контроллер (3C905C-TX совместимый) |
| IP | 192.168.2.248 |
| MASK | 255.255.255.0 |
| DG | none |
| MAC | 00:06:5B:81:F6:27 |
| Контроллер | Adaptec AIC-7892 Ultra160/m PCI SCSI плата |
| C: | Диск #0, раздел #0 |
| File System | FAT |
| Size | 2,00 ГБ |
| Free Space | 556,78 МБ |
| Drive Model | ST320011A |
| D: | Диск #0, раздел #1 |
| File System | NTFS |
| Size | 16,65 ГБ |
| Free Space | 5,22 ГБ |
| Drive Model | ST320011A |

### 

## Nterm

### 

### Описание

HASP для RS Bank, WINS, контроллер домена NT 4.0

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | NTERM |
| ОS | Windows NT 4.0 Server |
| Производитель | Formoza |
| Процессор | x86 Family 6 Model 7 Stepping 3 GenuineIntel ~450 МГц |
| Память | 163 252 КБ |
| NIC | Adaptec PCI Fast Ethernet Adapter |
| IP | 192.168.2.14 |
| MASK | 255.255.255.0 |
| DG | 192.168.2.2 |
| MAC | 00:00:D1:1D:98:47 |
| Контроллер | IDE |
| C: | Диск #0, раздел #0 |
| File System | FAT |
| Size | 2 GB |
| Free Space | 399 MB |
| Drive Model | ST320420A |
| D: | Диск #0, раздел #1 |
| File System | NTFS |
| Size | 6 GB |
| Free Space | 3 GB |
| Drive Model | ST320420A |
| G: | Диск #0, раздел #2 |
| File System | NTFS |
| Size | 9 GB |
| Free Space | 2,6 MB |
| Drive Model | ST320420A |

## Ntserver

### 

### Описание

Интернет сервер (WinGate), почтовый сервер (MDaemon).

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | NTSERVER |
| ОS | Microsoft Windows NT 4.0 Server |
| Производитель | noname |
| Процессор | x86 Family 6 Model 8 Stepping 10 |
| Память | 512 MB |
| C: | Диск #0, раздел #0 |
| File System | FAT |
| Size | 2,00 ГБ |
| Free Space | 1,5 ГБ |
| Drive Model | IC35L020AVER07-0 |
| D: | Диск #0, раздел #1 |
| File System | NTFS |
| Size | 17 ГБ |
| Free Space | 6,4 ГБ |
| Drive Model | IC35L020AVER07-0 |

### 

## Proxy\_cs

### 

### Описание

Интернет сервер (WinGate), почтовый сервер (MDaemon).

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | PROXY\_CS |
| ОS | Microsoft Windows NT 4.0 Server |
| Производитель | noname |
| Процессор | x86 Family 6 Model 8 Stepping 6 |
| Память | 512 MB |
| Контроллер |  |
| C: | Диск #0, раздел #0 |
| File System | FAT |
| Size | 2,00 ГБ |
| Free Space | 1,5 ГБ |
| Drive Model | Fujitsu MPF3102AH |
| D: | Диск #0, раздел #1 |
| File System | NTFS |
| Size | 2,00 ГБ |
| Free Space | 1,1 ГБ |
| Drive Model | Fujitsu MPF3102AH |
| G: | Диск #0, раздел #2 |
| File System | NTFS |
| Size | 6 ГБ |
| Free Space | 4,2 ГБ |
| Drive Model | Fujitsu MPF3102AH |

## Skipper

### 

### Описание

### 

### Конфигурация

|  |  |
| --- | --- |
| Системное имя | SKIPPER |
| ОS | Microsoft Windows NT 4.0 Server |
| Производитель |  |
| Процессор | Celeron 1100 |
| Память | 640 MB |

# Результаты сканирования на уязвимость

|  |  |  |
| --- | --- | --- |
|  | Хост  194.84.236.131 | |
|  | Информация | |
|  | |  |  | | --- | --- | | Время отклика: | 734 мсек | | TTL: | 118 | | |
|  | Параметры сканирования | |
|  | |  |  | | --- | --- | | Начало сканирования: | 11:27:28 19.07.2004 | | Время сканирования: | 00:33:40 | | |
|  | Доступна информация  Windows | |
|  | Описание | |
|  | Вероятная версия операционной системы : Windows | |
|  | |  |  |  | | --- | --- | --- | | Сервис  FTP выключенный |  | порт  21 / tcp | | |
|  | Информация | |
|  | 421 Service not available (The FTP server is not responding.) | |
|  | |  |  |  | | --- | --- | --- | | Сервис  SMTP |  | порт  25 / tcp | | |
|  | Информация | |
|  | 220 derzhava.ru ESMTP service ready [3] (MDaemon v2.7 SP4 R)  Информация об имени сервера подтверждена эвристическим методом  Сервер : MDaemon SMTP Server X.X.X - 5.X.X | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  97 / tcp | | |
|  | Информация | |
|  | Сервис не определен  Имя сервиса устанавливаемого на этом порту по умолчанию : swift-rvf | |
|  | \*\* #24 B3200000000486d #13 #10 #17 | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  98 / tcp | | |
|  | Информация | |
|  | Сервис не определен  Имя сервиса устанавливаемого на этом порту по умолчанию : tacnews | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  99 / tcp | | |
|  | Информация | |
|  | Сервис не определен.  Имя сервиса устанавливаемого на этом порту по умолчанию : metagram | |
|  | |  |  |  | | --- | --- | --- | | Сервис  POP3 |  | порт  110 / tcp | | |
|  | Информация | |
|  | +OK derzhava.ru POP3 service ready [2] (MDaemon v2.7 SP4 R) | |
|  | |  |  |  | | --- | --- | --- | | Сервис  Microsoft RPC |  | порт  135 / tcp | | |
|  | Информация | |
|  | Имя сервиса : Microsoft Remote Procedure Call | |
|  | Серьезная уязвимость  Удаленное выполнение команд (ms04-012) |
|  | Описание |
|  | Возможно получение удаленной командной строки с правами системы из-за переполнения буфера в DCOM RPC сервиса. |
|  | Решение |
|  | Установите обновление:  http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx |
|  | Ссылки |
|  | CVE (CAN-2003-0813) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0813  CVE (CAN-2004-0116) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0116  CVE (CAN-2003-0807) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0807  CVE (CAN-2004-0124) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0124 |
|  | Доступна информация  Запущена служба DCOM |
|  | Описание |
|  | На компьютере запущена служба DCOM (Distributed Component Object Model). | |
|  | Решение | |
|  | Отключить службу DCOM, если она действительно не нужна. | |
|  | Ссылки | |
|  | CVE (CAN-1999-0658) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0658 | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  554 / tcp | | |
|  | Информация | |
|  | Сервис не определен  Имя сервиса устанавливаемого на этом порту по умолчанию : rtsp | |
|  | |  |  |  | | --- | --- | --- | | Сервис  Wingate Engine |  | порт  808 / tcp | | |
|  | Информация | |
|  | Имя сервиса : Wingate Remote Control Service - административная часть | |
|  | |  |  |  | | --- | --- | --- | | Сервис  RPC mstask.exe |  | порт  1027 / tcp | | |
|  | Информация | |
|  | Имя сервиса : Task Scheduler Engine | |
|  | Доступна информация  Scheduler Service | |
|  | Описание | |
|  | Если вы не используете планировщик задач, то разумным будет отключить его, т.к. данный сервис часто используется атакующими для запуска вредоносного кода. | |
|  | Решение | |
|  | Заблокируйте сервис следующим ключём реестра:  HKEY\_LOCAL\_MACHINE  SYSTEM\CurrentControlSet\Services\Schedule  Start = 4 | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1720 / tcp | | |
|  | Информация | |
|  | Сервис не определен  Имя сервиса устанавливаемого на этом порту по умолчанию : h323hostcall | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1723 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему  Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1755 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему  Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  2000 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему  Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  6666 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему  Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  6667 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему.  Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  6668 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис |  | порт  7070 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  8081 / tcp | | |
|  | Информация | |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. | |

|  |  |
| --- | --- |
|  | Хост  195.210.129.70 |
|  | Информация |
|  | |  |  | | --- | --- | | Имя хоста (полученное при обратном DNS запросе): | Derzhava.access.comstar.ru | | Время отклика: | 156 мсек | | TTL: | 122 | |
|  | Параметры сканирования |
|  | |  |  | | --- | --- | | Начало сканирования: | 11:37:57 19.07.2004 | | Время сканирования: | 00:52:37 | |
|  | Доступна информация  Windows NT 4.0 |
|  | Описание |
|  | Вероятная версия операционной системы : Windows NT 4.0 |
|  | |  |  |  | | --- | --- | --- | | Сервис  FTP выключенный |  | порт  2 / tcp | |
|  | Информация |
|  | 421 Service not available (The FTP server is not responding.) |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  33 / tcp | |
|  | Информация |
|  | Сервис не определен.  Имя сервиса устанавливаемого на этом порту по умолчанию : dsp |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  97 / tcp | |
|  | Информация |
|  | Сервис не определен  Имя сервиса устанавливаемого на этом порту по умолчанию : swift-rvf |
|  | \*\* #24 B3200000000486d #13 #10 #17 |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  98 / tcp | |
|  | Информация |
|  | Сервис не определен.  Имя сервиса устанавливаемого на этом порту по умолчанию : tacnews |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  99 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему  Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  Microsoft RPC |  | порт  135 / tcp | |
|  | Информация |
|  | Имя сервиса : Microsoft Remote Procedure Call |
|  | Серьезная уязвимость  Удаленное выполнение команд (ms04-012) |
|  | Описание |
|  | Возможно получение удаленной командной строки с правами системы из-за переполнения буфера в DCOM RPC сервиса. |
|  | Решение |
|  | Установите обновление:  http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx |
|  | Ссылки |
|  | CVE (CAN-2003-0813) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0813  CVE (CAN-2004-0116) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0116  CVE (CAN-2003-0807) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0807  CVE (CAN-2004-0124) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0124 |
|  | Доступна информация  Запущена служба DCOM |
|  | Описание |
|  | На компьютере запущена служба DCOM (Distributed Component Object Model). |
|  | Решение |
|  | Отключить службу DCOM, если она действительно не нужна. |
|  | Ссылки |
|  | CVE (CAN-1999-0658) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0658 |
|  | |  |  |  | | --- | --- | --- | | Сервис  Microsoft RPC |  | порт  135 / udp | |
|  | Информация |
|  | Имя сервиса : Microsoft Remote Procedure Call |
|  | |  |  |  | | --- | --- | --- | | Сервис  NetBIOS-SSN |  | порт  137 / udp | |
|  | Информация |
|  | Имя сервиса : NetBIOS (Network Basic Input/Output System) Session Service Protocol |
|  | |  |  |  | | --- | --- | --- | | Сервис  NetBIOS |  | порт  139 / tcp | |
|  | Информация |
|  | Имя сервиса : Network Basic Input/Output System |
|  | Уязвимость  Список ресурсов |
|  | Описание |
|  | Список ресурсов хоста  C – пользовательский  D – пользовательский  G – пользовательский  ADMIN$ (Remote Admin) - диск по умолчанию  IPC$ (Remote IPC) - pipe по умолчанию  C$ (Default share) - диск по умолчанию  D$ (Default share) - диск по умолчанию  G$ (Default share) - диск по умолчанию  Всегда следует чётко следить за теми данными, которые пользователь предоставляет для общего доступа. |
|  | Решение |
|  | Windows:  Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии")  Samba:  Разрешить доступ к серверу только зарегестрированным пользователям:  в файле smb.conf изменить ключ security= share на security= user (или security = server или security = domain ). |
|  | Уязвимость  Список пользователей ( 1 - 5 ) |
|  | Описание |
|  | Список пользователей хоста :  пользователь : 902  привилегии : Администратор  входов : 1  время последнего подключения : Wed Jul 14 13:59:00 2004  с момента последней смены пароля прошло (дней) : 4  статус аккаунта : срок действия пароля неограничен  пользователь : Administrator  привилегии : Администратор  комментарий : Built-in account for administering the computer/domain  входов : 133  время последнего подключения : Wed Jul 14 23:11:53 2004  время последнего отключения : Tue Jun 29 16:41:32 2004  с момента последней смены пароля прошло (дней) : 278  статус аккаунта : срок действия пароля неограничен  пользователь : but  привилегии : Администратор  входов : 830  время последнего подключения : Sun Jul 18 04:02:13 2004  время последнего отключения : Mon Jul 19 12:20:37 2004  с момента последней смены пароля прошло (дней) : 354  статус аккаунта : срок действия пароля неограничен  пользователь : Guest  привилегии : Гость  комментарий: Built-in account for guest access to the computer/domain  входов : 0  с момента последней смены пароля прошло (дней) : 1180  статус аккаунта : отключен (disabled), срок действия пароля неограничен  пользователь : vvs  привилегии : Администратор  входов : 0  время последнего подключения : Tue Oct 21 12:18:48 2003  с момента последней смены пароля прошло (дней) : 361  статус аккаунта : срок действия пароля неограничен  Получение списка пользователей позволяет удалённому атакующему начать перебор паролей к существующим учётным записям. |
|  | Решение |
|  | Windows:  Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии")  Samba:  Разрешить доступ к серверу только зарегестрированным пользователям:  в файле smb.conf изменить ключ security= share на security= user (или security = server или security = domain ). |
|  | Уязвимость  Список активных сессий |
|  | Описание |
|  | Список активных сессий:  хост :  пользователь :  длительность подключения : 00:00:31  Получение списка активных сессий позволяет удалённому атакующему атаковать менее защищенные хосты, с которых осуществляются подключения к серверу, с целью получения привилегий на сервере. |
|  | Решение |
|  | Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии") и/или отключить гостевой логин на сервере. |
|  | Доступна информация  Имя компьютера и домен |
|  | Описание |
|  | Имя компьютера : PROXY\_CS  Домен : PROXY |
|  | Доступна информация  Список групп пользователей |
|  | Описание |
|  | Список групп пользователей:  Локальные группы пользователей :  группа : Administrators  комментарий : Members can fully administer the computer/domain  группа : Backup Operators  комментарий : Members can bypass file security to back up files  группа : Guests  комментарий : Users granted guest access to the computer/domain  группа : Power Users  комментарий : Members can share directories and printers  группа : Replicator  комментарий : Supports file replication in a domain  группа : Users  комментарий : Ordinary users  Глобальные группы пользователей :  группа : None  комментарий : Ordinary users |
|  | Решение |
|  | Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии") и/или отключить гостевой логин на сервере. |
|  | Доступна информация  Список транспортных протоколов |
|  | Описание |
|  | Список транспортных протоколов, установленных на хосте :  устройство (протокол) : \Device\NetBT\_DE5282  имя сервера : PROXY\_CS  сетевой адрес : 0050badc4b60  число подключенных пользователей : 0  домен : PROXY  устройство (протокол) : \Device\NetBT\_DE5282  имя сервера : PROXY\_CS  сетевой адрес : 0050badc4b60  число подключенных пользователей : 0  домен : PROXY  устройство (протокол) : \Device\NetBT\_DE5281  имя сервера : PROXY\_CS  сетевой адрес : 0050badc5542  число подключенных пользователей : 0  домен : PROXY  устройство (протокол) : \Device\NetBT\_DE5281  имя сервера : PROXY\_CS  сетевой адрес : 0050badc5542  число подключенных пользователей : 0  домен : PROXY  устройство (протокол) : \Device\NetBT\_NdisWan5  имя сервера : PROXY\_CS  сетевой адрес : 000000000000  число подключенных пользователей : 0  домен : PROXY  устройство (протокол) : \Device\NetBT\_NdisWan5  имя сервера : PROXY\_CS  сетевой адрес : 000000000000  число подключенных пользователей : 1  домен : PROXY |
|  | Решение |
|  | Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии") и/или отключить гостевой логин на сервере. |
|  | Доступна информация  Доступ по нулевой сессии |
|  | Описание |
|  | Эта уязвимость существует только в том случае, если Вы не являетесь Администратором  на проверяемом хосте  Доступ по нулевой сессии представляет собой возможность неавторизованного подключения к хосту с операционной системой основанной на Windows NT (или ОС семейства UNIX с установленным пакетом Samba) с пустым логином и паролем. При включенной нулевой сессии анонимный пользователь может получить большое количество информации о конфигурации системы (список расшаренных ресурсов, список пользователей, список рабочих групп и т.д.). Полученная информация в дальнейшем может быть использованна для попыток несанкционированного доступа. |
|  | Решение |
|  | Windows:  В разделе реестра  HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSA  установить значение параметра RestrictAnonymous = 2 для Windows 2000/XP/2003 ( 1 для Windows NT3.5/NT4.0 ) ( тип параметра - REG\_DWORD )  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver  установить значение параметра RestrictNullSessionAccess = 1 ( тип параметра –  REG\_DWORD )  Перегрузить систему для вступления изменений в силу.  Samba:  Разрешить доступ к серверу только зарегестрированным пользователям:  в файле smb.conf изменить ключ security= share на security= user (или security = server или security = domain ). |
|  | Ссылки |
|  | CVE (CVE-2000-1200) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1200  http://support.microsoft.com/support/kb/articles/q143/4/74.asp |
|  | Доступна информация  LanManager и OS |
|  | Описание |
|  | LanManager: NT LAN Manager 4.0  OS: Windows NT 4.0 |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  389 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  554 / tcp | |
|  | Информация |
|  | Сервис не определен.  Имя сервиса устанавливаемого на этом порту по умолчанию : rtsp |
|  | |  |  |  | | --- | --- | --- | | Сервис  Wingate Engine |  | порт  808 / tcp | |
|  | Информация |
|  | Имя сервиса : Wingate Remote Control Service - административная часть |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1025 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  RPC mstask.exe |  | порт  1027 / tcp | |
|  | Информация |
|  | Имя сервиса : Task Scheduler Engine |
|  | Доступна информация  Scheduler Service |
|  | Описание |
|  | Если вы не используете планировщик задач, то разумным будет отключить его, т.к. данный сервис часто используется атакующими для запуска вредоносного кода. |
|  | Решение |
|  | Заблокируйте сервис следующим ключём реестра:  HKEY\_LOCAL\_MACHINE  SYSTEM\CurrentControlSet\Services\Schedule  Start = 4 |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1720 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1723 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  1755 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  2000 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  6666 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  6667 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  6668 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |
|  | |  |  |  | | --- | --- | --- | | Сервис  ? |  | порт  7070 / tcp | |
|  | Информация |
|  | Сервис разрывает соединение при попытке подключения к нему. Вероятно закрыт доступ к этому сервису для IP адреса с которого проводилась проверка. |

# Выводы

## 

## Состояние сетевой инфраструктуры

За время наблюдения не было замечено ни одной ошибки вызванной неправильной работой сетевого оборудования или неправильной конфигурацией сетевых протоколов. Внутренняя локальная сеть находится в отличном состоянии. Ширина канала подключения основных серверов превосходит агрегированную полосу пропускания клиентских компьютеров.

Но виду разнородности сетевого оборудования наблюдаются проблемы его объединение, что приводит к его нерациональному его использованию, как например коммутатор catalist1.

Сеть не обеспечивает избыточности каналов связи и вывод из строя любого коммутатора приведет к ее неработоспособности. В виду того, что конфигурация сети не включает в себя VLAN`ы и существует достаточное количество свободных портов, а загрузка магистрали такова, что роль центрального коммутатора можно временно возложить на другой, менее производительный. Прогнозируемый простой в результате выхода коммутатора из строя от 15 мин до 1 часа.

## Состояние серверов

Анализ загруженности серверов показал, что конфигурации практически всех серверов удовлетворяют возложенным на них задачам по производительности.

Исключением является сервер Exchserv на котором наблюдается острая нехватка оперативной памяти. Рекомендуется ее увеличение до 1 Гб. Так же дисковая система сконфигурированная на этом сервере не обеспечивает устойчивость хранимых данных к сбоям (по сути дисковая система на сервере представляет простой набор дисков JBOD). Учитывая выполняемую сервером роль (Exchange Server) можно предполагать, что его важность в современной организации может только расти и в скором времени превратится в «критичный для бизнеса» (business critical). В настоящее время сервер не обеспечивает каких либо перспектив для роста возложенной на него задачи, ни по производительности процессора, ни по объему дисковых накопителей.

И сервер ADMIRAL. Неудовлетворительная работа которого при выходе из строя сервера Cruiser в большей степени связана с нехваткой памяти.

Нарекание вызывает так же конфигурация дисковых систем некоторых серверов (EXCHSERV, CONCORD, MAIN2K, NTERM, NTSERVER, PROXY\_CS) которые не обеспечиваю избыточность хранения данных.

## Состояние безопасности

Сканирование внешних интерфейсов серверов доступа в Интернет выявил серьезные уязвимости в системе безопасности, устранение которых является срочной и первоочередной задачей.

Так же можно назвать следующие проблемы сетевой безопасности:

* Недостаточная защищенность серверов доступа в Интернет, наличие на них уязвимостей.
* Отсутствие системы обнаружения атак.
* Отсутствие документированной политики безопасности.
* Недостаточное внимание уделено защите от угрозы изнутри

Были найдены следующие серьезные уязвимости уязвимости:

|  |  |
| --- | --- |
|  | Хост  194.84.236.131 |
|  | Серьезная уязвимость  Удаленное выполнение команд (ms04-012) |
|  | Возможно получение удаленной командной строки с правами системы из-за переполнения буфера в DCOM RPC сервиса. |

|  |  |
| --- | --- |
|  | Хост  195.210.129.70 |
|  | |  |  | | --- | --- | | Имя хоста (полученное при обратном DNS запросе): | Derzhava.access.comstar.ru | |
|  | Серьезная уязвимость  Удаленное выполнение команд (ms04-012) |
|  | Возможно получение удаленной командной строки с правами системы из-за переполнения буфера в DCOM RPC сервиса. |
|  | Уязвимость  Список ресурсов |
|  | Список ресурсов хоста :  C – пользовательский  D – пользовательский  G – пользовательский  ADMIN$ (Remote Admin) - диск по умолчанию  IPC$ (Remote IPC) - pipe по умолчанию  C$ (Default share) - диск по умолчанию  D$ (Default share) - диск по умолчанию  G$ (Default share) - диск по умолчанию  Всегда следует чётко следить за теми данными, которые пользователь предоставляет для общего доступа. |
|  | Уязвимость  Список пользователей ( 1 - 5 ) |
|  | Список пользователей хоста :  пользователь : 902  привилегии : Администратор  входов : 1  время последнего подключения : Wed Jul 14 13:59:00 2004  с момента последней смены пароля прошло (дней) : 4  статус аккаунта : срок действия пароля неограничен  пользователь : Administrator  привилегии : Администратор  комментарий : Built-in account for administering the computer/domain  входов : 133  время последнего подключения : Wed Jul 14 23:11:53 2004  время последнего отключения : Tue Jun 29 16:41:32 2004  с момента последней смены пароля прошло (дней) : 278  статус аккаунта : срок действия пароля неограничен  пользователь : but  привилегии : Администратор  входов : 830  время последнего подключения : Sun Jul 18 04:02:13 2004  время последнего отключения : Mon Jul 19 12:20:37 2004  с момента последней смены пароля прошло (дней) : 354  статус аккаунта : срок действия пароля неограничен  пользователь : Guest  привилегии : Гость  комментарий : Built-in account for guest access to the computer/domain  входов : 0  с момента последней смены пароля прошло (дней) : 1180  статус аккаунта : отключен (disabled), срок действия пароля неограничен  пользователь : vvs  привилегии : Администратор  входов : 0  время последнего подключения : Tue Oct 21 12:18:48 2003  с момента последней смены пароля прошло (дней) : 361  статус аккаунта: срок действия пароля неограничен  Получение списка пользователей позволяет удалённому атакующему начать перебор паролей к существующим учётным записям. |

Найденные уязвимости позволяют получить полный контроль над пограничными серверами (Proxy\_CS и NTerm), контроль над этими серверами даст атакующему следующие возможности:

* полный контроль над системой электронной почты
* возможность перехвата конфиденциальной информации от клиентов банка подключающихся через систему Клиент-Банк
* данные узлы могут быть использованы в качестве плацдарма для атаки на внутреннюю сеть банка.

В качестве временного решения может быть установка на существующие сервера файрволла (например Kerio WinRoute Firewall), однако для более полноценной защиты рекомендуется использовать Microsoft Internet Security and Acceleration Server.

Наличие внутреннего протокола IPX затрудняет организацию внутренней безопасности сети в веду большой дороговизны маршрутизирующих устройств и невозможности организовать защиту конфиденциальной информации без разделения сети на широковещательные домены. И хотя протокол IPX затруднен для анализа при перехвате это не может быть хорошей защитой при целенаправленной атаке. Рекомендуется отказ от протокола IPX в пользу IP, что позволит реализовать следующие преимущества

- разделение внутренней локальной сети на широковещательные домены, возможность фильтрации трафика

- использование технологии IPSec

## Общая оценка

В целом состояние сети можно характеризовать как «хорошее», однако проблемы в организации безопасности довольно серьезны и требуют серьезного и целостного подхода к данной проблеме.

Нет комплексного подхода в выборе типа оборудования и его производителя. Можно наблюдать большой выбор однотипного оборудования от разных производителей, как серверного так и сетевого. Отсутствие единых корпоративных стандартов в этом вопросе увеличивает издержки на поддержание и сопровождение, в тоже время снижая надежность всей сети в целом и качество ее сопровождения (знание персоналом нескольких типов одного оборудования, не способствует его глубокому знанию, в тоже время затраты на обучение возрастают).

Нельзя не отметить высокую подготовку технического персонала. Однако можно порекомендовать следующие курсы:

* М2273 Управление и поддержка среды Microsoft Windows Server 2003 ($525)
* М2823 Настройка и администрирование безопасности в сетях Microsoft Windows Server 2003 ($511)
* М2400 Внедрение и поддержка Microsoft Exchange Server 2003 ($511)
* 10842/U3965S Управление системами на базе hp ProLiant ($620)
* CCNP: Поиск и устранение неисправностей в сетях Cisco (от $640)

Приложение 1

# Отчет для руководителя

## 

## Отчет по состоянию сервера ADMIRAL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: ADMIRAL  Операционная система: Novell NetWare 6.0  Роль сервера: BackUp сервер для Cruiser | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ✔ | ⬜ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ✔ | ⬜ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ✔ | ⬜ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ⬜ | ✔ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ⬜ | ✔ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ⬜ | ✔ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера BREEZE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: BREEZE  Операционная система: Novell NetWare 6.0  Роль сервера: BackUp сервер для Cruiser | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ⬜ | ✔ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2.5 | Питание | | ⬜ | ⬜ | ✔ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ⬜ | ✔ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ⬜ | ✔ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера CRUISER

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: CRUISER  Операционная система: Novell NetWare 6.0  Роль сервера: Файло | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ✔ | ⬜ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ⬜ | ✔ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ⬜ | ✔ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ⬜ | ✔ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера Captain

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Captain  Операционная система: Windows 2000 Server  Роль сервера: Выполняет функции сервера баз данных Oracle. Также на него происходит бэкап баз данных с SQL сервера Boatsman | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ⬜ | ✔ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ⬜ | ✔ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ⬜ | ✔ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера Boatsman

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Boatsman  Операционная система: Windows 2000 Server  Роль сервера: Выполняет функции сервера баз данных SLQ. Также на него происходит бэкап баз данных с Oracle сервера Captain | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ⬜ | ✔ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ⬜ | ✔ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ⬜ | ✔ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера Exchserv

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Exchserv  Операционная система: Windows 2000 Server  Роль сервера: Почтовый сервер (MS Exchange 2000 Server) | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ✔ | ⬜ | ⬜ |
| 2 | Устойчивость к сбоям | ✔ | ⬜ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ✔ | ⬜ | ⬜ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ✔ | ⬜ | ⬜ |
| 1.3 | Дисковая подсистема | | ⬜ | ✔ | ⬜ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ✔ | ⬜ | ⬜ |
| 2.1 | Диски | | ✔ | ⬜ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ✔ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ✔ | ⬜ | ⬜ |

## Отчет по состоянию сервера Concord

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Concord  Операционная система: Windows 2000 Professional  Роль сервера: Обеспечивает трехзвенный режим работы RS Bank | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ✔ | ⬜ | ⬜ |
| 2.1 | Диски | | ✔ | ⬜ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ✔ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера Main2K

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Main2K  Операционная система: Windows 2000 Server  Роль сервера: Active Directory, WINS, DHCP | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ✔ | ⬜ |
| 2 | Устойчивость к сбоям | ✔ | ⬜ | ⬜ |
| 3 | Восстановление после сбоев | ✔ | ⬜ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ✔ | ⬜ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ✔ | ⬜ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ✔ | ⬜ | ⬜ |
| 2.1 | Диски | | ✔ | ⬜ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ✔ | ⬜ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ✔ | ⬜ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ✔ | ⬜ | ⬜ |

## Отчет по состоянию сервера BackUp

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: BackUp  Операционная система: Windows 2000 Professional  Роль сервера: Arc Serve, технологическая функция «закрытие дня» для RS Bank. | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ✔ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ✔ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера Nterm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Nterm  Операционная система: Windows 2000 Professional  Роль сервера: HASP для RS Bank, Wins, контроллер Windows NT 4.0 | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ✔ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ✔ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ⬜ | ✔ | ⬜ |
| 4.3 | Аудит доступа | | ⬜ | ✔ | ⬜ |
| 5 | Общая оценка состояния сервера | | ⬜ | ✔ | ⬜ |

## Отчет по состоянию сервера Ntserver

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Ntserver  Операционная система: Windows NT 4.0  Роль сервера: Интернет сервер (WinGate), почтовый сервер (MDaemon) | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ✔ | ⬜ | ⬜ |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ✔ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ✔ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ✔ | ⬜ | ⬜ |
| 4.3 | Аудит доступа | | ✔ | ⬜ | ⬜ |
| 5 | Общая оценка состояния сервера | | ✔ | ⬜ | ⬜ |

## Отчет по состоянию сервера Proxy\_CS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н | Имя сервера: Proxy\_cs  Операционная система: Windows NT 4.0  Роль сервера: Интернет сервер (WinGate), почтовый сервер (MDaemon) | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | ✔ | ⬜ | ⬜ |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Загруженность сервера | | ⬜ | ⬜ | ✔ |
| 1.1 | Процессор | | ⬜ | ⬜ | ✔ |
| 1.2 | Память | | ⬜ | ⬜ | ✔ |
| 1.3 | Дисковая подсистема | | ⬜ | ⬜ | ✔ |
| 1.4 | Сетевые интерфейсы | | ⬜ | ⬜ | ✔ |
| 2 | Устойчивость к сбоям | | ⬜ | ✔ | ⬜ |
| 2.1 | Диски | | ⬜ | ✔ | ⬜ |
| 2.2 | Память | | ⬜ | ✔ | ⬜ |
| 2.3 | Процессоры | | ⬜ | ✔ | ⬜ |
| 2.4 | Сетевые интерфейсы | | ⬜ | ✔ | ⬜ |
| 2.5 | Питание | | ⬜ | ✔ | ⬜ |
| 3 | Восстановление после сбоев | | ⬜ | ✔ | ⬜ |
| 3.1 | Восстановление данных | | ⬜ | ✔ | ⬜ |
|  | 3.1.1 | Стратегия восстановления данных | ⬜ | ⬜ | ✔ |
|  | 3.1.2 | Наличие проверенного BackUp | ⬜ | ✔ | ⬜ |
| 3.2 | Восстановление программного обеспечения | | ⬜ | ✔ | ⬜ |
|  | 3.2.1 | Наличие дистрибьютивов ПО | ⬜ | ⬜ | ✔ |
|  | 3.2.2 | Наличие Recovery BackUp | ⬜ | ✔ | ⬜ |
| 3.3 | ЗИП | | ⬜ | ✔ | ⬜ |
| 4 | Защита данных от НСД | | ⬜ | ✔ | ⬜ |
| 4.1 | Антивирусная защита | | ⬜ | ✔ | ⬜ |
| 4.2 | Firewall | | ✔ | ⬜ | ⬜ |
| 4.3 | Аудит доступа | | ✔ | ⬜ | ⬜ |
| 5 | Общая оценка состояния сервера | | ✔ | ⬜ | ⬜ |

## Отчет по состоянию сети

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/н |  | Критично | Не удовлет-ворительно | Удовлет-ворительно |
| 1 | Сегмент ЛВС | ⬜ | ⬜ | ✔ |
| 2 | Канал выхода в Интернет | ⬜ | ⬜ | ✔ |
| 3 | Защита от НСД изнутри | ✔ | ⬜ | ⬜ |
| 4 | Защита от НСД из вне | ✔ | ⬜ | ⬜ |
| 5 | Общая оценка состояния ЛВС | ⬜ | ✔ | ⬜ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Сегмент ЛВС | | ⬜ | ⬜ | ✔ |
|  | 1.1 | Загрузка коммутаторов | ⬜ | ⬜ | ✔ |
|  | 1.2 | Загрузка связей комутаторов | ⬜ | ⬜ | ✔ |
|  | 1.3 | Процент широковещательного трафика | ⬜ | ⬜ | ✔ |
|  | 1.4 | Процент неизвестных («битых») пакетов | ⬜ | ⬜ | ✔ |
| 2 | Канал выхода в Интернет | | ⬜ | ⬜ | ✔ |
|  | 2.1 | Загрузка канала выхода в Интернет | ⬜ | ⬜ | ✔ |
|  | 2.2 | Кэширование запросов | ⬜ | ⬜ | ✔ |
| 3 | Защита от НСД изнутри | | ✔ | ⬜ | ⬜ |
|  | 3.1 | Ограничение доступа в Интернет | ⬜ | ⬜ | ✔ |
|  | 3.2 | Наличие конфиденциальной информации в широковещательном домене | ✔ | ⬜ | ⬜ |
|  | 3.3 | Возможность несанкционированного подключения | ⬜ | ✔ | ⬜ |
|  | 3.4 | Политика пароля | ✔ | ⬜ | ⬜ |
| 4 | Защита от НСД из вне | | ✔ | ⬜ | ⬜ |
|  | 4.1 | Firewall по периметру сети | ✔ | ⬜ | ⬜ |
|  | 4.2 | Аудит известных атак | ✔ | ⬜ | ⬜ |
| 5 | Общая оценка состояния ЛВС | | ⬜ | ✔ | ⬜ |

Процесс замены серверов был разбит на три очереди:

Первая очередь – рекомендуется немедленная замена сервера или замена сервера в ближайшее время

Вторая очередь – рекомендуется замена сервера в ближайшие один-два года.

Третья очередь – в замене сервера на прогнозируемый период нет необходимости.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: ADMIRAL  Операционная система: Novell NetWare 6.0  Роль сервера: BackUp сервер для Cruiser | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ✔ | ⬜ | Недостаточно памяти, увеличить память до 1Gb |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Не является серьезной проблемой |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Не является серьезной проблемой |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | После увеличения объема памяти и решения проблем связанных с безопасностью состояние сервера можно будет признать удовлетворительным.  В виду того, что в настоящее время функции «страховочного» сервера для CRUISER выполняет сервер BREEZE замена данного сервера после окончания срока службы вряд ли обоснована. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: BREEZE  Операционная система: Novell NetWare 6.0  Роль сервера: BackUp сервер для Cruiser | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Сервер предусматривает защиту от сбоя в случае выхода из строя практически всех основных компонентов, необходимо конфигурирование. |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». Рекомендуется провести данную архивацию. |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | Рекомендуется настройка сервера для максимального противодействия сбоям, проведение Disaster Recovery BackUp и решение проблем с безопасностью. И перевод RS-Bank на этот сервер в качестве основного в виду его наибольшей производительности и надежности.  Срок службы сервера 3 -5 лет.  Через 3 года рекомендуется понижение роли сервера для выполнения менее ответственных задач.  Третья очередь замены серверов |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: CRUISER  Операционная система: Novell NetWare 6.0  Роль сервера: Основной сервер RS-Bank | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Технологии реализованные в сервере позволяют обеспечить дублирование большинства основных компонентов сервера, рекомендуется установка дублирующих компонентов и настройка сервера на противодействие сбоям |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». Рекомендуется провести данную архивацию. |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | Рекомендуется настройка сервера для максимального противодействия сбоям, проведение Disaster Recovery BackUp и решение проблем с безопасностью.  Рекомендуется понижение роли сервера до «страховочного» для Breeze  Третья очередь замены серверов |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Captain  Операционная система: Windows 2000 Server  Роль сервера: Выполняет функции сервера баз данных Oracle. Также на него происходит бэкап баз данных с SQL сервера Boatsman | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Не является серьезной проблемой |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». Рекомендуется провести данную архивацию. |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | Рекомендуется проведение Disaster Recovery BackUp и решение проблем с безопасностью.  Вторая очередь замены серверов |

Предложение по замене

|  |  |  |
| --- | --- | --- |
| количество | p/n | описание |
| 1 | 292889-421 | HP ProLiant DL360 G3 X2.8GHz EU Server  ProLiant DL360R03 P2800-512KB, 512MB #3 |
| 2 | 286778-B22 | HP 72GB 15K U320 Pluggable Hard Drive |
| 1 | 300678-B21 | HP 512MB PC2100 DDR SDRAM DIMM Memory |
| 1 | 293703-B21 | HP DL360 325W HP 5-15P RPS IEC Cord |
| 1 | P73-00663 | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Boatsman  Операционная система: Windows 2000 Server  Роль сервера: Выполняет функции сервера баз данных SLQ. Также на него происходит бэкап баз данных с Oracle сервера Captain | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Не является серьезной проблемой |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». Рекомендуется провести данную архивацию. |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | Рекомендуется проведение Disaster Recovery BackUp и решение проблем с безопасностью.  Вторая очередь замены серверов |

Предложение по замене.

|  |  |  |
| --- | --- | --- |
| количество | p/n | описание |
| 1 | 292889-421 | HP ProLiant DL360 G3 X2.8GHz EU Server  ProLiant DL360R03 P2800-512KB, 512MB #3 |
| 2 | 286778-B22 | HP 72GB 15K U320 Pluggable Hard Drive |
| 1 | 300678-B21 | HP 512MB PC2100 DDR SDRAM DIMM Memory |
| 1 | 293703-B21 | HP DL360 325W HP 5-15P RPS IEC Cord |
| 1 | P73-00663 | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Exchserv  Операционная система: Windows 2000 Server  Роль сервера: Почтовый сервер (MS Exchange 2000 Server) | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ✔ | ⬜ | ⬜ | Нехватка памяти, дисковая система является узким местом, процессор не сможет обеспечить рост нагрузки |
| 2 | Устойчивость к сбоям | ✔ | ⬜ | ⬜ | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». Рекомендуется разработать и проверить методику архивации Exchange Servera. |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ | Рекомендуется замена сервера.  Первая очередь замены серверов. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Concord  Операционная система: Windows 2000 Professional  Роль сервера: Обеспечивает трехзвенный режим работы RS Bank | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы однако возможность переложить задачи данного сервера на другую машину позволяет не рассматривать данную проблему как критичную. Остальные компоненты сервера также не могут обеспечить избыточность. |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | Рекомендуется замена сервера.  Вторая очередь замены серверов. |

Предложение по замене.

|  |  |  |
| --- | --- | --- |
| количество | p/n | описание |
| 1 | 336549-422 | HP ProLiant DL320 G2 P3.06GHz EU Server  ProLiant DL320R02 P3060-512KB #4 |
| 1 | 278424-B21 | HP 80GB ATA Non-Hot Plug Hard Disk Drive |
| 2 | 287496-B21 | HP 512MB PC2100 DDR SDRAM DIMM Memory |
| 1 | P73-00663 | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Main2K  Операционная система: Windows 2000 Server  Роль сервера: Active Directory, WINS, DHCP | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ✔ | ⬜ | Дисковая подсистема является узким местом |
| 2 | Устойчивость к сбоям | ✔ | ⬜ | ⬜ | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы Остальные компоненты сервера также не могут обеспечить избыточность. |
| 3 | Восстановление после сбоев | ✔ | ⬜ | ⬜ | Отсутствует проверенный BackUp сервера |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ | Рекомендуется замена сервера.  Часть задач выполняемых этим сервером можно возложить на Exchange Server, что уменьшит критичность требований к надежности данного сервера.  Вторая очередь замены серверов. |

Предложение по замене.

|  |  |  |
| --- | --- | --- |
| количество | p/n | описание |
| 1 | 292889-421 | HP ProLiant DL360 G3 X2.8GHz EU Server  ProLiant DL360R03 P2800-512KB, 512MB #3 |
| 2 | 286778-B22 | HP 72GB 15K U320 Pluggable Hard Drive |
| 1 | 293703-B21 | HP DL360 325W HP 5-15P RPS IEC Cord |
| 1 | P73-00663 | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: BackUp  Операционная система: Windows 2000 Professional  Роль сервера: Arc Serve, технологическая функция «закрытие дня» для RS Bank. | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы однако возможность переложить задачи данного сервера на другую машину позволяет не рассматривать данную проблему как критичную. Остальные компоненты сервера также не могут обеспечить избыточность. |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствует проверенный BackUp сервера |
| 4 | Защита данных от НСД | ⬜ | ✔ | ⬜ | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | ✔ | ⬜ | Задачи выполняемые данным сервером могут быть возложены на другие машины.  Рекомендуется замена сервера.  Вторая очередь замены серверов. |

Предложение по замене.

Сервер для функции «закрытие дня», функции Back UP рекомендуется возложить на другой сервер.

|  |  |  |
| --- | --- | --- |
| количество | p/n | описание |
| 1 | 336549-422 | HP ProLiant DL320 G2 P3.06GHz EU Server  ProLiant DL320R02 P3060-512KB #4 |
| 1 | 278424-B21 | HP 80GB ATA Non-Hot Plug Hard Disk Drive |
| 2 | 287496-B21 | HP 512MB PC2100 DDR SDRAM DIMM Memory |
| 1 | P73-00663 | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Nterm  Операционная система: Windows 2000 Professional  Роль сервера: HASP для RS Bank, Wins, контроллер Windows NT 4.0 | Критично | | Не удовлет-ворительно | | | Удовлет-ворительно | |  |
| 1 | Загруженность сервера | ⬜ | | ⬜ | | | ✔ | | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | | ✔ | | | ⬜ | | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы однако возможность переложить задачи данного сервера на другую машину позволяет не рассматривать данную проблему как критичную. Остальные компоненты сервера также не могут обеспечить избыточность. |
| 3 | Восстановление после сбоев | ⬜ | | ✔ | | | ⬜ | | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». |
| 4 | Защита данных от НСД | ⬜ | | ✔ | | | ⬜ | | Является частью общей проблемы обеспечения безопасности |
| 5 | Общая оценка состояния сервера | ⬜ | | ✔ | | | ⬜ | | Задачи выполняемые данным сервером могут быть возложены на другие машины, в виду того, что эти задачи не ресурсоемки это не приведет к увеличению их нагрузки.  В виду того что основная задача выполняемая данным сервером (Контроллер домена Windows NT 4.0) уже устарела и не актуальна, замена данного сервера после окончания срока службы не рациональна. |
| п/н | Имя сервера: Ntserver  Операционная система: Windows NT 4.0  Роль сервера: Интернет сервер (WinGate), почтовый сервер (MDaemon) | | Критично | | Не удовлет-ворительно | Удовлет-ворительно | |  | |
| 1 | Загруженность сервера | | ⬜ | | ⬜ | ✔ | | Нет проблем | |
| 2 | Устойчивость к сбоям | | ⬜ | | ✔ | ⬜ | | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы однако возможность переложить задачи данного сервера на другую машину позволяет не рассматривать данную проблему как критичную. Остальные компоненты сервера также не могут обеспечить избыточность. | |
| 3 | Восстановление после сбоев | | ⬜ | | ✔ | ⬜ | | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». | |
| 4 | Защита данных от НСД | | ✔ | | ⬜ | ⬜ | | Очень серьезные проблемы безопасности (см. результаты сканирования на уязвимость) | |
| 5 | Общая оценка состояния сервера | | ✔ | | ⬜ | ⬜ | | Очень серьезные проблемы связанные с обеспечением безопасности, данный сервер может быть взломан из Internet и использован в качестве плацдарма для доступа во внутреннюю локальную сеть.  В качестве временных мер решения данных проблем можно порекомендовать установку firewall (например Kerio WinRoute Firewall).  Рекомендуется полная замена данного сервера.  Первая очередь замены серверов. | |

# сеть интерфейс трафик протокол

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/н | Имя сервера: Proxy\_cs  Операционная система: Windows NT 4.0  Роль сервера: Интернет сервер (WinGate), почтовый сервер (MDaemon) | Критично | Не удовлет-ворительно | Удовлет-ворительно |  |
| 1 | Загруженность сервера | ⬜ | ⬜ | ✔ | Нет проблем |
| 2 | Устойчивость к сбоям | ⬜ | ✔ | ⬜ | Дисковая подсистема не настроена на противодействие сбоям, выход из строя одного из винчестеров приведет к краху всей системы однако возможность переложить задачи данного сервера на другую машину позволяет не рассматривать данную проблему как критичную. Остальные компоненты сервера также не могут обеспечить избыточность. |
| 3 | Восстановление после сбоев | ⬜ | ✔ | ⬜ | Отсутствие Disaster Recovery BackUp увеличивает время восстановления сервера «с нуля». |
| 4 | Защита данных от НСД | ✔ | ⬜ | ⬜ | Очень серьезные проблемы безопасности (см. результаты сканирования на уязвимость) |
| 5 | Общая оценка состояния сервера | ✔ | ⬜ | ⬜ | Очень серьезные проблемы связанные с обеспечением безопасности, данный сервер может быть взломан из Internet и использован в качестве плацдарма для доступа во внутреннюю локальную сеть.  В качестве временных мер решения данных проблем можно порекомендовать установку firewall (например Kerio WinRoute Firewall).  Рекомендуется полная замена данного сервера.  Первая очередь замены серверов. |

# Приложение 2

## Предложения и рекомендации

### 

### Предложение по обеспечению защиты периметра сети

### 

### Общая схема

Данная схема соответствует существующей в Банке в настоящий момент, но в тоже время обеспечивает высокую степень защиты и контроля сетевой безопасности. За счет сохранения неизменности сетевой структуры риски простоя связанные с внедрением новой системы защиты удается свести к минимуму.

Изменения касаются аппаратного программного обеспечения серверов доступа.

В качестве аппаратной платформы предлагается использовать сервера HP ML110.

В качестве программного обеспечения Windows 2000 Server с установленным Internet Security & Acceleration Server и Symantec Antivirus for Microsoft ISA Server.

Данное решение позволяет достичь следующих результатов:

* Защита от несанкционированного доступа в локальную сеть извне
* Контроль и протоколирование использования Internet ресурсов локальными пользователями
* Фильтрация нежелательно web и SMTP контента
* Антивирусная проверка входящего web трафика, а также всего почтового
* Протоколирование распространенных сетевых атак (например попытка сканирования открытых портов)
* Немедленное оповещение администратора о сетевых атаках
* Немедленное оповещение администратора о вирусах
* Кэширование web контента позволяет сэкономит Интернет трафик одновременно увеличивая скорость работы Internet

### Организация почтовой системы

Данное решение предполагает использование сервера доступа в Интернет для контроля SMTP трафика (проверка на вирусы, контроль нежелательной почты) переложив задачи хранения и авторизации клиентов на Exchange сервер.

Это позволит использовать единую пользовательскую базу, что в свою очередь упростит ее администрирование и сократить количество возможных ошибок, разграничить выполняемы функции между серверами.

В тоже время это накладывает ряд требований связанных к надежности и производительности Exchange сервера. В качестве аппаратной платформы для Exchangr Servera предлагается использовать HP ML350.

### Организация доступа в Интернет

Контроль использования Интернет ресурсов может основываться целым рядом параметров таких как:

* IP адрес пользователя, его имя и принадлежность к группе
* Тип запрашиваемой информации или конкретный Интернет ресурс
* Время

В тоже время осуществляется антивирусная проверка полученной из Интернета информации. Количество пользователей использующих доступ в Интернет ограничено количеством клиентских лицензий антивирусной программы. В предложении количество лицензий – 70.

### 

### Подключение внешних пользователей к RS-Bank

Подключение внешних пользователь к системе RS-Bank останется неизменным для существующих пользователей.

Информация для заказа:

|  |  |  |
| --- | --- | --- |
| 339044-421 | ProLiant ML110T01 P2.8/800HT 256 SCSI-36 (P4-2.8GHz/1MB/256MB/36,4GB SCSI/CD/1x10/100/1000NIC) | 1 |
| 353377-B21 | HP NC1020 10/100/1000T Gigabit Server Adapter 32 PCI | 1 |
| 271832-B21 | 36GB 10K U320 Non-Plug Ultra320 10K Hard Drive (1") (for all non HotPlag bays and servers) | 1 |
| 354557-B21 | 256 UNREG PC3200 1X256 ML110 | 1 |
| 354560-B21 | 512 UNREG PC3200 1X512 ML110 | 1 |
| P73-00663 in pack | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt | 1 |
| E84-00005 | ISA Server 2000 English Intl CD 1 Processor License | 1 |
| 10149637-IN | SYMANTEC ANTIVIRUS 4.3 FOR MICROSOFT ISA SERVER IN MEDIA PACK | 1 |
| 10202006 | SYMANTEC ANTIVIRUS 4.3 FOR MICROSOFT ISA SERVER LIC | 70 |

|  |  |  |
| --- | --- | --- |
| 339044-421 | ProLiant ML110T01 P2.8/800HT 256 SCSI-36 (P4-2.8GHz/1MB/256MB/36,4GB SCSI/CD/1x10/100/1000NIC) | 1 |
| 353377-B21 | HP NC1020 10/100/1000T Gigabit Server Adapter 32 PCI | 1 |
| 271832-B21 | 36GB 10K U320 Non-Plug Ultra320 10K Hard Drive (1") (for all non HotPlag bays and servers) | 1 |
| 354557-B21 | 256 UNREG PC3200 1X256 ML110 | 1 |
| P73-00663 in pack | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt | 1 |
| E84-00005 | ISA Server 2000 English Intl CD 1 Processor License | 1 |

Microsoft Internet Security and Acceleration (ISA) Server 2000 — это расширяемый многоуровневый сервер брандмауэра предприятия и кэширования веб-содержимого, который обеспечивает безопасную быструю и управляемую работу с интернетом. Сервер ISA — это комплексное решение, направленное на защиту на уровне приложений, работу с виртуальными частными сетями (VPN), динамическую проверку пакетов и безопасную публикацию, защищающую ресурсы пользователей. Кроме того, сервер ISA может выступать в роли надежного, масштабируемого и высокопроизводительного веб прокси и сервера кэширования, повышающих эффективность вашей работы и рационально расходующих ресурсы сети.

| Возможности | Технологии |
| --- | --- |
| Дополнительная защита на уровне приложений | |
| Фильтры приложений | Создают дополнительный удобный в управлении уровень защиты почтовых серверов, веб-серверов и серверов Microsoft Exchange Outlook® Web Access (OWA), расположенных за брандмауэром. К возможностям этих фильтров относится поддержка протоколов HTTP, FTP, SMTP (Simple Mail Transport Protocol), H.323 (протокол передачи мультимедиа), поддержка потокового мультимедиа, удаленного вызова процедур (RPC) и т. д. |
| Почтовые фильтры | Позволяют находить сообщения, содержащие нежелательные слова или приложения, тем самым повышая безопасность почтового сервера. |
| Фильтрация удаленного вызова процедур Exchange | Обеспечивает защиту удаленных пользователей сервера Exchange Server от угроз, связанных с сетями без доверия, не использующими VPN. |
| Улучшенная безопасность OWA и IIS | Улучшенные системы проверки подлинности и защиты серверов, использующих службы IIS (Internet Information Services) и OWA (Outlook Web Access), от различных типов атак из интернета. |
| Динамическая проверка | Проверка данных, проходящих через брандмауэр, в контексте их протокола и состояния подключения. При динамической фильтрации пакетов порты открываются только в тех случаях, когда это необходимо. |
| Расширяемая архитектура фильтров | Партнерские дополнения (EN) для сервера ISA, поддерживающие фильтрацию адресов URL, антивирусную проверку, балансировку нагрузки и т. д., позволяют вам разрабатывать фильтры приложений для перехвата, анализа и изменения данных, приходящих на любой порт и по любому протоколу. Кроме того, вы сможете создавать на базе интерфейса ISAPI (Internet Server Application Programming Interface) веб-фильтры для просмотра, анализа, блокировки, пересылки и изменения трафика HTTP, HTTPS и FTP. |
| Приоритеты полосы пропускания | Позволяют оптимизировать выделение ресурсов полосы пропускания в зависимости от пользователя, группы, приложения, узла назначения или типа содержимого. |
| Быстрый и безопасный прокси- и кэш-сервер | |
| Высокопроизводительный веб-прокси и сервер кэширования | Быстрое кэширование в оперативной памяти и эффективное использование кэша на сервере ISA увеличивают скорость доступа пользователей в интернет и снижают нагрузку на сеть. |
| Масштабируемость | Динамическая балансировка нагрузки сети и применение протокола CARP (Cache Array Routing Protocol) дают вам возможность быстро и эффективно наращивать мощность системы добавлением новых серверов. Кроме того, сервер ISA поддерживает архитектуру многопроцессорной симметричной обработки (SMP). |
| Распределенное и иерархическое кэширование | Вы можете объединять серверы кэширования в иерархические структуры, располагая кэши вблизи от пользователей и создавая резервные каналы передачи данных. |
| Активное кэширование | Регулярное обновление постоянно используемых объектов позволяет снизить нагрузку на сеть. |
| Планирование загрузки данных | С помощью расписания вы можете планировать загрузку объектов в кэш, чтобы эффективнее использовать ресурсы сети, обслуживать зеркальные серверы и иметь автономный доступ к необходимым данным. |
| Поддержка потокового мультимедиа | Сервер ISA обеспечивает прозрачную поддержку популярным форматам мультимедиа и экономно использует полосу пропускания, разделяя потоки данных, проходящих через шлюз. |
| Встроенные средства повышения производительности, управления доступом и безопасностью, поддержки VPN | |
| Интеграция с Windows 2000 Server | Пользователи, параметры конфигурации и правила сервера ISA используют службу каталогов Microsoft Windows® 2000 Active Directory®. Службы проверки подлинности и управления полосой пропускания, сетевые службы и средства управления построены на базе технологий Windows 2000 Server. |
| Многоуровневый брандмауэр | Улучшенная система защиты, включающая в себя фильтрацию трафика на уровне пакетов, каналов и приложений. |
| Поддержка широкого круга приложений | Вы можете работать с десятками основных приложений Интернета с помощью предварительно заданных протоколов, в том числе прозрачных средств SecureNAT (Secure Network Address Translation), RSA SecurID, Active Directory, IIS, OWA, Exchange, Microsoft SQL Server™ 2000, Microsoft BizTalk® Server 2002, клиентов веб-прокси и фильтров приложений. |
| Встроенная поддержка VPN | Стандартные службы протоколов PPTP и L2TP/IPSec системы Windows 2000 обеспечивают безопасное соединение между узлами и удаленное подключение через виртуальные частные сети. |
| Усиление защиты системы | Вы можете защитить операционную систему Windows 2000 Server, задав соответствующий уровень безопасности с помощью готовых шаблонов. |
| Единая система обнаружения вторжений | Технология, созданная на базе систем Internet Security Systems (ISS) (EN), позволяет обнаруживать попытки совершения таких атак, как сканирование портов, WinNuke и Ping of Death, и принимать ответные меры. |
| Прозрачность для всех клиентов | Сервер ISA с помощью службы SecureNAT создает защиту брандмауэром, прозрачную для всех клиентов, использующих протокол IP (Internet Protocol). При этом не нужно устанавливать дополнительных клиентов или клиентскую программу брандмауэра, выполнять прозрачную проверку подлинности и обеспечивать поддержку широкого круга приложений. |
| Улучшенные механизмы проверки подлинности | Встроенная проверка подлинности Windows (NTLM и Kerberos), цифровые сертификаты, поддержка простого и цифрового режима проверки подлинности делают систему защиты еще более надежной. |

Дополнительная защита на уровне приложений

Сервер ISA и пакет дополнений Feature Pack 1 позволяют создать дополнительный удобный в управлении уровень защиты почтовых серверов, веб-серверов и серверов Exchange для OWA (Outlook Web Access), расположенных за брандмауэром. Почтовые серверы становятся более безопасными, поскольку теперь они могут вовремя перехватывать сообщения, содержащие нежелательные слова или вложения. Кроме того, сервер ISA и пакет дополнений Feature Pack 1 обеспечивают защиту пользователей Outlook, удаленно подключающихся к серверу Exchange с помощью сетей без доверия, не использующих VPN.

Один из примеров тщательной проверки передаваемых данных. Сервер ISA Server и пакет дополнений Feature Pack 1 могут на уровне приложений останавливать атаки, связанные с декодированием Unicode, прохождением каталогов и неправильным формированием запросов HTTP, и предупреждать проникновение опасных запросов в сеть.

Быстрый и безопасный прокси- и кэш-сервер

Сервер ISA может повысить эффективность работы ваших сотрудников, увеличив скорость доступа в Интернет. Более высокая скорость доступа достигается за счет хранения веб-содержимого физически вблизи пользователей. Сервер ISA имеет легко масштабируемую архитектуру, позволяющую с помощью протокола CARP объединить несколько компьютеров с серверами ISA в кластер и увеличить объем кэша. При применении иерархического кэширования данные автоматически распределяются между серверами, которые могут быть расположены по всему миру. Использование средств управления доступом обеспечивает не только высокую скорость доступа в Интернет, но и контроль над ним.

Средства управления доступом, протокол CARP и иерархическое кэширование дают следующие преимущества.

Сервер ISA позволяет выполнять фильтрацию по адресам URL и типам MIME, а также обеспечивать защиту от незаконного использования ресурсов сети.

Применение протокола CARP позволяет автоматически масштабировать кэш в массиве серверов, повышая эффективность его использования. При этом объекты автоматически загружаются, кэшируются и передаются клиенту.

Иерархическое кэширование позволяет хранить данные физически вблизи пользователей, повышая тем самым производительность сети.

Единая система кэширования, безопасности и служб VPN предоставляет следующие преимущества.

За счет хранения данных физически вблизи пользователей кэширование позволяет повысить производительность сети и увеличить максимальное число поддерживаемых ею пользователей.

Сервер ISA поддерживает управление доступом как изнутри сети, так и извне, вы можете размещать в Интернете свои службы, будучи уверены, что никто из ваших сотрудников не имеет доступа к незаконным ресурсам Интернета. Единая система доступа подразумевает, что повышение производительности сети с помощью сервера ISA не создает угроз безопасности.

Интеграция с VPN позволяет удаленным пользователям подключаться к внутренней сети организации и управлять безопасностью сети с помощью одного переходного устройства.

### Symantec AntiVirus for Microsoft Internet Security and Acceleration (ISA) Server

Ключевые возможности

Использует лучшие в своей области технологии Symantec, чтобы обеспечить надежную и масштабируемую защиту от вирусов для веб- и SMTP-трафика

Разработан специально для защиты трафика, обслуживаемого сервером ISA Server

Без труда настраивается для защиты пользовательской информации от комбинированных угроз и для проверки файлов всех основных типов, включая сжатые файлы

Эффективно использует возможности генерации предупреждений, которыми располагает сервер ISA Server

Включает развитые функции, позволяющие блокировать вирусы, поступающие с сообщениями электронной почты, до того, как будет найдено средство для лечения заражения

Позволяет администраторам фильтровать почтовые сообщения, создающие чрезмерную нагрузку на сеть

Поддерживает как автономную реализацию сервера ISA Server, так и реализацию в виде массива серверов (array implementation), что способствует гибкому развертыванию

Легко масштабируется, позволяя справляться с растущим объемом трафика

Оптимизирован для достижения высоких скоростных характеристик, что позволяет потреблять минимум ресурсов существующей сетевой инфраструктуры

Обеспечивает поддержку многих платформ при работе в гетерогенных сетевых средах

Поддержку продукта осуществляет Symantec Security Response – организация, занимающаяся исследованиями и обслуживанием пользователей в сфере интернет-безопасности и являющаяся мировым лидером в этой области

Быстродействующая, масштабируемая и надежная защита от вирусов для веб- и SMTP-трафика

Symantec AntiVirus для Microsoft® Internet Security and Acceleration (ISA) Server представляет собой быстродействующее надежное средство антивирусного осмотра и лечения Данное решение создавалось специально для защиты трафика HTTP, FTP и SMTP на сервере ISA Server; оно опирается на лучшие в своей области технологии Symantec, оптимизированные для достижения высоких скоростных характеристик и потребляющие минимум ресурсов существующей сетевой инфраструктуры.

С помощью консоли ISA Management Console администраторы могут без труда настраивать пакет Symantec AntiVirus и управлять им, защищая пользователей от распространяемых по электронной почте и через Интернет вирусов, "червей", вредоносных мобильных кодов и от "троянских" компонентов в файлах всех основных типов, в т. ч. в сжатых файлах. Благодаря использованию функции LiveUpdate™ и технологии NAVEX™ средства нейтрализации вирусов можно быстро развертывать в масштабах предприятия, что обеспечивает эффективную защиту всей корпоративной информации. Развитые возможности продукта позволяют администраторам: обновлять описания вирусов как автоматически (по расписанию), так и в ручном режиме (с немедленным вводом в действие); блокировать вирусы, поступающие с сообщениями электронной почты, до тех пор, пока не будет найдено средство для лечения заражения; отфильтровывать почтовые сообщения, создающие чрезмерную нагрузку на сеть. Администраторы могут немедленно получать уведомления о вирусной активности как с помощью средств SNMP или SMTP, так и путем использования встроенных в сервер ISA Server механизмов генерации предупреждений; существует также возможность подготовки сводных отчетов через веб-интерфейс.

Symantec AntiVirus для ISA Server поддерживает как автономную реализацию сервера ISA Server, так и реализацию в виде массива серверов, что способствует гибкому развертыванию. Осмотры могут проводиться на том сервере, где установлено программное обеспечение ISA Server, или (при росте трафика) на многих серверах в сети, работающих под управлением операционных систем Microsoft Windows® 2000, Sun™ Solaris™ или Red Hat® Linux®. Организации и предприятия, в сети которых установлен пакет Symantec AntiVirus для ISA Server, получают дополнительный уровень защиты от вирусов, предохраняющий от комбинированных угроз, связанных с атаками по многим сетевым протоколам.

HP ProLiant ML110 — идeальноe рeшeниe для малых и срeдних прeдприятий, которым нужны надeжныe высокопроизводитeльныe сeрвeры по цeнe настольных компьютeров. Это новоe дополнeниe сeрии сeрвeров HP ProLiant 100 с процeссором Intel Pentium 4 с шиной 800 МГц, расширeнным объeмом двухканальной памяти PC3200, встроeнным гигабитным сeтeвым контроллeром Ethernet и поддeржкой до 5 устройств PCI (из них 3 — PCI-X). Кромe того, сeрвeр обладаeт достаточными возможностями модeрнизации для удовлeтворeния растущих потрeбностeй прeдприятия — используя систeму сeйчас, ee можно расширить в будущeм.

Для обeспeчeния дополнитeльной гибкости при выборe выпускаются модeли этого сeрвeра с дисковым интeрфeйсом SCSI и ATA/100, а так же может комплектоваться опциональным RAID-контроллером.

|  |  |
| --- | --- |
| характеристика | описание |
| типичное применение | файл и принт — сервер, централизованный доступ в интернет, приложения небольших рабочих групп |
| количество процессоров | 1 |
| набор микросхем | Intel E7210 |
| оперативная память | от 256 МБ до 4 ГБ PC3200 DDR SDRAM |
| расширенная защита памяти | Advanced unbuffered ECC |
| сетевой контроллер | Broadcom 5705 PCI Gigabit NIC (embedded) 10/100/1000 WOL (Wake on LAN) |
| слоты ввода / вывода | 64 рязрядные 66 МГц PCI-X — 3 (модели с интерфейсом ATA)/2 (модели с интерфейсом SCSI)  32 рязрядные 33 МГц PCI — 2 |
| дисковый контроллер / RAID-контроллер | одноканальный Ultra320 SCSI адаптер HP |
| флоппи-дисковод | 1,44 МБ |
| оптический привод | 48× CD-ROM |
| максимальное количество стандартных внутренних дисковых отсеков | 4×1″ (SCSI) |
| максимальная емкость внутренних накопителей | 144 ГБ (4×36 ГБ) |
| интерфейсы | USB — 2  последовательный — 1  параллельный — 1  указательное устройство (мышь) — 1  графический — 1  клавиатура — 1  разъем RJ-45 — 1 |
| графический адаптер | интегрированный видеоконтроллер ATI RAGE XL с 8 МБ видеопамяти SDRAM |
| форм-фактор | башня (высота 5U) |
| соответствие отраслевым стандартам | ACPI V1.0b Compliant  PCI 2.2 Compliant  PXE Support  WOL Support  Microsoft® Logo certifications  Novell Logo certifications |
| габариты (В×Ш×Г) | 43×20×55 см |
| вес | 16,8 кг |
| требования к питанию | напряжение от 90 до 135 В / от 180 до 265 В частота тока от 50 до 60 Гц |
| максимальная выходная мощность (одного источника питания) | 350 Вт |
| температура | рабочая: от 10 до 35 ºC хранения: от -40 до 66 ºC |
| влажность (без конденсации) | рабочая: от 20% до 80% хранения: от 5% до 90% |
| гарантия (части / работы / выезд) | 1 / 1 / 1 |

## Сeрвeр приложeний начального уровня, прeдназначeнный для использования на прeдприятиях малого и срeднeго бизнeса и в филиалах крупных организаций. Срeдства повышeния надeжности, такиe как возможность установки 6 дисков с горячeй замeной и рeзeрвного блока питания, рeализованныe в этом сeрвeрe, дeлают eго очeнь удачным приобрeтeниeм для нeбольших организаций, которым нeобходимо обeспeчить постоянную доступность данных и приложeний.

|  |  |
| --- | --- |
| характеристика | описание |
| типичное применение | файл- и принт-сервисы, централизованный доступ в интернет, приложения небольших рабочих групп |
| процессоры | Intel Xeon 2,8 ГГц |
| кэш-память | 1 МБ кэш-памяти третьего уровня (модель 2,8 ГГц)  512 КБ кэш-памяти третьего уровня (модели 2,8 и 3,06 ГГц)  512 КБ кэш-памяти второго уровня (все модели) |
| количество процессоров | до 2 |
| набор микросхем | чипсет ServerWorks Grand Champion LE с шиной 533 МГц FSB |
| оперативная память | 1 ГБ PC2100 DDR SDRAM |
| расширенная защита памяти | Advanced ECC |
| сетевой контроллер | интегрированный NC7760 10/100/1000 WOL |
| слоты ввода / вывода | 5 (4×64-бит / 100 МГц PCI-X + 1×32-бит / 33 МГц PCI (5V совместим со старыми платами) |
| дисковый контроллер / RAID-контроллер | интегрированный двухканальный Wide Ultra3 SCSI |
| флоппи-дисковод | 1,44 МБ |
| оптический привод | 48x CD-ROM  опциональный DVD-ROM  опциональный CD-RW/DVD Combo |
| максимальное количество стандартных внутренних дисковых отсеков | 8×1" Ultra3 / Ultra320 (с установленной опциональной корзиной для двух дисков с «горячей» заменой)  2 отсека для сменных накопителей |
| максимальная емкость внутренних накопителей | 1,174 ТБ SCSI (6×146,8 ГБ + 2×146,8 ГБ) с опциональной корзиной для двух дисков с «горячей» заменой |
| интерфейсы | USB — 2  последовательный — 1  параллельный — 1  манипулятор (мышь) — 1  графический — 1  клавиатура — 1  разъем RJ-45 — 1  внешние SCSI — 2 |
| графический адаптер | интегрированный видеоконтроллер ATI RAGE XL с 8 МБ видеопамяти SDRAM |
| поддержка ленточных накопителей с возможностью «горячей» замены | да |
| поддержка remote insight lights-out edition II |  |
| поддержка proliant essentials foundation pack |  |
| поддержка proliant essentials value pack | RDP, WMP, RSO, PMP |
| форм-фактор | башня (трансформируется для монтажа в стойку, высота 5U) |
| соответствие отраслевым стандартам | ACPI V1.0B Compliant  PCI 2.2 Compliant  PXE Support  WOL Support  PCI-X 1.0 Compliant  Novell Certified  Microsoft Logo certifications |
| габариты (В×Ш×Г) | 46,99×26,04×66,04 см |
| вес | 27,24 кг |
| требования к питанию | напряжение от 100 до 120 В / от 200 до 240 В  частота тока от 50 до 60 Гц |
| максимальная выходная мощность (одного источника питания) | 500 Вт |
| температура | рабочая от 10 до 35 ºC  хранения от -40 до 70 ºC |
| влажность (без конденсации) | рабочая от 10 до 80%  хранения от 5 до 90% |
| гарантия (части / работы / выезд) | 3/3/3 |

### Информация для заказа:

Exchange

|  |  |  |
| --- | --- | --- |
| 311525-421 | Proliant ML350T03 G3 X2800/533 SA641 (Tower Xeon 2.8Ghz(512kb)/512mb/HotPlug/RAID SA641/noHDD/CD/GigabitEth) | 1 |
| 286776-B22 | 36GB 15K U320 HotPlugUniversal HDD (For HP Proliant Hot Plug servers and modular smart array storage systems) | 2 |
| 286778-B22 | 72GB 15K U320 HotPlug Universal HDD (For HP Proliant Hot Plug servers and modular smart array storage systems) | 3 |
| 287496-B21 | 512 REG PC2100 DDR SDRAM DIMM Kit (ML310/ML350G3/DL320G2/ML330G3) | 1 |
| 312-02613 | Exchange Svr 2003 English CD 5 Clt | 1 |
| P73-00663 in pack | Windows Svr Std 2003 Russian DSP OEI CD 1-4CPU 5 Clt | 1 |

## Рекомендации по средствам управления сетью

Компания HP первой начала работу в области управления серверами в начале 1990-х годов и с тех пор неизменно лидирует в этой области, разрабатывая и популяризируя стандарты, которые сегодня широко применяются в компьютерной индустрии. Компания HP накопила огромный опыт по управлению сетями, можно увидеть, что все обсуждаемые инструментальные средства основаны на протоколе SNMP. Повсеместное применение протокола SNMP значительно упрощает интеграцию инструментов управления серверами HP в другие платформы BMC, Computer Associates, IBM/Tivoli и других ведущих производителей.

средства управления

|  |  |
| --- | --- |
| название | описание |
| Продукты Legacy Intelligent Manageability | Многие устаревшие продукты, ранее поставлявшихся на компакт-дисках Compaq SmartStart и Management, и сейчас можно загрузить из интернета. |
| ProLiant Essentials Foundation Pack | Инструменты настройки, управления и поддержки, упрощающие настройку и эксплуатацию серверов ProLiant в составе адаптивной инфраструктуры. Содержат агенты Insight Management, а также SmartStart. |
| Insight Manager | Полное управление серверами ProLiant с использованием функций Lights-Out, профилактическое прогнозирование неполадок, минимизация времени простоя системы. Контроль более чем 1000 параметров системы ProLiant, в том числе параметров сетевых адаптеров, дисков, памяти и питания. |
| Агенты Insight Management | Обеспечивают прямой доступ ко всей аппаратуре, встроенной в серверы, рабочие станции, настольные компьютеры и портативные компьютеры HP для отслеживания более чем 1000 параметров. |
| Агенты интеграции для Insight Manager | Интеграция возможностей интеллектуального управления в популярные среды (например, HP OpenView или MS MOM) за счет наблюдения за выполнением отдельных функций сервера с помощью специализированных агентов. |
| SmartStart | Единый инструмент автоматизации настройки серверов с драйверами для всех версий основных операционных систем. Поставляется на компакт-диске. Идеальное средство для первоначальной настройки аппаратного обеспечения, операционной системы и приложений на любых серверах ProLiant. |
| Профилактическая гарантия | На основе предупреждений о возможных неполадках, выданных программой Insight Manager, компания HP осуществляет гарантийную замену памяти, дисков и процессоров в серверах ProLiant до того, как они выйдут из строя. |
| Active Update — уведомление об изменениях | Уведомление за 30—60 дней до предстоящих изменений, которые могут повлиять на работоспособность вычислительной среды. Позволяет автоматизировать развертывание программных заплаток с помощью Insight Manager. |
| Встроенный процессор Lights-Out | Стандартный компонент современных серверов ProLiant. Позволяет получать текущие данные о состоянии сервера и осуществлять удаленное управление по сети с любого клиента, оснащенного веб-браузером. |
| Remote Insight Lights-Out Edition | Плата PCI, предоставляющая расширенные возможности по удаленному управлению серверами ProLiant, расположенных в центрах обработки данных и удаленных филиалах, с помощью браузера. Это решение позволяет управлять серверами независимо от того, где они находятся — в соседней комнате или на другой стороне земного шара. |
| Integrated Administrator | Единая консоль управления полкой блейд-серверов ProLiant BL e-класса, работающая совместно с Compaq Insight Manager и SNMP. |
| Наборы инструментов ProLiant Essentials Value Pack | Платные специализированные наборы инструментов управления от HP. В эту категорию входят наборы Insight Lights-Out Advanced Pack, Workload Management Pack, Performance Management Pack, Recovery Server Option и Rapid Deployment Pack. |
| Набор инструментов ProLiant Essentials Integrated Lights-Out Advanced Pack | Предоставляет те же возможности, что и Remote Insight Lights-Out Edition, для любых серверов, в которых установлены интегрированные процессоры Lights-Out. |
| ProLiant Essentials Workload Management Pack | Этот набор инструментов рассчитан на потребителей, которым требуется защита важнейших приложений или четкое распределение ресурсов по приложениям. Набор WMP позволяет распределять память и процессоры между приложениями, работающими под управлением Windows® 2000 Server. |
| ProLiant Essentials Performance Management Pack | Применяется совместно с Insight Manager для тонкой настройки систем ProLiant. |
| ProLiant Essentials Recovery Server Option | Этот продукт позволяет осуществлять высокоэффективный аварийный перенос ресурсов в кластере из двух идентичных систем ProLiant и хранилища Smart Array. Он позволяет минимизировать время простоя серверов в случае отказа. |
| ProLiant Essentials Rapid Deployment Pack | Один из лучших инструментов с графическим интерфейсом. Для оперативного удаленного развертывания нескольких серверов ProLiant достаточно выполнить простейшие операции с помощью мыши. Этот продукт позволяет оперативно включать и отключать нужные ресурсы и выполнять повторное развертывание рабочих серверов. |

Здесь ключевой элемент управления — HP Insight Manager. Это первое приложение для управления серверами, поставляемое вместе с оборудованием. Оно уже стало стандартным корпоративным средством управления, сочетающим в себе информацию об отказах, производительности и управлении узлами сети.

Объединяя современные технологии управления предприятием с последними достижениями веб-технологий, Insight Manager позволяет системным администраторам вести наблюдение и управлять группами серверов, клиентов и сетевых продуктов через стандартные браузеры. Insight Manager может осуществлять поиск и управление устройствами HP и других изготовителей по стандартным протоколам, в том числе SNMP, DMI и HTTP. Программа записывает сигналы тревоги от наблюдаемых устройств и отправляет по электронной почте или на пейджер уведомление ответственному лицу, основываясь на значениях ролей и ответственности.

Insight Manager использует стандартную базу данных SQL в качестве конечного хранилища данных управления. Программу можно настроить для сбора отдельных статистических данных о производительности, конфигурации и неполадках. Следует отметить еще одно важное свойство — при необходимости администраторы могут выполнять запросы к базе данных SQL для просмотра данных о состоянии определенных устройств или типов событий. Кроме того, администраторы могут настраивать Insight Manager с учетом физической структуры сети. Например, при заметном замедлении работы через медленные сети WAN управление удаленными системами можно осуществлять через системы, расположенные рядом, с использованием функции опроса определенных устройств в сети через различные интервалы в зависимости от расположения.

## Комплексное решение

### Обеспечение высокой доступности сети и балансировка нагрузки.

Для достижения максимальной доступности сети предлагается использовать резервирование, как каналов связи, так и центральных узлов сети и комплекс технологий для построения отказоустойчивых сетей.

Для построения отказоустойчивого ядра сети применяются коммутаторы семейства Catalyst 3750 объединённые в стек при помощи технологии StackWise. Коммутаторы семейства Catalyst 3750 обладают повышенной степенью доступности в сети, по сравнению с аналогичными стекируемыми решениями других производителей. Каждый коммутатор может работать в двух режимах — как главный коммутатор стека и как процессор коммутации пакетов. Любой коммутатор в стеке может быть главным, за счет чего обеспечивается отказоустойчивость системы по схеме 1:N. При выходе из строя одного из коммутаторов стека, независимо от выполняемой им функции, остальные будут продолжать выполнение своих функций без остановки работы всей сети. Коммутаторы объединяются в стек при помощи технологии Cisco Systems StackWise. Технология Cisco StackWise позволяет объединить в одном стеке до девяти устройств Gigabit Ethernet, используя специальные стекирующие кабели и программное обеспечение.

Стек коммутаторов логически представляет собой одно устройство, которое управляется внутри стека главным коммутатором (Master Switch). Он автоматически создает и обновляет все таблицы маршрутизации и коммутации стека. Состав работающего стека коммутаторов можно изменять в «горячем режиме», не отключая неизменяемые коммутаторы и не оказывая влияния на общую производительность сети. При выходе из строя основного коммутатора (Master Switch) в течение нескольких секунд все функции маршрутизации переносятся на резервный коммутатор, причём данная процедура абсолютно прозрачна для конечных пользователей.

Каждый коммутатор уровня доступа имеет два гигабитных подключения, по одному к каждому коммутатору уровня ядра и распределения. При этом оба канала работают, обеспечивая общую пропускную способность в 2 Гбит/с и балансировку нагрузки при помощи средств технологии EtherChannel.

### Высокоскоростная коммутация пакетов.

Высокоскоростную коммутацию пакетов в сети предлагается осуществлять при помощи многоуровневых коммутаторов уровня ядра и распределения Catalyst 3750G-24TS-S. Коммутаторы, объединённые в стек при помощи технологии Cisco StackWise, имеют максимальную производительность коммутации на уровне 2 и 3 - 32 Гбит/с. Производительность коммутации стека (64-байтные пакеты) - 38,7 млн. пакетов/сек.

Коммутаторы серии Catalyst 3750 обеспечивают поддержку:

* аппаратной функции CEF (Cisco Express Forwarding);
* статической маршрутизации и динамической маршрутизации с использованием протоколов RIPv1 и RIPv2;
* аппаратной маршрутизации протокола IPv6;
* протоколов динамической маршрутизации OSPF, IGRP, EIGRP и BGPv4 (в ПО EMI);
* PBR (Policy Based Routing);
* протокола PIM (Protocol Independent Multicast);
* туннелирования по протоколу DVMRP (Distance Vector Multicast Routing Protocol);
* функций Fallback Bridging для передачи трафика не IP протоколов между VLAN;
* маршрутизации на всех устройствах стека;
* до 1000 виртуальных интерфейсов и до 468 маршрутизируемых физических интерфейсов в одном стеке;
* до 12 тыс. МАС-адресов;
* до 20тыс. уникальных маршрутов;
* до тысячи групп IGMP;
* кадров Jumbo: до 9018 байт для Gigabit Ethernet и 1546 байт для Fast Ethernet.

### Средства безопасности.

Некоторые из нижеперечисленных функций могут быть недоступны при использовании стандартного образа (SMI).

Поддержка протокола IEEE 802.1x обеспечивает:

* создание динамических правил доступа к каждому порту коммутатора, включая аутентификацию пользователя;
* в сочетании с настройками VLAN, динамическое распределение VLAN вне зависимости от места подключения пользователя;
* в сочетании с настройками голосовых VLAN, принятие решения о подключении IP-телефона вне зависимости от настроек конечного порта коммутатора;
* в сочетании с параметрами безопасности порта коммутатора, аутентификацию порта и управление всеми МАС-адресами клиентов;
* в сочетании со списками доступа, аутентификацию пользователя и настройку порта все зависимости от места подключения пользователя;
* в сочетании с настройками «гостевой» VLAN, обработку запросов протокола IEEE 802.1x от пользователей, желающих получить ограниченный доступ к сети из «гостевой» VLAN.

Списки доступа VLAN (VACL) обеспечивают предотвращения передачи нежелательных потоков данных между различными VLAN в режиме бриджинга.

Списки доступа уровня 2 на каждом порту коммутатора обеспечивают блокировку нежелательных подключений к этому порту.

Обеспечение безопасного доступа к параметрам конфигурации коммутаторов решается с использованием протоколов SSH, Kerberos и SNMPv3.

Механизм Private VLAN Edge позволяет изолировать индивидуальные порты коммутатора друг от друга.

Двунаправленный режим обмена данными на портах SPAN (Switch Port Analyzer) позволяет устройствам IDS (Intrusion Detection System) автоматически предпринимать действия по изоляции нарушителей безопасности.

Доступ к параметрам настройки коммутаторов возможен при авторизации по протоколам TACACS+ и RADUIS.

Система оповещений позволяет администраторам отслеживать добавления и удаления пользователей из сети на основе информации об их МАС-адресах.

По истечении определенного времени информация о МАС-адресах конечных устройств, в случае их отключения, автоматически удаляется из памяти коммутатора, что позволяет другим устройствам подключаться к коммутатору.

Специальный механизм делегирования привилегий предоставляет коммутатору доступ в голосовой VLAN при подключении к нему IP-телефона и запрещает такой доступ при отключении IP-телефона, что не позволяет нарушать политики безопасности.

Многоуровневая система контроля доступа к параметрам конфигурации коммутатора.

Настраиваемый механизм Address learning.

Поддержка сообщений BPDU (Bridge Protocol Data Unit), предотвращающая образование петель в топологии сети на портах PortFast.

Поддержка механизма STRG (Spanning Tree Root Guard).

Функции фильтрации пакетов IGMP.

Поддержка динамической настройки VLAN при использовании сервера VMPS (VLAN Membership Policy Server).

Наличие встроенного ПО Cisco CMS облегчает настройку коммутаторов.

Поддержка до тысячи уникальных правил контроля доступа.

### Подключение серверов.

Выбранная топология и набор технологий позволят обеспечить высокоскоростное надёжное подключение серверов (при необходимости). Если будут использоваться сервера HP возможно использование следующих технологий: Network Fault Tolerance (NFT), Transmit Load Balancing (TLB) и Switch-Assisted Load Balancing (SLB).

|  |  |  |
| --- | --- | --- |
| P/N | Описание | Количество |
| WS-C3750G-24T-S | Catalyst 3750 24 10/100/1000T Standard Multilayer Image | 1 |
| CAB-STACK-50CM= | Cisco StackWise 50CM Stacking Cable | 2 |
| WS-C2950-12 | 12 port, 10/100 Catalyst Switch, Standard Image only | 8 |
| WS-C2950-24 | 24 port, 10/100 Catalyst Switch, Standard Image only | 2 |

Предлагается следующий план перехода:

### 

### 1 этап

Выполняется сейчас

|  |  |
| --- | --- |
| Работы | Бюджет |
| Замена сервера Proxy\_CS | 6205.64 |
| Замена сервера NTServer | 4865.31 |
| Замена сервера Exchange | 8831.63 |
| Обучение сотрудников | 2167.00 |
| Внедрение средств за мониторингом сети HP Insight Manager | 0 |
| Итого: | 22069.58 |

### 

### 2 этап

Выполняется в течении 2-3 лет

|  |  |
| --- | --- |
| Работы | Бюджет |
| Прокладка дополнительных кабелей для обеспечения избыточности | Требуется уточнение |
| Перенос серверов в серверную (желательно совместить с заменой серверов) | 0 |
| Замена сервера Captain | 6122.6 |
| Замена сервера Boatsman | 6122.6 |
| Замена сервера Concord | 3800 |
| Замена сервера Main2K | 5750 |
| Замена сервера BackUp | 3800 |
| Отказ от протокола IPX | 0 |
| Установка дополнительного центрального коммутатора | 6070 |
| Замена коммутаторов доступа | 9150 |
| Итого: | 40815.2 |